Grado en Derecho
Facultad de derecho
Universidad de León
Curso 2015/2016

EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

Informational self-determination Right

Realizado por el alumno D. Víctor Aparicio Fernández

Tutorizado por la profesora Dña. María Esther Seijas Villadangos

ÍNDICE

RESUMEN

Estudio sobre el derecho a la autodeterminación informativa, también conocido como el derecho a la protección de datos. Se pretende llevar a cabo de forma que abarque todos los aspectos necesarios para el conocimiento del derecho en cuestión, desde sus orígenes a su situación actual, pasando por su estructura esencial y su desarrollo a nivel comunitario y estatal.

En una primera parte se hablará de algunas cuestiones previas, como son la explicación de varios conceptos que pueden suscitar dudas y una introducción a las razones por las que se hace necesaria la existencia del derecho objeto de este Trabajo. En la segunda parte, donde se encuentra la mayor parte del Trabajo, se tratará el origen de este derecho en el mundo y en nuestro ordenamiento, su contenido y estructura, su desarrollo normativo y los organismos encargados de su aplicación. Finalmente, en una tercera parte se hará un pequeño análisis sobre la evolución de la protección de datos, desde su origen hasta sus posibles avances en el futuro. En síntesis, la materia de este trabajo se tratará desde la óptica constitucional y en parte administrativa, en lo que se refiere a los mecanismos de aplicación del derecho, para darlo a conocer de forma básica.

Palabras clave: Constitución, intimidad, privacidad, datos personales, Tribunal Constitucional, Europa, autoridades de control.

ABSTRACT

Essay about the informational self-determination right, also known as data protection right. It seeks to include every aspect necessary for the understanding of the right, from its origins to its current situation through its essential structure and its legislative development on a European and Spanish level.

The first part will be about some previous questions, such as the explanation of several concepts that may arise confusion and an introduction to the reasons why it is necessary the existence of the right of which this essay is about. The second part, where most of this Essay lies, will be about the origins of the right in the world and in our law system. It deals about its content and structure, its legislative development and the organizations in charge of its protection. Finally, in a third part a short analysis will be made about the

evolution of the data protection, from its origins to its possible evolution in the future. In short, the object of this essay will be covered from a constitutional perspective and in some parts from an administrative perspective, referring to the mechanisms used to protect the right, and so will be done to make this right better known on its basics.

Key words: Constitution, intimacy, privacy, personal data, Constitutional Court, Europe, supervisory authorities.

ABREVIATURAS

AEPD = Agencia Española de Protección de Datos

BVerfGE =*Bundesverfassungsgerichts*(Tribunal Constitucional Federal de Alemani1.-

CCAA = Comunidades Autónomas

CE = Constitución Española de 1978

DOUE = Diario Oficial de la Unión Europea

DPO = *Data Protection Officer*(Delegado de Protección de Datos)

GPDP = Grupo de protección de las personas en lo que respecta al tratamiento de datos personales

LOPD = Ley Orgánica de Protección de Datos

LOPJ = Ley Orgánica del Poder Judicial

LORTAD = Ley Orgánica de de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

OCDE = Organización para la Cooperación y el Desarrollo Económicos

RGPD = Reglamento 679/2016, General de Protección de Datos

SEPD = Supervisor Europeo de Protección de Datos

SSTC = Sentencias del Tribunal Constitucional

SSTJUE = Sentencias del Tribunal de Justicia de la Unión Europea

STC = Sentencia del Tribunal Constitucional

STJUE = Sentencia del Tribunal de Justicia de la Unión Europea

TC = Tribunal Constitucional

TJUE = Tribunal de Justicia de la Unión Europea

OBJETO DEL TRABAJO

El punto de partida del presente Trabajo es la actual carencia en la doctrina constitucional de un estudio que reúna elementos pedagógicos claros y concisos a la hora de abordar la esencia y los aspectos estructurales del derecho a la autodeterminación informativa.

Si bien se han tratado en numerosos textos varias facetas del derecho en cuestión, ninguno de dichos escritos busca un enfoque didáctico; más bien al contrario: abundan los análisis de jurisprudencia, las tesis y sus antítesis, los estudios de normativa y de supuestos fácticos… Pero basta echar un vistazo a los manuales de Derecho Constitucional para constatar que solo mencionan este asunto, si lo hacen, superficialmente.

Puede considerarse, como más adelante analizaré, que no es ésta una materia que requiera una inmediata y profunda atención; al fin y al cabo los derechos fundamentales a la intimidad y a la libertad de expresión han sido suficientemente trabajados, cubriendo un amplio espectro de situaciones sociales y en este caso sí existe variedad de textos explicativos que se ocupan de todo lo necesario para su correcto entendimiento. Sin embargo, como también tendré ocasión de mencionar en este Trabajo, no hay que minusvalorar la importancia de los derechos de nueva generación que, propiamente desarrollados, darían solución a una serie de problemas actuales y futuros para los cuales los ordenamientos no están de momento preparados.

Igualmente considero importante destacar que los textos mencionados comienzan a quedarse anticuados. Esto suena contradictorio observando que el tratamiento que hago de la autodeterminación informativa es la de un derecho reciente, de última generación (tercera o cuarta, depende del autor), pero hay que tener presente que la vinculación del mismo con las nuevas tecnologías hace que sea necesaria su revisión de forma continua para asegurar su efectividad, puesto que de lo contrario la normalidad superará con creces a la normatividad y la hará inútil[1]. No es exagerado hablar de un derecho fotónico, por lo rápido que se mueve.

Por lo anterior expuesto me dispongo a elaborar un Trabajo que aspira a colmar esta laguna, exponiendo, en su justa medida, las características esenciales del derecho a la

[1] Al respecto se pronuncia el Legislador en la Exposición de Motivos de la LORTAD, epígrafe 6º.

autodeterminación informativa, recogiendo las tesis mayoritarias de la doctrina y la jurisprudencia y explicando su aplicabilidad actual.

Siendo el fin pedagógico el principal, no querría desaprovechar la oportunidad de escudriñar el futuro, tratar de averiguar la dirección hacia la que avanza este joven derecho, así como explorar las futuras oportunidades que ofrece en el ámbito laboral. Esto último porque siendo importante conocer el derecho, también ayuda el tener incentivos para hacerlo.

METODOLOGÍA UTILIZADA

Para la realización de este Trabajo he empleado el método de razonamiento deductivo. El contenido del derecho a la autodeterminación informativa queda identificado mediante el estudio de grandes pronunciamientos legislativos y jurisprudenciales, pasando después a la normativa específica y a los supuestos concretos en los que el derecho queda plasmado en la sociedad.

Así pues, se empezará con la lectura de textos que recojan los citados pronunciamientos legislativos y jurisprudenciales, creando una base de sentencias (muchas de ellas de nuestro Tribunal Constitucional, pero también del Supremo, del Tribunal de Justicia de la Unión Europea, así como de tribunales de otros Estados), normativa (principalmente española -Leyes Orgánicas y sus reglamentos de desarrollo- y europea -Convenios, Directivas y Reglamentos-) y decisiones de distintas organizaciones (desde las agencias de protección de datos -autonómicas, españolas y europeas- hasta la Asamblea de las Naciones Unidas). Asimismo, con carácter ilustrativo y con vistas a un análisis posterior, he añadido a la base noticias y otros documentos provenientes de diversos medios.

Habiendo construido una estructura lógica a seguir para la presentación del contenido el trabajo consistirá en la extracción de la base de los elementos necesarios para elaborar la materia, añadiendo cuando fuese oportuno comentarios propios pero sin olvidar la finalidad didáctica que se pretende que tenga el trabajo.

He de hacer mención igualmente al seguimiento realizado sobre la normativa de este sector a todos los niveles, siendo particularmente importante el reciente Reglamento de la Unión Europea 679/2016 (aprobado el 27 de abril de 2016 y publicado en el Diario Oficial de la Unión Europea el 4 de mayo)por el hito que supone en la regulación de la protección de datos personales y por su inmediata aplicabilidad en los Estados miembros; lo que en el caso de nuestro país va a suponer la revisión y puesta al día, una vez la situación política lo permita, de la legislación aplicable, concretamente de la Ley Orgánica de Protección de Datos de 1999 y su Reglamento de Desarrollo de 2007. En la materia objeto de este Trabajo hay que destacar la trascendencia de los avances normativos, y ello por dos razones: en primer lugar porque al ser un derecho de reciente creación, o mejor dicho, de reciente reconocimiento, cada nuevo paso que se dé en este sentido supondrá un progreso destacable a la hora de definirlo y delimitarlo; y en segundo lugar, porque se trata de un derecho fuertemente vinculado a las nuevas

tecnologías, que como es bien sabido evolucionan a una velocidad tal que van quedando anticuadas de forma continua conforme aparecen versiones mejoradas.

I.- INTRODUCCIÓN

1.- Cuestiones conceptuales

En este primer apartado me gustaría precisar algunos términos que pueden llevar a confusión en el estudio de esta materia.

A) Intimidad-privacidad

Posiblemente el mayor debate que se ha producido en el ámbito de la protección de datos radica en si dicha protección constituye una faceta o una ampliación del ámbito del derecho a la intimidad, o bien se trata de una protección autónoma; igualmente se discute si, en el caso de no formar parte del derecho a la intimidad, nos encontramos ante un derecho fundamental o no.

El origen de esta discusión en nuestro país se encuentra en la redacción del artículo 18.4 de la Constitución:

> "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."

Según la interpretación que se dé a este precepto, es fácil considerar que la protección de los datos personales (ese límite que deberá imponer la ley al uso de la informática) sirve únicamente para hacer efectivo el derecho a la intimidad. Los defensores[2] de esta posición consideran que los avances tecnológicos han creado nuevas formas de obviar la protección a la intimidad de las personas, y por ello este precepto busca constitucionalizar la protección de la intimidad frente a este tipo de agresiones. Por supuesto, esta interpretación del artículo da pie a pensar que el último apartado no es necesario, puesto que el apartado primero del mismo ya protege el derecho a la intimidad por completo, en cualquier aspecto (de forma razonable, dado que no hay derechos absolutos) que se plantee.

Es interesante el análisis de la cuestión que hace el Tribunal Constitucional en su STC 253/1993. El procedimiento al que pone fin esta sentencia se inicia a raíz de la petición

[2] Vgr.: Miguel Rodríguez-Piñero y Bravo-Ferrer; Jesús Sancho Rof; Óscar Alzaga Villaamil. Para el primero, vid. infra en este mismo epígrafe. Para los otros dos, ver nota al pie 28.

de información por parte de un ciudadano a una Administración Pública, petición que no solo se rechaza, sino que ni siquiera es respondida, ni en primera instancia (Gobernador Civil de Guipúzcoa), ni tras recurrir a una instancia superior (el Ministerio del Interior). Tras ver su petición denegada en los tribunales ordinarios, el ciudadano interpone recurso de amparo por considerar que se no se ha respetado su derecho a la intimidad, basando su pretensión en el artículo 18 de la Constitución y en el artículo 8 del Convenio 108 del Consejo de Europa. Si bien en ese momento el concepto que tenía del derecho a la protección de datos era aún ambiguo[3], el Tribunal afirma que el artículo 18.4 CE regula no solo un instituto de garantía de la intimidad y el honor, sino un instituto que es en sí mismo un derecho o libertad fundamental[4]. Este argumento le sirve para conceder el amparo al solicitante, dado que al tratarse de un derecho o libertad independiente cabe la aplicación de lo que sería su núcleo pese a no haber sido desarrollado legalmente, mientras que si se tratase de una extensión del derecho a la intimidad no podría protegerse sin su correspondiente desarrollo legal, porque su contenido escaparía del núcleo del derecho a la intimidad. La falta de desarrollo legal queda suplida mediante la aplicación del artículo 10.2 CE, que dictamina que las normas relativas a derechos fundamentales y libertades reconocidos en la Constitución se interpretarán conforme a los tratados y acuerdos internacionales, en este caso, el artículo 8 del Convenio 108 del Consejo de Europa de 1981.

Igualmente hay que citar como ejemplo de la posición contraria mediante el voto particular que hace Don Miguel Rodríguez-Piñero y Bravo-Ferrer en la misma sentencia. En este voto el Presidente del Tribunal se muestra contrario a conceder el amparo porque considera que la protección de datos personales es una medida complementaria a la protección de la intimidad, y por ende su aplicación en nuestro ordenamiento no es posible sin desarrollo legislativo.

Frente a la idea de que la protección de datos es una garantía más del derecho a la intimidad, se encuentra la tesis según la cual el ámbito de la autodeterminación informativa va más allá de los datos íntimos. Se trata de la privacidad. Esta distinción la explica bien la exposición de motivos de la LORTAD:

[3] A pesar de lo que explico a continuación, el FJ 8º comienza diciendo lo siguiente: "Al desconocer estas facultades, y no responder a las peticiones deducidas por el Sr. O., la Administración del Estado hizo impracticable el ejercicio de su **derecho a la intimidad**…" (la negrita es nuestra)
[4] FJ 6º

> "El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la **privacidad** en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues **en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona** -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, **la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado**. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.[5]"

Distinción que también hace patente el Tribunal Constitucional en su Sentencia 292/2000:[6]

> "…el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el art. 18.4 CE, e igualmente, en expresión bien amplia del propio art. 18.4 CE, al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona…"

La autodeterminación informativa, entonces, es un derecho que funciona en el ámbito de la privacidad, y no de la intimidad, y por lo tanto debe tratarse de forma autónoma respecto a ésta.

[5] Exposición de motivos de la LORTAD, apartado 1º, párrafo 2º. La negrita es nuestra
[6] FJ 6º, párrafo segundo

B) Habeas Data

La primera mención que se hace en un texto normativo al *habeas data* es en la Constitución de Brasil de 1988. El artículo 5 apartado LXXII de la misma reza lo siguiente:

> "LXXII Se concederá "habeas data":
> a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público;
> b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;"

Igualmente es mencionado en la Constitución de la Provincia de Buenos Aires de 1994:

> "Artículo 20
> 3- A través de la garantía de Habeas Data que se regirá por el procedimiento que la ley determine, toda persona podrá conocer lo que conste de la misma en forma de registro, archivo o banco de datos de organismos públicos, o privados destinados a proveer informes, así como la finalidad a que se destine esa información, y a requerir su rectificación, actualización o cancelación. No podrá afectarse el secreto de las fuentes y el contenido de la información periodística.
> Ningún dato podrá registrarse con fines discriminatorios ni será proporcionado a terceros, salvo que tengan un interés legítimo. El uso de la informática no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos.
> Todas las garantías precedentes son operativas. En ausencia de reglamentación, los jueces resolverán sobre la procedencia de las acciones que se promuevan, en consideración a la naturaleza de los derechos que se pretendan tutelar."

Aunque no siempre se mencione la expresión habeas data, su contenido se halla presente en la mayoría de leyes de protección de datos[7]. Así, por ejemplo, se encuentra en los artículos 34 a 40 de la ley francesa, 19 a 24 de la alemana, 27 a 31 de la

[7]De hecho, Heredero Higueras, en su Comentario a la LORTAD, afirma lo siguiente: "[el habeas data]Es, sin duda, el aspecto en el que coinciden todas las legislaciones, aun cuando varíen entre sí en cuanto a las excepciones admisibles y otros extremos"**HEREDERO HIGUERAS, Manuel. 1996.***La Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentario y textos.* Madrid : Editorial Tecnos, 1996. Pág. 129

portuguesa… y en lo que a nuestro país respecta, en el artículo 8.b) del Convenio 108 del Consejo de Europa, en el artículo 15 del Reglamento 679/2016, y en el artículo 15 de la LOPD.

Como se desprende de todos estos artículos, el habeas data (también llamado derecho de acceso) es, esencialmente, el derecho que una persona tiene a conocer qué datos personales sobre la misma se guardan en qué ficheros y con qué finalidad, amén de otra serie de derechos complementarios, como el derecho a saber si se han transmitido o van a transmitir a otros ficheros o personas, el derecho a saber de qué forma se han obtenido los datos, o el derecho a saber a qué órgano de control, si es posible, debe dirigirse para expresar su disconformidad con los datos registrados.

C) Autodeterminación informativa

La RAE define la autodeterminación, en su segunda acepción, como ″Capacidad de una persona para decidir por sí misma algo.″. A modo de ejemplo, la autodeterminación de los Pueblos es el derecho de los mismos a decidir sus propias formas de gobierno, perseguir su desarrollo económico, social y cultural, y estructurarse libremente.

La autodeterminación informativa, en parte, es el derecho de las personas a decidirtodo lo relativo a sus datos personales: cuáles pueden conocerse, cuáles no, quién puede saberlos, en qué momento dejan de ser importantes o vuelven a serlo… Pero esta definición no es suficiente, puesto que aún queda demasiado cerca de la intimidad. Dando un paso más allá, la autodeterminación informativa es también el derecho a que los datos que escapen a nuestro control no supongan un obstáculo para la toma de decisiones del resto de nuestra vida. Un ejemplo:

> "Así, por ejemplo, pensemos en el caso en el que una empresa dedicada a suministrar informes sobre solvencia económica incluya en sus ficheros a una persona cuyo nombre haya aparecido vinculado a una quiebra en una información periodística que, posteriormente, se revele inexacta y que, por olvido o cualquier otra razón, tal empresa no cancele ese registro informático. Ocurrirá entonces que el nombre del perjudicado continuará figurando, normalmente sin que él lo sepa, en

las relaciones de personas de solvencia dudosa que la empresa en cuestión suministre"[8].

Podemos diferenciar la autodeterminación informativa de la intimidad en que el daño provocado a ésta última es irreversible, mientras que el daño hecho a la primera puede detenerse volviendo a poner los datos bajo control. Por ello la protección de la autodeterminación informativa sigue un esquema distinto al de la protección de la intimidad; éste consiste en la ilegalización de las conductas intromisivas en la vida íntima ajena, en las acciones de indemnización cuando se incumplan dichas prohibiciones… Para asegurar el ejercicio de la autodeterminación informativa ha de implementarse un sistema en el que los poderes públicos lleven a cabo una labor activa dirigida a mantener bajo control los datos personales, y por ello se han establecido obligaciones de información y de control de ficheros por parte de quien lleve a cabo el tratamiento de datos.[9]

D) Autoridades de control

Autoridad de control es el nombre que la legislación comunitaria da a los organismos estatales y supraestatales encargados de supervisar el cumplimiento de la normativa de protección de datos; no se incluye en esta definición a las personas que lleven a cabo esta función desde dentro de los organismos que tratan datos personales.

En este Trabajo las referencias hechas a una o a las autoridades de control deben entenderse hechas a la que en cada caso en la práctica vaya a ser competente. En unos casos será la AEPD, en otros una agencia autonómica, o bien una autoridad de otro país o de nivel europeo (el SEPD y el Comité).

[8] **MURILLO DE LA CUEVA, Pablo Lucas. 1993.** *Informática y protección de datos personales. (Estudio sobre la Ley Orgánica 5/1993, de regulación del tratamiento automatizado de los datos de carácter personal).* Madrid : Centro de estudios constitucionales, 1993 ISBN 84-259-0940-6. Pág. 17.

[9] Al respecto de las medidas específicas de protección de datos, ver Capítulo II, apartados 2.- (Análisis del derecho) y C) (Regulación en nuestro ordenamiento siguiendo un criterio cronológico).

2.- La importancia de los datos en la actualidad

El objeto de este Trabajo, como se ha dicho, es el derecho a la autodeterminación informativa, que en lenguaje cotidiano puede entenderse como el derecho a la protección de los datos propios de carácter personal. La razón por la que esta cuestión ha tomado tanta importancia en el mundo en general y en el continente europeo en particular, de forma previsora al principio y cada vez con más fuerza, es que se ha tomado conciencia de los riesgos que entrañan las nuevas tecnologías para los derechos de los ciudadanos.

El hecho de que un dato, una vez subido a la red (lo cual es cada vez más sencillo), pueda ser consultado en tiempo real en cualquier lugar del globo es a la vez una herramienta útil y una potencial fuente de problemas. Uno de ellos, y en lo que a la materia de este Trabajo se refiere, es que la persona a la que se refiere ese dato fácilmente desconocerá a qué fin se destinará el mismo, bien porque desconoce que está en internet, bien porque alguien se ha apropiado de él.

Está muy extendida, aunque cada vez en menor medida, la opinión según la cual los datos que se comparten en red, generalmente, no pueden afectar negativamente a su titular, pues de otro modo no los habría compartido. Al respecto hay que hacer dos reflexiones. En primer lugar, actualmente cualquier acción que se lleve a cabo en la sociedad va a dejar algún rastro en forma de datos: hacerse socio de un club, llevar a cabo una transacción, viajar a algún lugar, tener una conversación con una persona a distancia… todo ello dará lugar a que, consciente o inconscientemente, voluntaria o involuntariamente, una persona ajena a uno mismo posea informaciones que le afectan. En segundo lugar existe la llamada teoría del mosaico. Según esta teoría el riesgo no procede de cada dato individual que se conozca sobre una persona, sino por la organización de todos esos datos individuales en un conjunto o mosaico que permita extraer conclusiones de algún tipo; por ejemplo, una búsqueda realizada por un usuario de internet no acarrea en sí mayores consecuencias, pero esa información juntada con otras búsquedas, con las compras que ha llevado a cabo, y con el haber dado su correo en algún momento llevarán a que diversas compañías se dediquen a enviarle correos muchas veces indeseados; otro ejemplo: la localización de dispositivos que llevan a cabo algunos servidores de internet permiten que se conozca la localización de los

usuarios sin darse estos cuenta, que se sepa las acciones que realizan en sus ordenadores o en sus teléfonos móviles…[10]

Los legisladores estatales y comunitario han entendido que el problema en torno a los datos personales gira en torno a su agrupación en ficheros ordenados que permiten su utilización de forma rápida y masiva, y han actuado al respecto. Para lograr la protección de estos datos se han llevado a cabo y se siguen tomando medidas en varias direcciones.

De forma no poco importante, se está intentando concienciar a la población de la problemática de este asunto para que en su vida diaria tengan más cuidado con sus datos personales. Sin embargo las actuaciones más decisivas son la elaboración de cuerpos normativos que prohíben la recogida y el uso indiscriminado de datos personales, y regulan las condiciones mínimas de seguridad de los ficheros en los que se almacenan.

Puede decirse que aunque aún quede camino por recorrer ya se han dado pasos para responder a los riesgos que entrañan las nuevas tecnologías en este campo.

[10] Un caso reciente de este tipo es la polémica surgida en torno al último sistema operativo de Windows, Windows 10. Este sistema operativo se ha intentado introducir en todos los equipos informáticos de Windows de forma agresiva, tanto en los nuevos como en los que ya utilizaban sistemas antiguos. Y el problema es que la configuración estándar permite controlar la ubicación del usuario, los "*clicks*" del ratón y la pulsación de teclas, entre otras cosas, y enviarlas a terceras personas u organizaciones. El resultado es que el usuario no sabe que está siendo "monitorizado" prácticamente en todo momento, con la excusa de ofrecerle servicios más personalizados; a juzgar por el rechazo que generan los anuncios no deseados (en Windows 10 aparecen anuncios hasta para jugar al clásico juego de cartas "Solitario"), la personalización de ofertas no cosecha demasiados éxitos. Más información sobre Windows 10 puede encontrarse en gran número de publicaciones en internet; por citar dos ejemplos, el diario digital El Confidencial: http://www.elconfidencial.com/tecnologia/2015-08-01/windows-10-espia-tus-movimientos-pero-puedes-evitarlo-siguiendo-estos-pasos_950244/ (visitado el 29 de junio) y la revista también digital RockPaperShotgun: https://www.rockpapershotgun.com/2015/07/30/windows-10-privacy-settings/ (visitado el 29 de junio de 2016).

II.- EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

1.- Génesis del derecho

A) Origen del concepto de la autodeterminación informativa

La idea de que la divulgación de datos personales puede afectar a los derechos de los ciudadanos no es nueva: ya en el siglo XIX juristas de diversos países consideraban el daño que podría suponer la revelación de datos privados al público. Warren y Brandeis, en su afamado artículo "*The Right to Privacy*" (el Derecho a la Privacidad)[11] consideraron que era necesario desarrollar un derecho que protegiese de la divulgación de datos personales, y argumentaban, en contra de otras tesis de la época[12], que este derecho no era meramente una protección de la propiedad intelectual: "la protección concedida a pensamientos, sentimientos y emociones, expresados por medio de la escritura o de las artes, en tanto consista en la prevención de la publicación, no es más que un elemento de la aplicación del más general derecho a la soledad (*the right to be let alone*[13])"[14]; y que tampoco erauna especie de incumplimiento contractual o de traición a una relación de confianza: "los derechos así protegidos, cualquiera que sea su naturaleza, no son derechos que surgen de un contrato o de una especial confianza, sino derechos frente al mundo"[15]. En el mismo artículo se cita la Ley de Prensa francesa de 1868, que en su artículo 11 establece una multa de quinientos francos para aquel que publique un escrito periodístico relativo a la vida privada de alguien.

Con todo, cuesta distinguir estas menciones del actual derecho a la intimidad, por lo que aún quedaba mucho camino por recorrer. A pesar de ello, el hecho de que mucho antes de la aparición de los *mass media* ya se temiese el daño que podía hacer la divulgación de datos personales da cuenta de lo real del peligro, más aún en nuestros días debido a la facilidad con la que se mueve la información.

---

[11] *The Right to Privacy.* **WARREN, Samuel D. y BRANDEIS, Louis D. 1890.**Cambridge, Massachusetts : The Harvard Law Review Association, diciembre de 1890, Harvard Law Review, Vol. IV.

[12] Según Heredero Higueras, el "derecho a la privacidad" en el mundo anglosajón incluía cuatro ilícitos civiles: "a) la intromisión ilegítima en asuntos privados; b) la revelación pública de hechos privados embarazosos sobre una persona; c) publicidad que sitúa al interesado bajo una falsa luza los ojos del público; d) usurpación del nombre o imagen del interesado, en beneficio de otro". **HIGUERAS HEREDERO, Manuel**. 1996. *La Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentario y textos*. Madrid : Editorial Tecnos, 1996. Pág. 12

[13] Literalmente, "el derecho a ser dejado solo", ya mencionado unos años antes en un texto del juez Thomas Cooley.

[14] Ibídem, 205

[15] Ibidem, 213

En los años setenta del siglo pasado se comienza a pensaren el desarrollo de un nuevo derecho autónomo desgajado de la intimidad.A nivel estatal, la Constitución portuguesa de 1976 recoge en su artículo 35, anticipando de forma inteligente la legislación posterior, un derecho a controlar el flujo de datos propios[16], y nuestra propia Norma Suprema contiene en el artículo 18.4[17] una norma que dará pie a la elaboración jurisprudencial del derecho a la autodeterminación informativa en nuestro país. Fuera de la península existían Leyes relativas a la protección de datos en Suecia y en el *Land* de Hesse (Alemania). A nivel europeo, preocupaba que la proliferación de normas estatales sobre esta materia acabase generando contradicciones entre países, lo que minaría la seguridad jurídica de los ciudadanos. Por esta razón en 1975 se inicia un proceso de elaboración de informes y resoluciones[18] que culmina en la Directiva 95/46 del Parlamento Europeo y del Consejo de 24 de octubre de 1995; 21 años más tarde, en abril de 2016, se aprobó el Reglamento que sustituye a esta Directiva: el Reglamento 679/2016[19].

Durante el periodo anterior a la finalización de la Directiva destaca la aprobación en 1981 por el Consejo de Europa del Convenio 108 para la Protección de Personas referido al Tratamiento Automatizado de Datos, que sirve de modelo para la normativa elaborada en las dos décadas siguientes; a título de ejemplo, el artículo 5 requiere que los datos almacenados sean obtenidos de forma legal, con fines legítimos, y que sean adecuados, relevantes y correctos[20], y el artículo 8 regula los derechos de información[21], acceso[22], rectificación y cancelación[23].

[16] "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."

[17] "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."

[18] Al respecto vid. infra apartado 3.-, epígrafe A) sobre la elaboración de la Directiva 95/46.

[19] Sobre el Reglamento 679/2016, vid. infra apartado 3.- epígrafe C).

[20] Artículo cuatro de la LOPD:

"4.-Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."

[21] Artículo catorce de la LOPD:

"14.- Cualquier persona podrá conocer[…] la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento"

[22] Artículo quince de la LOPD:

"15.- El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento"

[23] Artículo dieciséis de la LOPD: "El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días."

Ciñéndonos al objeto de este apartado, hay que señalar como origen del concepto jurídicode autodeterminación informativa la emblemática sentencia dictada en 1983 por el Tribunal Constitucional alemán relativa a la publicación de datos para la elaboración de un censo[24] en la que se menciona por vez primera este derecho (*informationelle Selbsbestimmungsrecht*). El argumento para hablar de la existencia de este derecho es el siguiente: la Constitución contempla como base de los derechos fundamentales la dignidad humana, que permite a los individuos la conducción de su vida privada con libertad para lograr así su autodeterminación, para decidir su destino[25]quien no conozca en todo momento qué, por quién, y para qué se conoce de él fuera de su ámbito privado, no podrá vivir su vida con libertad, puesto que si las personas actuasen teniendo en mente que todo lo que hagan puede ser conocido por los demás, probablemente se comportarían de forma distinta a como querrían hacerlo, incluso en detrimento de sus otros derechos fundamentales; por lo tanto, debe garantizarse como derecho fundamental la capacidad de los ciudadanos de tener bajo control todos sus datos personales, si bien se admiten ciertas limitaciones con arreglo al interés general.[26]

Tres décadas más tarde, el Reglamento 679/2016 de la UE consagra como derecho fundamental la protección de las personas físicas en relación con el tratamiento de datos personales[27].

B) La aparición de la autodeterminación informativa en nuestro ordenamiento

Como he mencionado más arriba, el artículo 18.4 CE contiene la norma que, si bien por sí misma no es suficiente para hablar de la existencia del nuevo derecho, con la ayuda de la jurisprudencia del Tribunal Constitucional sienta las bases para ello.

La elaboración de este precepto no fue tarea fácil, y pudo haber sido suprimido durante la revisión del Anteproyecto. De las 8 enmiendas propuestas, 3 pretendían eliminar este precepto, al entender que su contenido (lo que estos Diputados pensaban que integraba) ya se encontraba reflejado en otros puntos de la Norma[28]. De las otras cinco, la del

[24] Sentencia BVerfGE 65, 1 [Censo de Población]

[25] Artículos 1 y 2.1 de la Ley Fundamental de Bonn. El primero garantiza que "La dignidad humana es intangible", y el segundo contempla el derecho de toda persona "al libre desarrollo de su personalidad".

[26] Vid. infra. apartado sobre los límites del derecho.

[27] Considerando 1º del RGPD

[28] El Diputado de UCD D. Jesús Sancho Rof considera que el apartado 4º no es más que una reiteración de la protección de la intimidad del apartado 1º, mientras que la opinión general del Grupo Parlamentario es que para aportar algo nuevo este precepto debería incluir menciones a otros medios no

Grupo Parlamentario Socialista era una cuestión interpretativa[29], dos ampliaban el concepto de "informática"[30], y una cuarta concretaba el ámbito de protección del precepto, prescindiendo de la mención al honor y la intimidad[31] . En fin, la enmienda propuesta por el Grupo Parlamentario de Minoría Catalana, que fue la que finalmente se llevó a cabo, añadía al final del precepto la expresión "y el pleno ejercicio de sus derechos". Se argumentó para ello que el uso de la informática podría provocar daños que van más allá de la intimidad y el honor, llegando a afectar al resto de derechos fundamentales; argumento que el Tribunal Constitucional alemán haría suyo unos años más tarde en su sentencia sobre el censo de población[32].

Tras la aprobación del texto, tal como sigue vigente hoy en día, faltaba el desarrollo legal que diese forma a la protección otorgada constitucionalmente. Algo que aun tardaría más de una década en implementarse: hasta 1992 no se elabora la Ley Orgánica 5/1992 de 29 de octubre de Regulacióndel Tratamiento Automatizado de los Datos de carácterpersonal (en adelante LORTAD), desarrollada reglamentariamente por el Real Decreto 1332/1994 de 20 de junio. Posteriormente, para adaptar la legislación a la Directiva Comunitaria en materia de protección de datos (Directiva 95/46), se aprueban la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) y su Reglamento de desarrollo (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).

Sin embargo, más importante que la legislación a este respecto ha sido, con diferencia, la jurisprudencia del Tribunal Constitucional, por lo que se puede sostener que estamos ante un derecho de construcción jurisprudencial.

---

informáticos; opinión que refleja Óscar Alzaga en su libro **ALZAGA VILLAAMIL, O**.: *Comentario sistemático a la Constitución española de 1978.* Ediciones del Foro, Madrid, 1978, págs. 209 y 210.

Por otra parte, el diputado de Alianza Popular D. Antonio Carro Martínez entendía que el contenido del apartado cuarto se encontraba reflejado en el artículo 20.6 del Anteproyecto, hoy inexistente, que imponía como límite al derecho de libertad de expresión el respeto al resto de derechos.

[29] Pretendían suprimir la expresión "de los ciudadanos" para dar a entender que la protección de este precepto se brindaría a todos los hombres

[30] Una cambiaba la palabra "informática" por "información"; la otra añadía la expresión "y de cualesquiera otros medios".

[31] Haciendo referencia a las materias concretas que deberían regularse por ley, a saber: "el acopio, uso y difusión de los datos personales contenidos en archivos o registros, susceptibles de acceso automático".

[32] Sentencia BVerfGE 65, 1 [Censo de Población]

Si bien con la aprobación de la LORTAD nadie dudaba de la necesidad de proteger nuestros datos personales, no se terminaba de concebir la existencia de un derecho autónomo únicamente con esta función, que quedaba englobada en la protección de la intimidad. La primera mención que se hace a un "instituto de garantía de otros derechos[…] pero también […] que es, en sí mismo, un derecho o libertad fundamental" es en la STC 254/1993, en la que el intérprete de la Constitución considera adecuados los fundamentos del solicitante de amparo, que argumenta que el derecho a la protección de sus datos goza de protección propia y no requiere de desarrollo legal para su alegación. A partir de este momento el TC dicta una serie de sentencias, destacadamente las SSTC 143/1994 [33] , 11/1998 y 94/1998 [34] , 144/1999 [35] y 202/1999[36],que culmina con las SSTC 290/2000 y 292/2000.

[33] Sentencia regresiva, en el sentido de que considera que la ausencia de garantías en la protección de datos personales supone una lesión a la intimidad, como queda de manifiesto en este extracto: " habría que convenir en que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el **derecho a la intimidad** de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta"(FJ 7º, párrafo 1º *in fine*). La negrita es nuestra.

[34]Ambas forman parte de un grupo de sentencias referidas a la misma cuestión: el sindicato de una empresa convoca una huelga, y la empresa, desconociendo qué empleados en concreto la han secundado, decide retener la parte correspondiente de salario a los trabajadores afiliados al sindicato, hubiesen atendido la huelga o no. El TC falla a favor de los trabajadores, puesto que la empresa utilizó unos datos (la afiliación al sindicato) obtenidos con un determinado fin (transferencia de la cuota sindical) para otro fin distinto (averiguar qué empleados se pusieron en huelga) . Estas sentencias se alejan un poco más de la concepción de la protección de datos como elemento del derecho a la intimidad, al considerar que el artículo 18.4 CE " no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática […], sino que además, consagra un **derecho fundamental autónomo** a controlar el flujo de informaciones que conciernen a cada persona -a la **privacidad** según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos" (STC 11/1998, FJ 5º, párrafo 3º). La negrita es nuestra.

[35] De nuevo una sentencia regresiva: tanto el recurrente en amparo como el TC confunden, en mi opinión, el derecho a la intimidad con el derecho a la autodeterminación, informativa, puesto que consideran de aplicación el artículo 18.1 CE a la protección de datos personales: "Del precepto constitucional[el artículo 18.1] se deduce, de un lado, que el derecho a la intimidad garantiza al individuo un **poder jurídico sobre la información relativa a su persona** o a su familia, pudiendo imponer a terceros, sean éstos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida.[…] De otro lado, el **derecho a la intimidad** impone a los poderes públicos la obligación de adoptar cuantas medidas fuesen necesarias para hacer efectivo aquel poder de disposición, y preservar de potenciales agresiones a ese ámbito reservado de la vida personal y familiar, no accesible a los demás; en especial, cuando la protección de otros derechos fundamentales o bienes constitucionalmente protegidos pueden justificar que ciertas informaciones relativas a una persona o su familia sean **registradas y archivadas por un poder público**". (FJ 8, párrafo 4º).La negrita es nuestra. A mi parecer, cuando las informaciones no están ya al alcance exclusivo del interesado, no corresponde hablar del derecho a la intimidad, puesto que nos encontramos en el ámbito de la privacidad. Al respecto de la distinción privacidad-intimidad, ver capítulo I, apartado 1.- , epígrafe A).

[36] En realidad esta sentencia utiliza los argumentos, extraídos de forma literal, de las SSTC 254/1993 y 143/1994

La STC 290/2000 examina los recursos de inconstitucionalidad presentados por el Grupo Parlamentario Popular, el Defensor del Pueblo, la Generalitat de Cataluña y el Parlamento de Cataluña contra una serie de preceptos de la LORTAD. Al momento de dictar sentencia, la LOPD ya había derogado a su predecesora, por lo que los recursos interpuestos por los populares y por el Defensor del Pueblo son sobreseídos por pérdida sobrevenida del objeto de litigio. El TC sí entra a juzgar la constitucionalidad de las competencias de la AEPD, que según los recursos del Ejecutivo y Legislativo catalanes se extralimitan e invaden el ámbito competencial de la Comunidad Autónoma. El Tribunal rechaza estos recursos argumentando que la protección de datos es un derecho fundamental autónomo, no un mero derecho instrumental[37], y por lo tanto es el Estado el que debe asegurar su disfrute por todos los ciudadanos en situación de igualdad *ex* artículo 149.1.1ª[38].

Finalmente, la STC 292/2000 es la que elabora jurisprudencialmente el derecho a la autodeterminación informativa, en el sentido de que concreta cuál es su contenido esencial y sus límites. En resumen, puesto que sobre ello tratará el capítulo siguiente, el Tribunal concibe la autodeterminación informativa como un derecho al control de los datos personales propios, diferente de la intimidad en tanto que genera obligaciones jurídicas positivas a terceros para su cumplimiento, y limitado por la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

[37] A lo largo de la fundamentación jurídica el Tribunal se refiere a la protección de datos como un derecho fundamental, llegando a afirmar que "la LORTAD […] es la Ley que ha desarrollado un derecho fundamental específico, el derecho a la protección de los datos personales frente al uso de la informática, […]. De lo que se desprende, en definitiva, que el objeto de la Ley cuyos preceptos se han impugnado no es el uso de la informática, sino la protección de los datos personales. De suerte que esta protección mal puede estar al servicio de otros fines que los constitucionales en relación con la salvaguardia de los derechos fundamentales, ni tampoco puede ser medio o instrumento de actividad alguna."(FJ 11 párrafos 6º y 7º).

[38] Dicho artículo reza como sigue:

1. El Estado tiene competencia exclusiva sobre las siguientes materias:

1.ªLa 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.

2.- Análisis del derecho

A) Núcleo del derecho

El carácter cerrado del catálogo de derechos de nuestra Constitución limita el reconocimiento de nuevos derechos constitucionales. Existen dos vías para llevar esto a cabo: o bien se modifica la Constitución[39], o bien el Tribunal Constitucional debe llevar a cabo una labor de construcción jurisprudencial interpretando preceptos de la Constitución.

Para que el TC elabore (interprete) un nuevo derecho constitucional es necesario un "anclaje" en el texto de la Norma Suprema. Para el derecho a la autodeterminación informativa esta base la proporciona el artículo 18.4, como ya se ha visto. Para describir el contenido de este nuevo derecho hay que acudir por ello tanto a la redacción del precepto como a la argumentación que hace el TC.

Del precepto constitucional se deduce que la finalidad de este derecho es evitar el uso indiscriminado de la informática para la transmisión de datos personales, debiéndose regular los límites concretos mediante nuevos textos normativos (Leyes y Reglamentos estatales, Reglamentosy Directivas Europeos…)

Según el TC el derecho fundamental a la protección de datos posee dos peculiaridades que lo hacen único y lo distinguen del derecho a la intimidad. Por un lado los datos a los que se debe brindar su protección son absolutamente todos los que conciernan a la persona, no solamente los íntimos[40]. Por otro lado la protección consiste en atribuir a su titular "un haz defacultades consistente en diversos poderes jurídicos cuyo ejercicio impone aterceros deberes jurídicos, que no se contienen en el derecho fundamental a laintimidad, y que sirven a la capital función que desempeña este derechofundamental: garantizar a la persona un poder de control sobre sus datos personales"[41].

[39] Una medida ciertamente complicada por dos razones: la tradicional dificultad de los partidos políticos españoles para llegar a acuerdos en la inmensa mayoría de las materias, y la rigidez del sistema de reforma constitucional. Sobre las deficiencias de nuestro modelo de reforma constitucional, véase **García Cuadrado, Antonio M.***Principios de Derecho Constitucional.* León : Eolas, 2011, páginas 661 y 662 (parágrafo 492).

[40] FJ 6º de la STC 292/2000, párrafos 1, 2 y 3.

[41] FJ 6º de la misma sentencia, párrafo 4.

A consecuencia de lo anterior, puede decirse que el contenido más elemental del derecho a la autodeterminación informativa son las limitaciones impuestas a la transmisión de datos personales, que incluyen derechos ejercitables por los interesados y obligaciones para terceros y para los poderes públicos. Así, el núcleo del derecho a la autodeterminación informativa, entendiendo como tal el contenido sin el cual dicho derecho quedaría irreconocible, lo componen los derechos de los interesados, denominados frecuentemente "derechos ARCO" [42] , y las obligaciones de los responsables y encargados del tratamiento de datos de procurar unos niveles suficientes de seguridad[43].En efecto, la protección de los datos personales no se entiende sin que existan medidas que impidan el manejo indiscriminado de los mismos.

Definida la base mínima del núcleo del derecho resta describir hasta qué punto llega el núcleo y dónde empieza la parte del derecho susceptible de interpretación. Sin perjuicio de lo dicho en el párrafo anterior hay que señalar que el desarrollo legislativo del artículo 18.4 CE forma esta parte interpretativa, este anillo exterior del contenido del derecho. Puede resultar difícil de entender que los derechos del interesado sean a la vez parte esencial e interpretativa del derecho. Pues bien, la regulación legal, que es lo que da carácter de alterabilidad al desarrollo de las facultades del interesado, no es más que la transposición por escrito de la parte nuclear del derecho, de forma que de no existir, por ejemplo, la LOPD o la LORTAD, debería respetarse igualmente el límite al uso de la informática para la transmisión de datos personales, ya sea acudiendo a otros textos normativos (como el Convenio 108 del Consejo de Europa), ya sea en aplicación directa del artículo 18.4 CE.[44]

En síntesis, la parte nuclear del derecho es la garantía de que los ciudadanos puedan mantener sus datos personales bajo control, y esta parte nuclear puede adoptar la forma que el legislador (español o europeo) quiera darle.

---

[42] Siglas referidas a los derechos de Acceso, Rectificación, Cancelación y Oposición. Aunque estos derechos fueron los que primero surgieron en materia de protección de datos, actualmente han aparecido varios más, siendo importante el derecho al olvido.

[43] Las obligaciones pasivas de los responsables y encargados del tratamiento se han acentuado con el nuevo Reglamento 679/2016 General de Protección de Datos.

[44] Este mismo argumento es utilizado por el TC en su STC 254/1993 al señalar, en primer lugar que "**Un primer elemento, el más «elemental», de ese contenido, es, sin duda, negativo,respondiendo al enunciado literal del derecho: El uso de la informática encuentra un límite enel respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos**" (FJ 7, párrafo 2º ; en negrita en el original); y añadiendo en segundo lugar que a falta de desarrollo legislativo en el momento de iniciarse el proceso corresponde aplicar el Convenio 108 del Consejo de Europa, haciendo así valer el contenido esencial del derecho a la autodeterminación informativa.

B) Límites del derecho

"[N]o existen derechos ilimitados. Todo derecho tiene sus límites que, como señalaba este Tribunal en Sentencia de 8 de abril de 1981 («Boletín Oficial del Estado» de 25 de abril) en relación a los derechos fundamentales, establece la Constitución por sí misma en algunas ocasiones, mientras en otras el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos."[45] Así se expresó el TC sobre la cuestión de la limitación de los derechos constitucionales hace ya 34 años.

Siguiendo el esquema trazado por el Tribunal, pueden distinguirse dos clases de límites: internos y externos. Los primeros se derivan de la propia regulación del derecho, es decir, no se puede extender el contenido del mismo más allá de lo que el Constituyente haya querido hacerlo. Los segundos hacen referencia a las colisiones entre distintos derechos: si no es posible la conciliación de ambos en el mismo espacio, uno deberá prevalecer sobre el otro y actuar como límite para él.

En el caso que nos ocupa, el derecho a la autodeterminación informativa, hay que recordar que es un derecho de construcción jurisprudencial, y por lo tanto para establecer sus límites internos ha de estarse tanto al artículo 18.4 CE como al desarrollo del TC.

La redacción del precepto constitucional puede dar pie a equivocaciones en este aspecto, ya que únicamente se refiere a la limitación de la informática, y no habla de ficheros analógicos de datos[46]. De hecho la LORTAD se refería únicamente a la protección de datos en soporte informático. Actualmente no se pone en duda que los datos en soportes no digitales también deben gozar de la misma protección que los datos en soporte informático, por lo que no puede considerarse éste un límite del derecho. Por lo demás, el artículo está redactado de forma tan amplia que el único límite que cabe interpretar es el de la propia literalidad del texto: el derecho a la autodeterminación informativa consiste en la limitación de la informática para garantizar el honor, la intimidad y el pleno ejercicio de los derechos, y no otra cosa.

[45] STC 2/1982, FJ 5 párrafo 2º.
[46] Entendiendo éstos como los datos recogidos en cualquier soporte no digital, esencialmente en papel.

Por otro lado, los límites externos vienen definidos por los derechos que entren en colisión con la autodeterminación informativa. Podría pensarse que el primer derecho con el que choca es la intimidad, ya que se ha dicho que en el fondo ambos derechos protegen lo mismo y por lo tanto esta duplicidad no tiene razón de ser; sin embargo no se trata de este tipo de choque cuando se habla de limitaciones externas precisamente por ello: ambos derechos protegen bienes jurídicos similares, y no va a haber intereses contrapuestos, es decir, no va a haber dos personas litigando porque el derecho a la autodeterminación informativa afecte negativamente a la intimidad, o viceversa.

En realidad la protección de datos está limitada principalmente por dos derechos: la libertad de expresión y el derecho a la información pública.

El primero viene recogido en el artículo 20 de nuestra Constitución. El punto en el que ambos derechos colisionan es en la expresión de informaciones que contengan datos personales, lo que en materia de protección de datos equivaldría a un tratamiento o a una transmisión a terceros (o al público) de datos personales generalmente sin el consentimiento del afectado. El RGPD, sin solucionar directamente la cuestión, permite a los Estados establecer excepciones a lo dispuesto en la mayor parte del mismo[47]. De momento no existe regulación normativa en nuestro país a este respecto, por lo que hay que acudir a la jurisprudencia constitucional en virtud de la cual la libertad de expresión prima siempre que las informaciones sean veraces y se refieran a figuras públicas.

El derecho a la información pública se encuentra en el artículo 105.b) de la CE. Según este precepto los ciudadanos deben poder acceder a los archivos y registros administrativos, previo desarrollo legal[48]. El problema surge cuando dichos archivos y registros contienen datos personales de ciudadanos. Precisamente el artículo 86 del RGPD habla de conciliar este derecho con la protección de datos, lo que en España se hace en el artículo 15 de la Ley de Transparencia. Aunque, como se hablará más adelante[49], la ponderación de la Administración que según este precepto debe hacerse en ciertas ocasiones ha dado y dará problemas, aún es pronto para saber si ofrece criterios suficientes para que se vayan resolviendo las disputas caso por caso.

[47] Artículo 85, en el Capítulo de Disposiciones relativas a situaciones específicas de tratamiento.

[48] Actualmente esto viene regulado por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

[49] Véase en el apartado siguiente el epígrafe D), que trata de supuestos concretos de regulación de la protección de datos en nuestro ordenamiento.

En síntesis, debido a la novedad que aún supone la protección de datos los límites externos no están del todo claros, pero sí se sabe que tendrán un papel importante la libertad de expresión y el acceso a los ficheros de las Administraciones públicas.

C) Principios de la protección de datos

La existencia del derecho a la autodeterminación informativa no es óbice para que sea posible el tratamiento de datos personales[50] con o sin medios informáticos de por medio. Ahora bien, para respetar el derecho de los interesados es necesario que dicho tratamiento se realice de acuerdo con una serie de principios, que son los que vienen a continuación.

A la hora de recoger los datos deben respetarse dos principios: en primer lugar debe haber una base jurídica para recogerlos, que puede ser el consentimiento del interesado o cualquiera de las excepciones que se prevén[51]. En segundo lugar los datos recogidos solo pueden ser los necesarios para la finalidad perseguida (principio de limitación de datos)[52].

Respecto al tratamiento de los datos es especialmente importante el principio de finalidad o limitación de finalidad, según el cual el uso que se les dé a los datos únicamente puede estar encaminado a la consecución del fin con el que fueron recogidos[53]. El tratamiento con otros fines es ilícito salvo que concurran causas legales que lo permitan. También deben respetarse el principio de exactitud, que prescribe que los datos deben mantenerse actualizados y tienen que modificarse o suprimirse si quedan obsoletos [54]; el principio de limitación de la conservación de los datos, puesto que únicamente pueden almacenarse durante el tiempo necesario para el cumplimiento

[50] El tratamiento de datos personales se encuentra definido de forma más o menos similar en todos los cuerpos normativos que tratan esta materia. La definición más actual, del Reglamento 679/2016, dice así: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

[51] Artículo 6 de la LOPD y artículos 6, 7 y 8 del RGPD

[52] Artículo 4.1 de la LOPD y 5.1.c) del RGPD

[53] Artículo 4.2 de la LOPD y 5.1.b) del RGPD

[54] Artículos 4.3 y 4.4 de la LOPD y 5.1.d) del RGPD

de la finalidad con la que fueron recogidos[55]; y el principio de integridad o seguridad de los datos, que obliga a la adopción de medios técnicos de protección que impidan el deterioro de los datos y su uso por parte de personas no autorizadas[56].

Durante el tiempo que dure el tratamiento el responsable y el encargado del mismo deben actuar de forma lícita, leal y transparente con el interesado (principios de licitud, lealtad y transparencia)[57], y además tienen que tener una actitud proactiva en el cumplimiento de todos estos principios, lo que significa que deben tomar las medidas necesarias "de oficio", sin que nadie se lo pida, y deben de poder demostrar que lo han hecho[58].

D) Facultades y obligaciones que genera

Para cumplir con su finalidad, la limitación del uso de la informática para salvaguardar los intereses de los ciudadanos, el derecho a la protección de datos da lugar a una serie de derechos para los interesados y de obligaciones para los responsables y encargados del tratamiento de datos.

En primer lugar existe un derecho de información para conjurar el principal peligro que corren los ciudadanos en materia de datos personales: no saber que se han tomado algunos de sus datos y van a ser sujetos a tratamiento. Así pues debe informarse siempre de los datos recogidos y de la finalidad con la que se ha hecho, tanto si se obtienen del interesado como de otra persona. Igualmente y con vistas a facilitar el cumplimiento del resto de derechos va a ser necesario que se informe detalladamente de quién o qué organismo es el que ha obtenido los datos y va a utilizarlos, y a quién van a transmitirse, también si van a enviarse a otro país… En definitiva, toda la información concerniente a los datos del interesado.

[55] Artículo 4.5 de la LOPD y 5.1.e) del RGPD
[56] Artículo nueve de la LOPD y 5.1.f) del RGPD
[57] El artículo 5.1.a) del RGPD menciona estos principios, mientras que el artículo 5 de la LOPD lo desarrolla como un derecho a la información del interesado, algo que el Reglamento hace ya en los artículos 12 y siguientes, pertenecientes al Capítulo sobre los derechos del interesado.
[58] Este es un principio que aparece de forma novedosa en el artículo 5.2 del RGPD. La LOPD únicamente menciona un deber de secreto de los responsables y encargados del tratamiento en el artículo 12, y habla de su responsabilidad por la comisión de infracciones en el Título VII.

Como desarrollo lógico del derecho de información existe el derecho de acceso o habeas data. Mientras el primero prescribe que se proporcionen una serie de informaciones en el momento de recoger los datos, el segundo permite al interesado conocer dichas informaciones en cualquier momento. Esta puesta a disposición del estatus de los datos personales sirve para conocer la evolución del tratamiento, también para facilitar el cumplimiento de los demás derechos.

El derecho de rectificación es una consecuencia del principio de exactitud de los datos: cuando hayan dejado de estar actualizados o de ser correctos es posible pedir su puesta al día para evitar que se tomen decisiones basadas en una información errónea. Es en el contexto de este derecho en el que encaja el supuesto utilizado en ocasiones para explicar la peligrosidad de que los datos propios circulen sin control de su titular: una persona contrae una deuda y llegado el límite de tiempo para devolver el dinero no puede hacerlo, por lo que se le cataloga como moroso y así aparece en listas hechas a tal efecto; más adelante consigue pagar la deuda, pero como no conoce la existencia de la lista de morosos (también es importante el derecho de información en este supuesto) y nadie recuerda suprimir su nombre de ella, se le sigue tachando de moroso con todas las consecuencias que esto acarrea. Esto se soluciona poniendo a disposición del interesado, además de la información de que algunos de sus datos han sido recogidos y están siendo utilizados, el derecho a la rectificación de los mismos.

Existen un derecho a la oposición al tratamiento y, en el nuevo RGPD, también un derecho a solicitar la limitación del tratamiento. Estos derechos ponen de manifiesto que el control sobre los datos propios debe ser lo más absoluto posible, habiendo algunas excepciones referidas a intereses mayores (interés público, intereses vitales del interesado o de terceros…). Ambos pueden ser ejercitados por el interesado cuando éste no desee que se utilicen sus datos pero no ve necesario que se supriman de los ficheros en los que se encuentran; esta disyuntiva entre pedir el no tratamiento y pedir la supresión de los datos de los ficheros viene motivada por la dificultad, hasta recientemente, de llevar a cabo lo segundo, puesto que no ha sido hasta la aprobación del RGPD (abril de 2016) cuando se ha regulado un procedimiento efectivo de eliminación de los datos propios en manos de otras personas.

La novedad más importante del RGPD en lo que a derechos de los interesados se refiere es el llamado "derecho al olvido". Si bien la Directiva recogía algo similar en el artículo 12.b)[59], lo hacía incluyéndolo en el derecho de acceso. La razón por la que se ha decidido incluir este derecho como uno autónomo está en la STJUE de 13 de mayo de 2014 en el caso conocido como "Google versus España"[60]. En esta sentencia el TJUE viene a decir tres cosas. En primer lugar, que la actividad del gestor de búsquedas en internet Google Search sí consiste en un tratamiento de datos personales[61], y por ello Google también es responsable de dicho tratamiento[62]. En segundo lugar, que puesto que Google "[ha creado]en un Estado miembro una oficina o filial destinada a la promoción y venta de losespacios publicitarios del motor, que dirige su actividad a los habitantes deese Estado"(párrafos 45 y 59 de la sentencia) corresponde aplicar la normativa española y europea al tratamiento que haga de datos personales. Finalmente, y como punto más importante, el Tribunal argumenta que, teniendo en cuenta lo anterior, el ciudadano interesado tiene efectivamente derecho a solicitar la supresión de sus datos en el buscador[63] en virtud del artículo 12.b) de la Directiva, y que debe llevarse a cabo dicha supresión por cuanto la información que aparece en el buscador no se ajusta a los principios del tratamiento de datos del artículo 6 letras c), d), y e)[64]. Además, el TJUE considera que no existe un interés prevalente sobre el del ciudadano a la protección de sus datos.

[59] Este precepto permite "la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones ce la presente Directiva".

[60] Más concretamente, el litigio, originado en unas cuestiones prejudiciales planteadas por la Audiencia Nacional, enfrentaba a Google Inc. y Google Spain S.L. por un lado y a la AEPD y un ciudadano español por otro.

[61] Tras analizar la actividad del gigante norteamericano el Tribunal concluye lo siguiente (párrafo 28):

"Por consiguiente, debe declararse que, al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas. Ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46, **deben calificarse de «tratamiento» en el sentido de dicha disposición**, sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales." (la negrita es nuestra)

[62] Específicamente, el Tribunal toma la definición que da de los responsables el artículo 2.d) de la Directiva, que dice que lo son los que determinen los fines y los medios del tratamiento. Teniendo en cuenta esta definición, y dado que Google efectivamente determina los fines y los medios de las búsquedas en internet, puede decirse que sí es el responsable del tratamiento (párrafo 33 de la sentencia).

[63] La AEPD consideró que la noticia del diario La Vanguardia a la que hacía referencia el buscador era lícita y no correspondía suprimirla.

[64] La noticia a la que remitía el buscador hacía referencia a una deuda impagada del ciudadano en cuestión, pero dicha deuda ya había sido cancelada en el momento de iniciarse el litigio. Por ello el TJUE consideró que la información ya no cumplía la finalidad para la que se originó.

A raíz de la STJUE el RGPD ha incluido el derecho al olvido como un derecho autónomo[65], del que hay que destacar tres características: se configura no solo como derecho del interesado, sino como una obligación del representante; se especifican las causas que llevan a la supresión de datos[66], como por ejemplo que desaparezca la base jurídica del tratamiento (consentimiento u otros), que se oponga el interesado (y no concurran motivos más legítimos en su contra) o que el tratamiento haya sido ilícito; y se enumeran también excepciones al uso de este derecho, como la concurrencia de razones de interés público en el tratamiento o la prevalencia del derecho a la libertad de expresión e información.

E) Garantías y aspectos procesales

En España, igual que en Europa, las garantías del derecho a la autodeterminación informativa están estructuradas en varios niveles.

El primer lugar al que pueden acudir los ciudadanos que ven afectado su derecho a la protección de datos es a la autoridad de control competente; en el caso de España, será la AEPD[67], o bien las Agencias catalana o vasca. Estos organismos tienen potestad de investigación y sanción, por lo que en principio pueden resolver cualquier controversia en esta materia de forma extra-judicial.

En virtud del artículo 18.4 ante una resolución de la AEPD cabe interponer un recurso contencioso-administrativo del que dependiendo de la entidad de los hechos será competente un Tribunal Superior de Justicia autonómico o la Audiencia Nacional, y ante la sentencia de estos Tribunales podrá interponerse recurso ante el Supremo. En el transcurso del proceso ante cualquiera de estos Tribunales puede interponerse, por parte de los litigantes o de los Magistrados, una cuestión ante el TJUE para que interprete la normativa Europea que sea de aplicación, como viene regulado en el artículo 267 del Tratado de la Unión Europea.

[65] Artículo 17: "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes…"

[66] El artículo 12.b) de la Directiva únicamente se refería a la supresión de datos cuyo tratamiento no se ajustase a las disposiciones de la misma.

[67] El artículo 18 de la LOPD establece que las actuaciones contrarias a dicha ley pueden ser objeto de reclamación ante la AEPD.

Finalmente, es posible acudir al Tribunal Constitucional en amparo, puesto que el derecho a la protección de datos se encuentra entre los denominados derechos fundamentales[68], que son los que gozan de la cobertura del recurso de amparo. Si bien es cierto que, al igual que ocurre con el resto de derechos que permiten recurrir en amparo, no puede acudirse directamente al TC por una actuación de particulares, debiéndose agotar antes la vía judicial.

[68] No otra cosa puede deducirse del hecho de que el precepto que da origen a este derecho, el artículo 18.4, se encuentre en la Sección 1ª del Capítulo II del Título I, a la que hace referencia el artículo 53.2 CE al delimitar el ámbito del recurso de amparo.

3.- Regulaciónen nuestro ordenamiento siguiendo un criterio cronológico

A) Europa: la Directiva 95/46

Origen de la Directiva

En Europa la preocupación por la protección de datos personales aparece a mediados de los setenta. Hasta entonces únicamente dos Estados habían implementado normativa al respecto (Suecia y el *Land* alemán de Hesse). En 1975 se expone en el Parlamento Europeo el informe de un estudio sobre la materia que concluye proponiendo la creación de una Directiva con dos objetivos: proteger los derechos de los ciudadanos y anticiparse a los desequilibrios normativos en las legislaciones de los Estados. Pese a la adopción en 1976 y 1979 de dos Resoluciones, que incluían recomendaciones y la aprobación del informe Bayerl[69] y buscaban agilizar el proceso, las actuaciones se ralentizan y llegan a paralizarse.

El impulso para seguir trabajando en la Directiva viene de la mano de la OCDE y del Consejo de Europa. En 1980 y 1981 emiten, respectivamente, unas Directrices[70] y el Convenio 108. "La Comisión preveía, sin duda, que, una vez ratificado el Convenio (108 del Consejo de Europa) por todos los Estados miembros, la Directiva sería innecesaria"[71], por lo que decidió esperar y emitir una Recomendación instando a los Estados miembros a firmar el Convenio. Por otro lado el Parlamento manifestaba su inquietud de que esto no fuese suficiente. Finalmente, tras la Conferencia de Autoridades de Protección de Datos celebrada en Berlín en 1989, la Comisión acoge la propuesta francesa de armonización de legislaciones en esta materia, y en 1990 presenta la Propuesta de Directiva del Consejo sobre la aproximación de determinadas disposiciones legislativas, reglamentarias y administrativas de los Estados miembros relativas a la protección de las personas con respecto al tratamiento de los datos de carácter personal.

---

[69] Emitido por la subcomisión de Informática y derechos de la persona, creada *ad hoc* para la elaboración del informe y cuyo relator fue Alfons Bayerl. Junto a las Recomendaciones, el informe recoge las materias que serían tratadas posteriormente en la Directiva.

[70] Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Con estas Directrices se quería salvaguardar tanto la protección de datos personales como el libre flujo transfronterizo de los mismos.

[71] **Heredero Higueras, Manuel. 1997.** *La Directiva Comunitaria de Protección de los Datos de Carácter Personal.* Pamplona : Aranzadi, S.A., 1997. Pág. 22.

"La propuesta de Directiva […] se concibe, desde un primer momento, no como un texto de protección de los derechos y libertades, sino como un medio de aproximar legislaciones con miras a facilitar la plena realización del mercado único"[72], ocupando la protección de derechos un lugar secundario; esto se manifiesta en los considerandos 5º, 7º y 8º, así como en el artículo 1, que supedita la protección de datos a la libre circulación de los mismos entre los Estados miembros. Tras cinco años de negociaciones, en octubre de 1995 se aprueba el texto definitivo de la Directiva.

La Directiva sigue la estructura de las Directrices de la OCDE y del Convenio 108, al igual que hacen la LORTAD y la LOPD españolas.Una glosa del contenido de la misma se circunscribe a los siguientes aspectos.

Disposiciones y principios generales

El Capítulo I contiene disposiciones generales para la aplicación de la Directiva. Concretamente, regula el objeto de su aplicación (la protección de los datos personales y la libertad de circulación de los mismos); su ámbito, a diferenciade la LORTAD, incluye tanto ficheros automatizados como no automatizados, puesto que el daño también puede provenir de estos últimos y su exclusión facilitaría el incumplimiento de la Directiva; las normas de determinación del derecho aplicable, no muy usadas dado que hasta la Directiva las normativas estatales en esta materia no estaban muy desarrolladas; y una serie de definiciones para facilitar la aplicación de la Directiva. Destacan el concepto de datos protegidos, que deben ser del ámbito personal y pertenecer a un sujeto identificado o identificable que además sea una persona física, y el de tratamiento, que abarca desde la recogida de los datos hasta su destrucción, pasando por todo tipo de modificaciones y comunicaciones.

El Capítulo II regula los principios generales del derecho a la protección de datos, lo que se traduce en especificar las condiciones de licitud e ilicitud del tratamiento. Se parte del modelo alemán, según el cual el tratamiento está prohibido en principio (*Verbotsprinzip*), pero puede ser lícito (*zulässig*) si se cumple una condición de las enumeradas, que esencialmente se resumen en dos: el consentimiento expreso o tácito

[72] Ibídem, pág. 27.

del afectado[73] o la existencia de un interés legítimo y preponderante. Si el tratamiento es lícito, debe llevarse a cabo conforme al principio de calidad o finalidad fijado en el artículo 6: los datos deben recogerse con un fin lícito determinado, de forma adecuada y no excesiva, atendiendo a la veracidad, y no deben conservarse por más tiempo del necesario para la realización de la finalidad para la que fueron recogidos. Aunque se cumplan estas condiciones, el artículo 8 prevé la existencia de unos datos sensibles para los que deben cumplirse condiciones adicionales. Estos datos sensibles serían el origen racial, las creencias religiosas, filosóficas y políticas, y la orientación sexual, y las condiciones para su tratamiento serían el consentimiento, en este caso únicamente expreso[74], del afectado, y la existencia de intereses reforzados, como el denominado interés vital, de entre los que destaca la necesidad de tratar datos sobre la salud con fines médicos. El último principio general es el de la conciliación del derecho a la protección de datos y del derecho a la libertad de expresión en los casos de publicaciones periodísticas y literarias.

Con respecto a la licitud del tratamiento de datos, el Capítulo IV, referente al movimiento internacional de datos, realiza interesantes precisiones. Siguiendo el mismo fundamento (*Verbotzprinzip*), la transmisión de datos a terceros países es ilícita en principio, debiendo darse unas circunstancias para hacerla lícita. Estas circunstancias son dos: o bien que el país garantice una protección de datos adecuada (artículo 25.1)[75], o bien que el país no garantice dicha protección pero sí lo haga el responsable del tratamiento (artículo 26.2), en cuyo caso deberá informarse a la Comisión y a los demás Estados miembros. El artículo 26.1 contiene más excepciones a la garantía de protección, basadas en el consentimiento del afectado y en la salvaguarda de intereses públicos o vitales.

Derechos de los interesados

Los siguientes preceptos, aunque se encuentren en el capítulo de los principios generales, contemplan derechos concretos de los afectados.

[73] Piénsese, como ejemplo de consentimiento tácito, en la firma de un contrato para cuyo cumplimiento es imperativo el tratamiento de datos del firmante. El consentimiento tácito no es una condición abierta para la licitud del tratamiento, sino que debe tratarse de supuestos tasados legalmente.
[74] Si bien el apartado 2.e) permite tratar datos sensibles que el interesado haya hecho manifiestamente públicos, lo que podría discutirse que es un supuesto de consentimiento tácito.
[75] El nivel de protección adecuado será el que establece la Directiva. Esto en principio no supone problemas en la transmisión de datos entre Estados miembros, porque en aplicación de la Directiva todos tendrán una protección equivalente. Así se indica en el Considerando 9º.

Se trata de los derechos básicos de la protección de datos: el derecho del afectado a ser informado, al obtenerse sus datos, de la existencia de un fichero al que se enviarán los mismos y de la identidad del responsable del tratamiento; el derecho de acceso a dichos datos (habeas data); el derecho a oponerse al tratamiento cuando se arguya interés público o del responsable del tratamiento; y el derecho a oponerse a decisiones tomadas a consecuencia de un tratamiento de datos personales destinado a analizar su personalidad. También se regulan las obligaciones del responsable del tratamiento: está sujeto al deber de secreto y debe notificar la realización del tratamiento a una autoridad de control, que se encargará de verificar la licitud del mismo. Finalmente, el artículo 13 contiene supuestos en los que los Estados pueden limitar los derechos de información, acceso, rectificación y cancelación, concretamente para la salvaguarda de la seguridad pública, de la economía del país, y de los derechos de otras personas.

Sistemas de control del cumplimiento de la normativa

Para facilitar el cumplimiento de los principios y derechos de protección de datos la Directiva conmina a la creación de códigos de conducta sectoriales, si bien no especifica la aplicabilidad que deben tener.

El Capítulo III, de solo tres artículos, únicamente prescribe que los Estados desarrollen un sistema de recursos ante autoridades de control y tribunales, que regule las sanciones y la responsabilidad de los responsables del tratamiento de datos.

La Directiva dedica el Capítulo VIa encomendar a los Estados la creación de autoridades de control que vigilen la aplicación de la normativa de protección de datos. Dada la disparidad de criterios de los Estados miembros[76], la Directiva permite que existan varias autoridades de control en cada uno. Por lo demás, se remite a los Estados para que creen normas otorgando a las autoridades las potestades necesarias para controlar el cumplimiento de la normativa en esta materia.

Además de las autoridades de control estatales, la Directiva dispone la creación de un Grupo para la Protección de Personas en lo que respeta al Tratamiento de Datos

[76] Por ejemplo, mientras que en Francia únicamente existe el CNIL(Comisión Nacional de la Informática y las Libertades), en Alemania hay Agencias de protección de datos en distintas instancias.

Personales (de aquí en adelante, GPDP), y de un Comité encargado de revisar las medidas ejecutivas dictadas por la Comisión.

El GPDP es un órgano independiente de carácter consultivo, formado por representantes de las autoridades estatales de protección de datos, de las autoridades comunitarias de la misma materia, y de la Comisión. Su función es emitir dictámenes y recomendaciones que no tienen efectos salvo que sean aprobados antes por la Comisión.

Entrada en vigor

Finalmente, en las disposiciones finales de los artículos 32 a 34 la Directiva establece un plazo general de 3 años para la adopción por los Estados de medidas legales y reglamentarias que apliquen la normativa, plazo que se extiende a los doce años en lo que se refiere a los ficheros manuales (no automatizados) de datos. También se dispone que la Comisión emita informes periódicamente sobre la aplicación de la Directiva.

B) España: la LORTAD, la LOPD y sus Reglamentos de desarrollo

Origen de las leyes de protección de datos españolas

La rapidez con la que avanzan las tecnologías, que hace que quede desfasada la regulación, implica que la misma debe poder ser modificada con relativa facilidad, y de ahí que se lleve a cabo mediante Reglamentos y Leyes, así como normas infralegales dictadas por la AEPD, que desarrollen normas más "pesadas" o "lentas" como son la Constitución y la normativa Comunitaria.

La aprobación de la LORTAD fue fruto de las presiones recibidas por la normativa europea de protección de datos. En primer lugar, el Convenio 108 del Consejo de Europa, ratificado por España en 1984, entró en vigor el 1 de octubre de 1985, y en su artículo 4 establecía que las partes firmantes debían incorporar a su derecho interno las medidas necesarias para su correcta aplicación. A pesar de algunos esfuerzos para llevar esto a cabo[77], España incumplió esta obligación. En segundo lugar, al compromiso contraído con el Convenio 108 se añadió el que se iba a contraer en virtud de los Acuerdos de Schengen, así como la presión moral ante el comienzo de la elaboración de

[77] Cabe citar, en materia legislativa, el Anteproyecto de Ley Orgánica de Regulación del Uso de la Informática para la Protección de Datos Personales (1984), y las proposiciones de Ley de Coalición Popular (1987) y IU-IC (1988)

la Directiva 95/46. Los Acuerdos de Schengen obligaban a los Estados firmantes a crear una normativa interna que garantizase un nivel de protección como mínimo equivalente al del Convenio 108[78].

De esta Ley hay que destacar, como contraposición a la LOPD, su exposición de hechos; básicamente porque en la segunda no hay tal exposición de hechos, por lo que la doctrina y los tribunales acuden a la de la primera cuando es necesario. Por lo demás la LORTAD se vio sustituida completamente por su sucesora, que amplió el número de artículos y los desarrolló un poco más.

La Directiva 95/46 daba un plazo de tres años para que los países miembros adoptasen las disposiciones normativas necesarias para su aplicación, lo que en nuestro país se pretendía hacer mediante una modificación de la Ley vigente. Sin embargo, al final se optó por la redacción de una nueva Ley, la LOPD, muy similar a la anterior en su articulado pero que aportaba algunas novedades.

La estructura de ambas Leyes es la misma:

Disposiciones generales

En primer lugar el Título I sienta las disposiciones generales de la norma: su objeto, su ámbito y la definición de conceptos cuya concreción es necesaria para aplicar la Ley. Es de destacar que mientras que la LORTAD centraba su objeto en la protección del derecho al honor y la intimidad, la LOPD deja estos derechos un poco apartados y se centra en el tratamiento de datos personales y en las libertades públicas y derechos fundamentales en general. El ámbito de aplicación también varía, pues mientras que la primera ley se aplica a los datos contenidos en ficheros automatizados, la segunda se refiere a todos los datos que sean susceptibles de tratamiento[79]. Respecto a las definiciones, la LOPD añade el concepto de encargado del tratamiento[80],

[78] Sobre los antecedentes a la aprobación de la LORTAD, ver **Heredero Higueras, Manuel. 1996.***La Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentario y textos.* Madrid : Editorial Tecnos, 1996. Págs. 20-24

[79] El tratamiento de datos viene definido en ambas leyes como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

[80] "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento."

distinguiéndolo del responsable del fichero/tratamiento[81], algo que será importante a la hora de fijar las infracciones y sanciones.

Principios y derechos de protección de datos

Los Títulos II y III forman la parte más importante de la ley, sentando los principios de la protección de datos y regulando los derechos de los ciudadanos al respecto. Tal y como se vio en el apartado anterior, los principios son: veracidad, pertinencia, finalidad, seguridad, consentimiento y almacenamiento limitado de datos personales; y los derechos: información, oposición, acceso (habeas data) y rectificación y cancelación. La LOPD altera dos preceptos respecto a su predecesora: el artículo 12 regula el acceso a datos personales por parte de una persona ajena, sin considerarlo como una transmisión o comunicación de datos, con dos condiciones: que dicho acceso corresponda únicamente a la finalidad de prestar un servicio al responsable del fichero, y que dicho servicio conste en un contrato expreso; además, en el artículo 13, relativo a la impugnación de decisiones basadas en información extraída de datos personales referentes a la personalidad del afectado, se distingue el derecho a no ser objeto de dicha decisión de la propia posibilidad de impugnación. Finamente se añade un artículo, el 19, que regula un derecho a indemnización por incumplimiento de la ley; este derecho lo incluía la Directiva en el apartado de sanciones.

El artículo 13 de la Directiva 95/46, relativo a la limitación de los derechos de información, acceso, rectificación y cancelación, se traspone en la LOPD en el apartado siguiente, puesto que las limitaciones se producen cuando el tratamiento lo realiza una Administración Pública. Los supuestos no varían: se trata de hacer prevaler la defensa del Estado, la protección de la economía y los derechos de otras personas. Sí se añade como excepción a estos derechos el supuesto de que dificulten la actividad de control de las Administraciones Públicas, si bien este precepto es suprimido por el TC[82].

Ficheros y transmisión internacional de datos

El Título IV contiene normas sobre la creación, modificación y supresión de ficheros, distinguiendo los de carácter público de los de carácter privado, y desarrollando varios

[81] "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento."
[82] STC 292/2000, vid. infra en este mismo epígrafe.

supuestos concretos, entre otros los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado (públicos), los de empresas de telecomunicaciones, y los de información relativa a situaciones patrimoniales y de solvencia (privados). Uno de los supuestos es el de los Códigos Tipo, que son conjuntos de reglas elaborados por responsables de ficheros agrupados para, dentro del marco de la LOPD, organizarse de forma homogénea.

El Título V se compone únicamente de dos artículos. El 33 proscribe la transmisión de datos a otros países si no cumplen los estándares de protección del nuestro; a diferencia de lo que se hacía en la LORTAD, este precepto contiene criterios para evaluar y comparar los niveles de protección de los países. El 34 contiene una serie de excepciones a lo anterior, doblando en número a las que regulaba la ley anterior; es decir, la LOPD es más permisiva con la transmisión internacional de datos. Entre las nuevas excepciones destaca la del apartado k), que hace referencia a la transmisión de datos entre países miembros de la UE, en el marco de aplicación por tanto de la Directiva 95/46 (hoy derogada por el RGPD).

Sistemas de cumplimiento de la ley

El Título VI contiene la regulación básica de la AEPD[83]. Sus funciones, ampliadas con la LOPD, consisten básicamente en controlar la aplicación de esta Ley y conocer de los recursos en vía administrativa por incumplimiento de la misma. La Agencia está compuesta por el Director, que la representa y dirige, el Consejo Consultivo, que asesora al Director, y el Registro General de Protección de Datos, en el que se inscriben los ficheros, tanto de titularidad pública como privada. La Ley hace hincapié en la independencia del Director, que en principio no recibe instrucciones de nadie, aunque es inevitable que surja polémica del hecho de que sea nombrado por el Gobierno

El último Título se refiere a las infracciones y sanciones, y desarrolla el Capítulo III de la Directiva 95/46. Se distinguen tres tipos de infracciones: leves, con multas de entre 900 y 40.000 euros, graves, con multas de entre 40.001 y 300.000 euros, y muy graves, con multas de entre 301.000 y 600.000 euros. La prescripción de las infracciones también varía según el tipo. Además, se prevé la inmovilización de los ficheros que incumplan grave o muy gravemente la Ley en tanto no cesen en su conducto.

[83] Regulación básica en tanto que es desarrollada por el Reglamento de desarrollo de la Ley y por el Estatuto de la Agencia.

Finalmente, respecto de los ficheros de titularidad pública, la LOPDse remite al régimen disciplinario de las Administraciones Públicas.

Para terminar de analizar la norma central en materia de protección de datos en España hay que fijarse en las SSTC 290/2000 y 292/2000. La primera es un curioso caso en el que el TC debe pronunciarse sobre la constitucionalidad de varios artículos de la LORTAD cuando en el momento de la sentencia la Ley ya había quedado derogada. Concretamente, el Tribunal considera que es el Estado el que debe encargarse de la protección del derecho a la autodeterminación informativa, teniendo las Comunidades Autónomas únicamente potestad de desarrollo.

Actuación del TC

Por otro lado, la STC 292/2000 declara inconstitucionales dos preceptos de la LOPD. El primero de ellos es un inciso del artículo 21 que permitía la transmisión de datos entre Administraciones Públicas cuando estuviese previsto en las disposiciones de creación del fichero, es decir, en normas de rango infra-legal. Resulta evidente que la argumentación que llevó a este fallo es la remisión de la ley a normas inferiores, cuando el artículo 18.4 de la Constitución especifica que su desarrollo debe llevarse a cabo por Ley, y más aún por cuanto la norma anulada pretendía dejar al arbitrio de la Administración encargada de dictar la disposición en cuestión la decisión de qué datos transmitir a otras Administraciones (sin el consentimiento del afectado). El otro precepto anulado se encuentra en el artículo 24, que regula excepciones a los derechos de los afectados. Concretamente son dos los preceptos anulados en este artículo: el primero permitía a las Administraciones Públicas omitir el deber de información recogido en el artículo 5 por razones de interés público, lo que prácticamente equivaldría a hacer que el afectado desconozca que se están almacenando sus datos, algo que a todas luces va en contra del derecho a la autodeterminación informativa, incluso habiendo razones de interés público de por medio; el segundo otorgaba a las Administraciones Públicas la potestad de denegar los derechos de acceso, rectificación y cancelación, también por razones de interés público[84].

[84] El texto anulado imponía a la Administración, con tintes burlescos, la obligación de informar al afectado de su derecho a "poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.", en una clara manifestación del principio administrativo *solve et repete* y del tópico decimonónico "vuelva usted mañana".

C) Europa: el Reglamento 679/2016

Origen y relación con la Directiva y la LOPD

Tras más de cuatro años trabajando sobre el texto propuesto por la Comisión, el 27 de abril de 2016 se aprobó el nuevo Reglamento 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. La finalidad de este Reglamento ha sido la de actualizar y modernizar los principios de la Directiva de protección de datos de 1995 en varios aspectos fundamentales.

No carece de importancia mencionar, en primer lugar, que este Reglamento sustituye y por ello deroga a la Directiva de Protección de Datos. Según se establece en las disposiciones finales, "Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento" (artículo 94.2 del RGPD). Por otro lado, se ha seguido una fórmula compleja para determinar la entrada en vigor y aplicación de esta norma: la entrada en vigor se ha producido el 25 de mayo de 2016, 20 días después de su publicación en el DOUE, pero pese a ello no será aplicable hasta el 25 de mayo de 2018, 2 años más tarde. Es lógico el margen de dos años de preparación que se da antes de empezar a aplicar el Reglamento, pero no se entiende que haya entrado en vigor un mes después de su publicación, puesto que ello solo genera dudas y no aporta nada.

Esto puede dar lugar a problemas a la hora de saber a qué norma atenerse, por ejemplo, por parte de las empresas e instituciones que tratan datos personales en el transcurso de sus actividades diarias.

Para evitar estos problemas, la AEPD ha emitido una nota de prensa en forma de 12 preguntas y respuestas para aclarar la situación. Según la Agencia, y haciendo una interpretación muy lógica del artículo 99 del RGPD, la Directiva 95/46 se seguirá aplicando hasta el 25 de mayo de 2018, momento a partir del cual quedará definitivamente sin efecto. "El periodo de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones Europeas y también las organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable […] En general, las organizaciones que tratan datos personales deberían comenzar a preparar la aplicación de estas medidas[…]La ventaja de una pronta aplicación es que permitirá detectar

dificultades, insuficiencias o errores en una etapa en que estas medidas no son obligatorias y, en consecuencia, su corrección o eficacia no estarían sometidas a supervisión. Ello permitiría corregir errores para el momento en que el Reglamento sea de aplicación."[85] Debe hacerse mención a la encomiable labor que la Agencia está llevando a cabo tanto para la concienciación de la población por la protección de sus datos como por el acercamiento al nuevo Reglamento.

Respecto a la LOPD, en principio podrá seguir aplicándose una vez derogada la Directiva. Ahora bien, hay que tener en cuenta que esta Ley fue elaborada para incorporar la Directiva a nuestro ordenamiento, y puede no coincidir con el nuevo Reglamento, que según se afirma en la última frase del texto "será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". Un ejemplo de contradicción entre la Ley y el Reglamento se encuentra en el artículo 1 de ambas normas, referido al objeto de aplicación: mientras que la primera habla de "garantizar y proteger […]especialmente [el] honor e intimidad personal y familiar", el segundo hace referencia a la defensa, "en particular, [del] derecho a la protección de datos personales"; matiz importante en lo que a este Trabajo se refiere, puesto que prueba la superación del debate intimidad-protección de datos como derechos fundamentales.

Centrándonos en las consecuencias de desavenencias como éstas, debe hacerse una breve mención a la problemática de la contradicción entre normas europeas y estatales; que por otro lado es un tema que daría suficiente para realizar otro Trabajo. Se trata de un debate también superado, en parte gracias a jurisprudencia ya antigua como las SSTJUE *Simmenthal*, *Vand Gend en Loos* y *Costa contra ENEL*, en parte gracias a argumentaciones como la esgrimida por nuestro TC en su Declaración del Pleno del Tribunal Constitucional 1/2004, de 13 de diciembre de 2004.[86] En resumen, la **supremacía** de la Constitución sobre el ordenamiento estatal no es incompatible con la **primacía** del derecho europeo en los ámbitos relativos a competencias cedidas en base al artículo 93 CE[87]. Así pues, las normas europeas se aplican con preferencia sobre las estatales, y el RGPD hará inaplicable los preceptos de la LOPD en cuanto se opongan a

[85] Extracto de la nota de prensa de la AEPD, publicada en su página web el 26 de mayo de 2016: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php (fecha de último acceso: 8 de junio de 2016).

[86] Esta Declaración tuvo lugar fruto del requerimiento formulado por el Gobierno acerca de la constitucionalidad de varios artículos del Tratado por el que se establece una Constitución para Europa, firmado en Roma el 29 de octubre de 2004.

[87] FJ 4º de la citada Declaración.

él. Esto muestra uno de los problemas que presenta el ordenamiento europeo en general: los textos normativos están bien hechos, pero suelen presentar problemas para llevarlos a la práctica; a la cuestión de las competencias estatales frente a las comunitarias hay que añadir lo complejo de los Reglamentos y Directivas, que deben poner de acuerdo a todos los Estados miembros en detrimento de su efectividad.

La estructura de la nueva norma reguladora del derecho a la protección de datos sigue siendo la de la Directiva y la del Convenio 108: se empieza situando el ámbito de aplicación y definiendo conceptos, a continuación se encuentran los principios generales de la protección de datos, los derechos concretos de los interesados y las limitaciones a los mismos, y tras regular las transferencias internacionales de datos se pasa a establecer una suerte de régimen sancionador y de responsabilidades. Además se añaden contenidos nuevos, como la figura del Delegado de Protección de Datos (DPO, por sus siglas en inglés), la cooperación entre autoridades de control y las situaciones específicas de tratamiento.

Disposiciones generales y ámbito de aplicación

De la primera parte del Reglamento hay que destacar las diferencias con la Directiva. La primera, ya mencionada, es la concepción de la protección de datos como un derecho fundamental, algo que se menciona en el artículo 1 y en el considerando 1º[88].

Otra diferencia importante se encuentra en el nuevo ámbito territorial: el artículo 3 del RGPD prescribe su aplicación fuera de la Unión cuando el tratamiento de datos se lleve a cabo en el contexto de una oferta de bienes y servicios a residentes de la Unión, o bien cuando el tratamiento tenga por objeto el control del comportamiento de dichos ciudadanos. Este cambio podría explicarse por la desconfianza actual de las instituciones europeas hacia Estados Unidos en dos sentidos: en primer lugar, los juristas del país norteamericano y los de la Unión Europea llevan tiempo discutiendo sobre cuál de los sistemas de protección de datos es mejor, el europeo o el americano, y por ello hay una mutua desconfianza en el tratamiento de los datos propios por parte del otro, lo que se traduce en querer aplicar la normativa propia incluso cuando los datos

[88] "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental"

sean tratados desde fuera[89]. En segundo lugar, "los documentos filtrados por Snowden dejan claro que los mecanismos que debían proteger la información de las empresas estadounidenses del conocimiento por parte de agencias de seguridad nacional han sido atravesados, si no completamente destruidos. Estas revelaciones han servido para alimentar las ya existentes preocupaciones de la Unión Europea sobre el fácil acceso de las agencias de inteligencia de Estados Unidos a la información de los gigantes de internet como Google, Facebook, Microsoft y otros"[90]; es decir, a consecuencia de las filtraciones de Edward Snowden en 2013, si bien esta preocupación ya existía antes, las instituciones europeas consideran que los datos personales no se encuentran seguros estando al alcance de las agencias de seguridad americanas.

Además del cambio en el ámbito territorial de aplicación, el RGPD añade nuevas definiciones a la tradicional lista de datos personales, ficheros, tratamiento, responsable… Algunos ejemplos con la elaboración de perfiles, que antes solo aparecía de forma casi indirecta en el articulado, la seudonimización, que facilita el tratamiento de datos, y el tratamiento transfronterizo, referido al tratamiento de datos llevado a cabo en varios Estados miembros.

Principios del tratamiento de datos. Licitud

El Capítulo II, referido a los principios del tratamiento de datos, además de contemplar los mismos de la Directiva (licitud, lealtad, exactitud, limitación del tiempo de conservación…) añade otros nuevos: la integridad y confidencialidad en el mantenimiento de los datos[91] y la responsabilidad proactiva. Si bien en la Directiva ya

[89] David Vladek, ex director de la Oficina de Protección de Consumidores de la Comisión Federal de Comercio (el órgano estadounidense encargado de proteger a los consumidores de las compañías, entre otras cosas, en supuestos de invasión de privacidad) resume en un artículo algunas diferencias entre el sistema americano y el Europeo. En síntesis, el modelo americano carece de una concepción del derecho a la protección de datos, y regula la privacidad en forma de normativas sectoriales, pero permite que los controles del cumplimiento de dichas normas sean más ágiles; por otro lado, el modelo europeo regula un alto nivel de protección de los datos personales cada vez más unificado, pero el régimen legal de protección (que Vladek denomina "*privacy on the books*") no se llega a aplicar realmente a la privacidad de los ciudadanos (que Vladek llama "*privacy on the ground*"). El artículo se encuentra en **Vladek, David.** Separated by common goals: A U.S: Perspective on narrowing the U.S.-EU privacy divide. [aut. libro] Artemi Rallo Lombarte y Rosario García Mahamut. *Hacia un nuevo derecho europeo de protección de datos*. Valencia : Tirant lo Blanch, 2015.

[90] *Ibídem*, página 208.

[91] Artículo 5.1.f): "de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental"

se encontraba el contenido de este último principio[92], ahora cobra una importancia que se refleja en la mención expresa del principio y su desarrollo en el Capítulo IV (que se verá un poco más adelante).

Sobre las causas que hacen lícito el tratamiento, se mantienen las condiciones de la Directiva con varias modificaciones. En primer lugar, el consentimiento otorgado para el tratamiento debe serlo para una finalidad determinada. Además, el tratamiento en base a una misión de interés público o al cumplimiento de una obligación legal del responsable requiere desarrollo previo por parte del Estado en cuestión o de la Unión. Finalmente, se enumeran varios criterios a tener en cuenta a la hora de decidir si la finalidad inicial del tratamiento es compatible con otra finalidad sobrevenida.

Respecto del consentimiento, el RGPD añade los artículos 7 y 8 con vistas a que sea tenido más en cuenta por los responsables y encargados de los tratamientos. El primero delimita las condiciones que debe cumplir: llegado el caso recae sobre el responsable la obligación de probar el consentimiento, que además puede ser retirado en cualquier momento con la misma facilidad con la que se otorgó, y para evitar los problemas que surgen en la práctica a la hora de recabarlo debe poder distinguirse fácilmente del otorgado simultáneamente para otros asuntos, debiéndose considerar que no se ha hecho de forma libre si estaba supeditada a él la validez de un contrato. El segundo establece como edad mínima para otorgar el consentimiento válidamente los 16 años, aunque los Estados pueden optar por una edad menor que sea al menos de 13 años[93]. La especial y novedosa incisión que se hace sobre el consentimiento de los interesados pone de manifiesto los subterfugios llevados a cabo por muchos tratantes de datos al respecto, como entender el consentimiento tácito si no se decía otra cosa, o escondiéndolo en forma de la típica "letra pequeña".

En cuanto a los datos de especial protección (convicciones políticas, filosóficas, religiosas, salud, vida sexual…) la regulación apenas varía respecto de la anterior: se requiere el consentimiento expreso para tratar estos datos, o bien que se den

[92] Artículo 6.2 (coincidente con el 5.2 del Reglamento salvo en el nombre que éste da al principio): "Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1". Dicho apartado contiene los principios aplicables al tratamiento de datos personales.

[93] La AEPD, en un informe jurídico del año 2000, ya contemplaba la edad mínima para otorgar el consentimiento en materia de datos personales en 14 años: "será necesario recabar el consentimiento de los menores para la recogida de sus datos[…], recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales."

circunstancias específicas más cualificadas que para el tratamiento de datos normales, debiéndose regular específicamente por los Estados o la Unión el tratamiento de datos relativos a responsabilidad penal.

Derechos de los interesados

El Capítulo III sobre los derechos del interesado comienza dedicándole un artículo a la transparencia, fenómeno muy reciente en nuestro país[94] pero que ya ha recorrido mucho camino en otros[95]. Este artículo busca facilitar el acceso de los interesados a la información que se detalla en los preceptos siguientes, y también que ésta sea más clara y fácil de entender.

El derecho de los interesados a la información consiste en darles a conocer, en el momento de obtener los datos, quién es el que va a realizar el tratamiento, con qué finalidad, y, como novedad en el Reglamento, con qué base jurídica, así como quién es el DPO con el que tendría que ponerse en contacto llegado el caso. También de los derechos que tiene el interesado a solicitar el acceso, limitación, oposición… Todo ello tanto si los datos se obtienen del interesado, como si se obtienen de un tercero, en cuyo caso se deberá informar de la fuente de la que se han obtenido los datos. El derecho de acceso contemplado en el artículo 15 en realidad no añade nada al derecho de información, más que la facultad del interesado de solicitar esa información en cualquier momento y de solicitar una copia de los datos registrados.

El artículo 17 añade una importante novedad: el derecho de supresión, conocido como "derecho al olvido". En síntesis, supone la facultad de solicitar la eliminación de datos personales en internet cuando los motivos que llevaron a publicarlos ahí han desaparecido[96].

[94] La Ley de Transparencia, Acceso a la información Pública y Buen gobierno fue aprobada en diciembre de 2013 y entró en vigor un año más tarde. Ocupa una posición intermedia-baja (puesto 71 de 103) en el ranking elaborado por la asociación canadiense *Centre forLaw and Democracy*, que puede encontrarse aquí: https://www.rti-rating.org/country-data (visitado el 11 de junio de 2016). Las Comunidades Autónomas han ido aprobando sus propias leyes de transparencia; la de Castilla y León, por ejemplo, es de marzo de 2015.

[95] La normativa de transparencia es en ocasiones tan antigua como la Ley de Libertad de Prensa sueca de 1766, y en otras tan moderna como la Ley Federal de acceso a la información del Gobierno alemana de 2005, pasando por las leyes francesa, holandesa (ambas de 1978), italiana (1990), portuguesa (1993) y británica (2000).

[96] Sobre el derecho al olvido en este Trabajo, ver Capítulo II, apartado 2.-, epígrafe C).

El derecho a la limitación del tratamiento del artículo 18, también nuevo, es una herramienta que sirve para hacer aplicables otras disposiciones; por ejemplo, cuando se impugne la exactitud de unos datos se puede solicitar la limitación del tratamiento hasta que se decida sobre dicha exactitud, o si el tratamiento no es lícito pero el interesado no desea que se supriman los datos, en cuyo caso podrá solicitar la limitación. La limitación supone que el único tratamiento que se podrá llevar a cabo sin permiso previo del interesado será para conservar los datos.

En el artículo 20 se regula un derecho a la portabilidad de los datos, esto es, a la transmisión de datos personales por parte de un responsable a otro responsable elegido por el interesado. La limitación de este derecho a los supuestos en los que la base jurídica para el tratamiento de los datos es el consentimiento del interesado o el cumplimiento de un contrato no parece ser de mucha utilidad, puesto que limita el derecho del interesado a que los datos sean transmitidos siempre que quiera; algo que, en cualquier caso, podría hacer por sí mismo solicitando primero los datos y transmitiéndolos después, por lo que las limitaciones de la portabilidad solo consiguen que se tenga que tomar un camino más largo.

Las limitaciones impuestas por el RGPD a los derechos de los interesados contemplan un mayor número de supuestos que en la Directiva, es decir, se pueden limitar con mayor frecuencia, pero también se ha añadido la obligación de la limitación de que "respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada".

Responsables y encargados. Responsabilidad proactiva

El Capítulo IV del Reglamento regula lo relativo a los responsables y encargados del tratamiento de datos. Lo que se busca con estos artículos es la responsabilidad proactiva de estos sujetos, que no deben esperar a las solicitudes de los interesados para preocuparse de la protección de datos, sino que deben tomar medidas al respecto "de oficio". Este objetivo se resume en el primer párrafo del artículo 24: "el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento". El artículo 25, llamado "Protección de datos desde el diseño y por defecto", también apunta en esta dirección. Estas nuevas responsabilidades de los responsables y

encargados del tratamiento de datos se concretan en dos nuevos mecanismos: en primer lugar, se crean una serie de obligaciones que van más allá de atender las peticiones de los interesados respecto de sus datos, y que incluyen la seudonimización y cifrado de datos, la confidencialidad y disponibilidad de los mismos, las evaluaciones periódicas de las medidas técnicas de protección, y la notificación obligatoria al interesado y a la autoridad de control cuando se produzca una violación en la seguridad. En segundo lugar, cuando un tratamiento conlleve un alto riesgo para los derechos y libertades de las personas físicas [97] deberá realizarse una evaluación previa sobre el impacto que tendrá el tratamiento, recabando el asesoramiento del DPO, de forma que la resolución, positiva o negativa, esté motivada. Cuando el resultado de la evaluación muestre que el tratamiento efectivamente entraña un alto riesgo, podrá seguirse adelante pero previa consulta con la autoridad de control.

Por lo demás, el RGPD también detalla la figura del responsable, el corresponsable y el representante del responsable[98], así como del encargado del tratamiento.[99]

Sistemas de control del cumplimiento del Reglamento

La gran novedad en este aspecto es la figura del Delegado de Protección de Datos, intermediario entre la autoridad de control y el responsable del tratamiento. Esta figura será analizada en el apartado siguiente, junto al resto de organismos de protección de datos.

La última parte del Capítulo IV se refiere a los códigos de conducta y a las certificaciones de protección.

[97] En estos términos se expresa el artículo 35, que además concreta en un enumeración no exhaustiva algunas situaciones de alto riesgo: la elaboración de perfiles sobre la cual se tomen decisiones con efectos jurídicos, el tratamiento a gran escala de datos especialmente sensibles (del artículo 9: afiliaciones políticas, religiosas, filosóficas, salud, vida sexual…) y la observación sistemática a gran escala de un espacio público. Además, se encarga a las autoridades de control que elaboren listas de situaciones de riesgo en las que se tenga que llevar a cabo esta evaluación.

[98] Los corresponsables se reparten entre sí las obligaciones del responsable mediante un acuerdo (artículo 26), y el representante del responsable es la figura que lleva a cabo sus funciones en la Unión cuando el responsable está establecido fuera de ella pero corresponde aplicar el Reglamento conforme al artículo 3.2 (artículo 27).

[99] El encargado del tratamiento es una persona elegida por el responsable que ofrece garantías suficientes para aplicar las medidas técnicas necesarias durante el tratamiento. Responde ante el responsable, y no puede delegar sus funciones en nadie sin su consentimiento

Los códigos de conducta son recopilaciones sectoriales parecidas a las que ya regula la LOPD en su artículo 32. El artículo 40 del RGPD encomienda a los Estados, las autoridades de control, el Comité y a Comisión la tarea de promocionar la elaboración de estos códigos por parte de asociaciones o agrupaciones de responsables de tratamiento en lo que respecta al cumplimiento de sus obligaciones, especialmente en sus relaciones con los interesados. El cumplimiento de estos códigos será obligatorio, y se encargará de controlarlo un organismo creado por la autoridad de control a tal fin.

Las certificaciones de protección se concederán por organismos creados para ello a los responsables de tratamiento que ofrezcan y cumplan con las garantías adecuadas. Estas certificaciones (o marcas o sellos) funcionarán únicamente para que el público general tenga un punto de referencia a la hora de saber si confiar en que sus datos van a ser tratados correctamente; pese a no tener efectos jurídicos, el RGPD regula con profusión los mecanismos de creación de organismos de certificación y de concesión de certificaciones. Otro ejemplo más de la excesiva burocratización del ordenamiento europeo, que mejor haría en dedicar esfuerzos en el establecimiento de mecanismos directos de control del flujo de datos que en regular hasta el más mínimo detalle de la estructura y funcionamiento de unos organismos cuya actividad no tiene un efecto directo en el cumplimiento del Reglamento; lo cual no quiere decir que las certificaciones de protección no tengan utilidad, pero sí que el Reglamento les ha dedicado demasiado interés.

La regulación que se hace en el Capítulo VI sobre las autoridades de control obliga, en primer lugar, al establecimiento de una o varias de estas instituciones en cada Estado miembro con la finalidad de supervisar la aplicación del Reglamento. Además, se incide en la independencia con la que deben actuar; por ejemplo deben tener recursos propios y sus miembros están sujetos a un régimen de incompatibilidades. Se regulan una larga serie de competencias y funciones, pero se remite a la legislación de los Estados para lo demás, sentando solo algunos principios generales.

Enlaza con lo anterior el Capítulo VII, titulado Cooperación y Coherencia. Se habla aquí de dos cosas: la coordinación entre autoridades de control, y la institución del Comité Europeo de Protección de Datos (el Comité).

La primera parte desarrolla la forma en que las autoridades de control deben ponerse de acuerdo en sus actuaciones. En líneas generales, las autoridades deben intercambiar entre sí toda la información relativa a sus actuaciones y resoluciones sin dilaciones indebidas. El Comité se encargará de presidir y controlar esta coordinación, y podrá adoptar decisiones vinculantes en los conflictos entre autoridades.

El Comité, como se ha dicho, supervisa el cumplimiento del Reglamento en lo relativo a la actividad de las autoridades de control. Está formado por representantes de las mismas. También asesora a la Comisión.[100]

El Capítulo VIII hace referencia al régimen sancionador del RGPD. Aunque no parece necesario, reconoce el derecho de los interesados a interponer reclamaciones ante autoridades de control, y a ejercitar acciones judiciales contra las resoluciones emanadas de éstas y contra la actuación de los responsables y encargados del tratamiento de datos.

Sí son interesantes los artículos 82 a 84, que contienen normas sobre indemnizaciones y sanciones. Los perjuicios materiales e inmateriales ocasionados por el tratamiento de datos cuando incumpla el Reglamento generarán un derecho a ser indemnizado por los responsables[101] que hayan participado. Más importante que la indemnización por daños, que no deja de estar ya regulada en el derecho civil, es la potestad otorgada a las autoridades de control para la imposición de multas administrativas, lo que las convierte *de facto* en órganos fiscalizadores de la protección de datos personales, de forma que puedan dispensar una defensa adecuada de los interesados sin que haya que recurrir a los tribunales. Las multas pueden llegar a ser de 10 millones de euros o el 2% del volumen de negocio anual de una empresa para infracciones leves, como el incumplimiento de las obligaciones del responsable relativas a la seguridad de los ficheros o de las obligaciones del organismo de certificación relativos a la misma; y de 20 millones o el 4% del volumen de negocio anual de una empresa para infracciones graves para infracciones graves, como no atender a las peticiones de los interesados relativas a sus derechos (acceso, información, rectificación…), incumplir las condiciones del consentimiento, o no respetar el Capítulo sobre transferencias internacionales de datos.

[100] Sobre el Comité, así como los demás organismos de protección de datos, ver el apartado siguiente.
[101] En concreto, de acuerdo a los apartados 4 y 5 del artículo 82 la responsabilidad va a ser solidaria cuando hayan participado varios responsables.

El artículo 83.2 enumera una serie de criterios a tener en cuenta a la hora de imponer las multas, tales como la intencionalidad de la infracción, las medidas tomadas para paliar el daño o el grado de reincidencia del responsable o encargado.

El artículo 84 encomienda a los Estados el establecimiento de otras normas que sancionen el incumplimiento del RGPD de forma distinta a la multa administrativa. Este precepto da pie a considerar un amplio rango de actuaciones, desde la creación de ficheros públicos en los que se recojan los responsables y encargados que incumplan la normativa, hasta la tipificación como delitos penales de las infracciones más graves, con tal de que las sanciones se consideren efectivas, proporcionadas y disuasorias.

Transmisión internacional de datos

El Capítulo V, relativo a las transferencias de datos a terceros países, pone nuevamente de manifiesto la desconfianza de la Unión a que el tratamiento de datos personales se lleve a cabo fuera de su control. Mientras que la Directiva permitía realizar dichas transmisiones siempre que el país receptor ofreciera "un nivel de protección adecuado", dejando esta decisión a la discrecionalidad del responsable[102], el artículo 45 del RGPD establece que para transferir datos personales fuera de la UE la Comisión debe haber decidido previamente que el lugar de destino cumple con las garantías de tratamiento necesarias; entre los criterios a tener en cuenta por la Comisión para evaluar el nivel de protección están el respeto a los derechos humanos, la existencia de autoridades de control, y los compromisos internacionales asumidos en este sentido.

De no existir autorización de la Comisión únicamente se podrán transferir los datos si el nivel de protección adecuado viene respaldado por normas vinculantes de algún tipo, de forma que los interesados cuenten con derechos exigibles y acciones legales efectivas. Finalmente, también se permite la transmisión en situaciones específicas, como cuando se cuente con el consentimiento explícito del interesado, concurran razones de interés público o deban protegerse intereses vitales.

El antepenúltimo Capítulo es una vez más una remisión a los Estados para que elaboren su propia legislación. En concreto, se hace referencia a los siguientes puntos:

[102] Si bien la Comisión podía publicar una lista con los países que no ofrecen dicha garantía, en cuyo caso la transferencia de datos no sería lícita (artículo 25.4 de la Directiva) .

conciliación de la protección de datos con la libertad de expresión e información[103] y con el derecho de acceso a documentos públicos[104], regulación del tratamiento del número nacional de identificación [105] y del tratamiento de datos en el ámbito laboral, y regulación del deber de secreto de los responsables y encargados.

Disposiciones finales

El Capítulo final del RGPD contiene tres disposiciones principales:

En primer lugar deroga la Directiva 95/46.

En segundo lugar se encarga a la Comisión la elaboración de informes cada cuatro años empezando el 25 de mayo de 2020 sobre la evaluación y revisión del presente Reglamento. Dichos informes se presentarán al Parlamento Europeo y al Consejo y se harán públicos.

Finalmente, se determina que será aplicable a partir del 25 de mayo de 2018.

D) España: supuestos concretos

Además de la normativa específica de protección de datos, este derecho aparece referido en otras normas. Algunos ejemplos son los siguientes:

El Código Penal dedica varios preceptos a protección de datos. En general se refieren a ella indirectamente, para la persecución de delitos contra otros bienes jurídicos[106]. Son

[103] Para ello se establecerán excepciones a los preceptos del Reglamento cuando el tratamiento se realice "con fines periodísticos o con fines de expresión académica, artística o literaria" (artículo 85.2).

[104] En el caso de España el acceso a documentos públicos se encuentra actualmente regulado en la Ley de Transparencia y Buen Gobierno, y dentro de ella se hace referencia a los datos personales en el artículo 15. Sobre esta normativa, ver el epígrafe siguiente.

[105] Sobre el DNI ha mantenido la AEPD diversas posiciones. En un principio no lo consideró un dato de carácter personal, como afirma en su Resolución E/00561/2004: "en principio es criterio de esta Agencia Española de Protección de Datos que el número del DNI, por si [sic] solo, no constituye un dato de carácter personal". Sin embargo, a raíz de la aprobación del Real Decreto 1553/2005, de 23 diciembre por el que se regula la expedición del documento nacional de identidad y certificados de firma electrónica del DNI cambia de criterio, y argumenta en su Informe jurídico 0476/2008 que "La naturaleza de dato personal del DNI resulta clara atendiendo a lo anteriormente expuesto"; se refiere a la definición del DNI que da el Real Decreto en su artículo 1.2: "Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo".

[106] Por ejemplo, el artículo 183 ter. tipifica el contacto con menores a través de algún medio tecnológico (para lo cual es necesario conocer algún dato de contacto del menor, es decir, un dato personal) con la finalidad de cometer un delito contra la indemnidad sexual.

dos los que lo hacen directamente: el artículo 197[107] y el 264. El primero contiene un error, y es que tipifica dos veces la actuación no autorizada sobre los datos personales: una vez cuando define el delito en sí en el apartado 2("al que, sin estar autorizado, se apodere, utilice o modifique […] datos reservados de carácter personal…"), y otra cuando se refiere a variantes agravadas en el apartado 4, letra b)(cuando los hechos "se lleven a cabo mediante la utilización no autorizada de datos de la víctima…"); se interprete como se interprete, la versión agravada se aplica cuando la utilización no es lícita, y el delito no existe si el apoderamiento, utilización o modificación son lícitos, por lo que la versión agravada se aplicará siempre. El segundo castiga los daños provocados a los datos informáticos.

La Ley de Transparencia y Buen Gobierno desarrolla, en cierto sentido, la previsión del artículo 105.b) de la Constitución, que reza como sigue: "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". Así, el artículo 12 de la Ley recoge el derecho de todas las personas "a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley". Pues bien, uno de los límites a este derecho de acceso a la información pública es la protección de datos personales, y por ello el artículo 15 establece que cuando la información contuviera datos personales deberá ponderarse el interés público de la información frente al carácter reservado de los datos, y solo podrá darse acceso cuando prevalezca el primero, o bien cuando sea posible la disociación de datos respecto del interesado. Si se trata de datos especialmente protegidos el acceso a la información no podrá tener lugar sin el previo consentimiento del interesado. En la práctica esto va a dar lugar a muchos problemas, puesto que la ponderación al fin y al cabo es dejar a la discreción de la Administración la decisión de permitir el acceso a la información, y es fácil que bien el solicitante de información bien el titular de los datos objeto de la misma están disconformes con la

[107] Se castiga con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses "al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero". Los apartados cuatro y cinco agravan la pena cuando el culpable sea el responsable del tratamiento, cuando el tratamiento de datos sea ilícito, o cuando los datos personales en cuestión pertenezcan a la categoría de sensibles (filiación política, religiosa, salud, vida sexual…).

resolución de la Administración e incluso, posteriormente, con la decisión del Consejo de Transparencia y Buen Gobierno o de sus homólogos autonómicos.

Los artículos 41 y siguientes de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones establecen la obligación de los operadores de redes públicas de comunicaciones electrónicas de tomar las medidas necesarias para garantizar la seguridad de los datos personales a los que tengan acceso durante la prestación de servicios. Se somete la actividad de los operadores en esta materia a la vigilancia de la AEPD.

El artículo 155 de la nueva (aún no ha entrado en vigor)Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público dispone el acceso entre Administraciones a los datos de carácter personal que obren en su poder. Dice este precepto que esto se regula de conformidad con lo dispuesto en la LOPD y su normativa de desarrollo, pero no especifica a qué parte de las mismas. Esta referencia debe entenderse hecha al artículo 21 de la LOPD y al 10.4.c) del Reglamento de desarrollo, según los cuales las Administraciones pueden cederse datos personales entre sí cuando se haga con fines estadísticos, históricos o científicos, cuando los datos se hayan recogido o elaborado expresamente para transmitirlos a otra Administración, o cuando los datos se vayan a usar con la misma finalidad por ambas Administraciones. El apartado 2 del artículo 155 de la Ley del Sector Público lo que hace es limitar un poco más la comunicación de datos personales entre Administraciones, puesto que además de lo regulado en la LOPD requiere que los datos hayan sido solicitados a los interesados para la tramitación de un procedimiento del que sea competente la Administración requerida.

Los artículos 17 y siguientes de la Ley 59/2003, de 19 de diciembre, de firma electrónica se refieren a las obligaciones de los prestadores de servicios de certificación de la firma electrónica respecto de la protección de datos. En general lo que hacen es una reiteración de lo ya regulado en la normativa de protección de datos[108], puesto que solo se permite la recogida de datos con el consentimiento del interesado, y la misma y

[108] De hecho el artículo 17.1 se refiere expresamente a ella: "El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo"

el tratamiento solo podrán hacerse sobre los datos que sean necesarios para la prestación del servicio.

Finalmente, hay otras normas que no elaboran lo establecido por la LOPD y su Reglamento, sino que se remiten a ellos. Por ejemplo, el artículo 16 de la Ley del Procedimiento Administrativo Común de las Administraciones Públicas y el artículo 3 de la Ley del Registro Civil contienen la misma previsión: el funcionamiento de los registros que regulan (los Registros Centrales Electrónicos de las Administraciones y el Registro Civil) se ajustará a las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

4.- Organismos

En este apartado se explican las diversas autoridades de control encargadas de hacer cumplir, sin llegar a los tribunales, la normativa de protección de datos.

A) El SEPD

"El Supervisor Europeo de Protección de Datos (SEPD) es la autoridad de control independiente de la UE responsable de:

- vigilar el tratamiento de datos personales efectuado por las instituciones y los organismos de la UE.
- Asesorar sobre políticas y legislación que afecten a la intimidad.
- Cooperar con autoridades similares a fin de asegurar una protección de los datos coherente."[109]

El SEPD se regula principalmente por los artículos 41 y siguientes del Reglamento 45/2001, salvo lo relativo a su retribución y a su sede, que se encuentran en la Decisión nº 1247/2002 del Parlamento Europeo, del Consejo y de la Comisiónde 1 de julio de 2002relativa al estatuto y a las condiciones generales de ejercicio de las funciones de SupervisorEuropeo de Protección de Datos[110].

La principal característica de este organismo es su independencia: no recibe instrucciones de nadie, y quien ocupe el cargo no puede desempeñar ninguna labor profesional, esté o no retribuida (artículo 44 del Reglamento 45/2001). Otra característica a resaltar es que su competencia se circunscribe a los órganos e instituciones de la Unión Europea, aunque entre sus funciones está la de colaborar con las autoridades de control de datos estatales.

El Supervisor se nombra por periodos de cinco años renovables por el Parlamento Europeo y el Consejo sobre una lista confeccionada por la Comisión, que solo puede estar formada por "personas cuya independencia esté fuera de toda duda y que posean

[109] Esta definición se puede encontrar en la página web del SEPD: (https://secure.edps.europa.eu/EDPSWEB/edps/lang/es/EDPS/cache/offonce); fecha de último acceso: 8 de junio de 2016.

[110]Según esta Orden, el Supervisor y el Supervisor Adjunto recibirán la misma retribución que los Jueces y el Secretario del TJUE. En cuanto a la sede, se encuentra en Bruselas.

una experiencia y competencia notorias para el cumplimiento de las funciones de Supervisor Europeo de Protección de Datos" (art. 42.2 del mismo Reglamento). Estará apoyado por un Supervisor Adjunto nombrado de igual forma y por una Secretaría cuyo personal elegirá el Supervisor.

La actividad del SEPD consiste en la investigación, bien de oficio, bien a instancia de una reclamación, de posibles irregularidades en la actuación de los órganos e instituciones de la Unión Europea en materia de protección de datos; se exceptúa el TJUE en el ejercicio de sus funciones jurisdiccionales. También funciona como órgano asesor de la UE en esta materia, y debe "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;" (artículo 46.e) del Reglamento).

El Supervisor lleva a cabo sus funciones gracias a las potestades que le han sido conferidas: puede hacer propuestas a los organismos y a las instituciones de la Unión, forzarles a atender las solicitudes de ejercicio de derechos o incluso ordenar directamente la rectificación, bloqueo, supresión o destrucción de los datos, así como prohibir el tratamiento de ciertos datos; puede someter asuntos a las instituciones y organismos y al TJUE para su consideración, y puede intervenir en los asuntos presentados ante éste último.

De todo ello tiene el Supervisor deber de guardar secreto, y de emitir un informe anual al Parlamento, al Consejo y a la Comisión.

B) El Comité Europeo de Protección de Datos

Se crea por el Reglamento 679/2016 (artículo 68), aunque dos meses después de la aprobación del mismo aún no se ha constituido.

Está formado por los directores de las autoridades de control de cada Estado miembro[111] y por el SEPD. La Comisión estará representada, pero sin derecho a voto. Los miembros

[111] El apartado 4 del artículo 68 señala que en los países en los que existan varias autoridades de control, se nombrará un representante común.

del Comité elegirán por mayoría simple a un presidente y dos vicepresidentes cada cinco años. El presidente se encarga de representar a la institución y preparar el orden del día de las reuniones. El Comité contará con una Secretaría que llevará a cabo las comunicaciones internas y externas de la institución, pero que por alguna razón está adjunta al SEPD; si bien únicamente seguirá las instrucciones del Comité.

El artículo 70 contiene una larga lista de funciones, que se resumen en 4: la emisión de un Dictamen sobre una medida llevada a cabo por una autoridad de control[112]; la emisión de resoluciones vinculantes ante las disputas entre autoridades de control[113]; el asesoramiento a la Comisión en materia de protección de Datos; y la elaboración de directrices, recomendaciones y códigos de buena prácticas. Además, emitirá un informe anual relativo al tratamiento de datos en la Unión y, cuando proceda, fuera de ella. En síntesis, se trata de una autoridad de control como las estatales pero que opera en toda la Unión y se encuentra por encima de ellas (en tanto deben recabar su opinión en ciertas ocasiones y pueden cumplir ciertas directrices).

El Comité actuará con total independencia y guardará secreto cuando corresponda.

Este Comité sustituye al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46.

C) Los DPOs

Los Delegados de Protección de Datos (en inglés *Data Protection Officers*, DPOs), también llamados Responsables de Protección de Datos, son una figura regulada en el Reglamento 679/2016 (artículos 37 y siguientes) con la finalidad de cooperar con el cumplimiento del Reglamento a nivel interno de las organizaciones.

No siempre es obligatoria su presencia. Deben nombrar un DPO: los organismos públicos excepto del orden judicial; los organismos cuya actividad requiera una

[112] El Dictamen y las medidas ante las que se debe emitir se encuentran regulados en el artículo 64.
[113] Estas resoluciones siguen el proceso del artículo 65.

observación habitual de interesados a gran escala[114]; y los organismos cuya actividad requiera el tratamiento a gran escala de datos personales especialmente protegidos y de datos relativos a condenas e infracciones penales. Un solo DPO puede ser designado conjuntamente por un grupo de empresas o de instituciones públicas. La relación puede ser contractual laboral o bien enmarcarse en un contrato de prestación de servicios.

Dentro del organismo u organismos el DPO debe tener a su alcance todas las cuestiones relativas al tratamiento de datos, y debe poderse contactar con él por parte de cualquier interesado. Sus funciones incluyen, aunque pueden contemplarse otras nuevas, el asesoramiento al responsable y al encargado en lo relativo al tratamiento de datos, en particular en lo referente a sus obligaciones y a la evaluación de impacto del tratamiento; la supervisión de la actividad del responsable y el encargado; y la comunicación entre el organismo en cuestión y la autoridad de control de datos correspondiente.

Lo no regulado en el Reglamento podrá ser desarrollado por la normativa estatal o por el contrato firmado entre el DPO y el organismo al que se le asigne.

Similares a los DPOs son los Responsables de protección de datos regulados en el Reglamento 45/2011 (artículos 24 y siguientes). Estos Responsables son nombrados para cada organismo europeo, y sus funciones son las mismas que las de sus homólogos salvo la obligación de llevar un registro de las operaciones de tratamiento, y que cooperan en su actividad con el SEPD.

D) La AEPD

La Agencia Española de Protección de Datos es la autoridad de control de ámbito estatal en España. Se regula por lo establecido en los artículos 35 y siguientes de la LOPD y en el Estatuto de la Agencia de Protección de Datos de 1993. Sobre éste último hay que decir que apenas ha sido actualizado en 23 años, por lo que hace referencia a normas e

[114] Por ejemplo, las operaciones de mercadotecnia que con la finalidad de mejorar las ventas de algunos productos conlleven el análisis del comportamiento de los consumidores, y por ello consistan en la toma de datos que revelen sus hábitos.

instituciones que ya no están en vigor; por ejemplo, remite al artículo 36 de la LORTAD para enumerar las funciones de la Agencia, y designa a la AEPD (entonces llamada simplemente APD, Agencia de Protección de Datos) como representante español en el Grupo de Protección de las Personas regulado en el artículo 29 de la Directiva 95/46 (sustituido desde mayo de 2016 por el Comité Europeo de Protección de Datos).

La AEPD es un ente de derecho público con personalidad jurídica propia que actúa con total independencia. Está formada por su Director, el Consejo Consultivo, el Registro General de Inspección de Datos y la Secretaría General, y cuenta con personal tanto funcionario como laboral para colaborar en el desempeño de sus funciones.

Dichas funciones son, básicamente, la supervisión del cumplimiento de la normativa de protección de datos, para lo que cuenta con diversas facultades: resolver reclamaciones frente a las actuaciones de responsables de tratamiento, requerir a éstos para que se ajusten a los procedimientos regulados en la ley, emitir directrices e instrucciones para adecuar los tratamientos a la normativa, hacer uso de la potestad sancionadora, remitir una memoria anual al Ministerio de Justicia, y en general cualquier tarea que le sea encargada por la LOPD, su estatuto[115] y la normativa europea[116]. El Reglamento de desarrollo de la LOPD regula en los artículos 115 y siguientes los procedimientos concretos que va a tramitar la Agencia, que son los siguientes: tutela de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), procedimiento sancionador, inscripción o cancelación de ficheros, transferencias internacionales de datos, códigos tipo y otros.

El Consejo Consultivo está compuesto por representantes de diversos ámbitos del Estado: un Diputado, un Senador, representantes de las Administraciones Central y

[115] Una función que regula directamente el estatuto es la participación de la AEPD en el Sistema de Información Schengen o SIS. El SIS II (de segunda generación) es un sistema de almacenamiento y transmisión de datos que almacena alertas sobre personas y objetos en relación con el control del espacio Schengen y cuya finalidad es garantizar la seguridad en dicho entorno. Está formado por una base de datos europea, otra en cada estado del espacio Schengen, y una infraestructura de comunicación entre ellos. El SIS cuenta con un grupo de supervisión coordinada compuesto por representantes de las autoridades nacionales de control, entre los que hay un representante de la AEPD, y por el SEPD cuya función es facilitar el intercambio de información. Sobre el SIS y la participación en él de la AEPD puede visitarse el apartado correspondiente de la web de la Agencia: https://www.agpd.es/portalwebAGPD/internacional/Europa/Cooperacion_Policial_Judicial/Sistema_de_Informacion_SCHENGEN/index-ides-idphp.php (visitado el 14 de junio).

[116] Un ejemplo importante es la representación que ejerce el director en el Comité Europeo de Protección de Datos.

Local y de las CCAA que hayan creado una agencia de protección de datos (actualmente Cataluña y País Vasco)…que se renuevan cada cuatro años. Será el Director de la Agencia, que además preside el Consejo, el que lo convoque para que le asesore. Para el procedimiento específico de actuación se remite el estatuto al Título II, Capítulo II de la Ley 39/1992 del Régimen Jurídico de las Administraciones Públicas, referente al funcionamiento de los órganos colegiados. Como esta disposición ha sido derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en aplicación de la Disposición Final Cuarta de esta norma, hay que acudir a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, Capítulo II, Sección 3ª. Sintetizando los artículos 15 a 18 de esta Ley, las reuniones se convocan atendiendo a la regulación Reglamentaria del órgano en cuestión, se ciñen al orden del día, y se levanta acta de lo tratado en ellas.

El Director es nombrado por el Gobierno de entre los miembros del Consejo Consultivo por un plazo de cuatro años, que solo se verán acortados por las causas establecidas en el artículo 15 del Estatuto[117]. Se encarga, en general, de dirigir y representar a la Agencia. Más en concreto, los artículos 12 y 13 del Estatuto contemplan una serie de funciones de dirección y de gestión; de entre las primeras destacan la competencia en materia de resoluciones sobre ficheros privados y sobre el Registro General de Protección de Datos, y la competencia en materia de expedientes sancionadores, que es completa para los referidos a responsables de ficheros privados, y únicamente básica[118] para los referidos a infracciones cometidas por Administraciones Públicas; de entre las segundas, controla todo lo relativo a los recursos económicos de la Agencia, aprueba la Memoria anual, y ordena la convocatoria de las reuniones del Consejo Consultivo.

El Registro General de Protección de Datos se define por el Estatuto (artículo 23) como "el órgano de la Agencia de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal,

[117] "a) Incumplimiento grave de las obligaciones del cargo.

b) Incapacidad sobrevenida para el ejercicio de sus funciones.

c) Incompatibilidad.

d) Condena por delito doloso."

[118] En concreto, el artículo 12.1.j) se refiere a la capacidad de "Instar la incoación de expedientes disciplinarios en los casos de infracciones cometidas por órganos responsables de ficheros de Administraciones Públicas".

con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación". En él se deben inscribir todos los ficheros, tanto públicos como privados, que contengan datos personales, así como las autorizaciones de transferencia de datos personales a otros países y los códigos tipo regulados por la LOPD[119]. La no inscripción de ficheros en el Registro está entre las infracciones leves reguladas en el Título VII de la LOPD, y puede acarrear una multa de entre 900 y 40.000 euros.

Una de las facultades que se otorga a la AEPD es la potestad de inspección de ficheros con el fin de cumplir con sus funciones. Esta potestad incluye desde la petición de exhibición de datos, hasta la entrada en los locales para el examen de los equipos físicos y lógicos[120]. Los funcionarios que ejerzan esta potestad tendrán el carácter de autoridad pública, y deberán guardar secreto. El responsable por su parte está obligado a facilitar el ejercicio de la potestad de inspección, ya sea enviando información o permitiendo la entrada en su local. La obstrucción de la inspección se considera una infracción grave que puede acarrear multas de entre 40.001 y 300.000 euros.

Finalmente, la AEPD cuenta con una Secretaría General que apoyará al personal de la Agencia de diversos modos. Las notificaciones y la gestión de medios personales y de asuntos de carácter general son algunas de sus tareas.

E) Organismos autonómicos: las agencias catalana y vasca

La LOPD permite en su artículo 41 la creación de órganos autonómicos que cumplan las mismas funciones que la AEPD salvo lo relativo a movimientos internacionales de datos, a las infracciones de las Administraciones y a la inmovilización de ficheros. Las

[119] Está por ver si los códigos de conducta regulados por el RGPD deberán ser también inscritos en el Registro, ya que, por un lado, se diferencian de los códigos tipo en que serán de obligatorio cumplimiento (el artículo 32.3 LOPD da a los códigos tipo un carácter de "código deontológico o de buenas prácticas"), y, por otro, deberá crearse un organismo de control del cumplimiento de estos códigos que podría tener su propio registro al respecto.

[120] El artículo 28 del Estatuto contiene una enumeración de las facultades concretas: "a) Examinar los soportes de información que contengan los datos personales. b) Examinar los equipos físicos. c) Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los algoritmos de los procesos de que los datos sean objeto. d) Examinar los sistemas de transmisión y acceso a los datos. e) Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la Ley Orgánica 5/1992. f) Requerir la exhibición de cualesquiera otros documentos pertinentes. g) Requerir el envío de toda información precisa para el ejercicio de las funciones inspectoras."

Comunidades Autónomas también pueden crear sus propios registros de ficheros. El Director de la AEPD puede convocar a los órganos autonómicos para coordinar criterios y procedimientos, así como requerirles que adopten las medidas necesarias cuando un fichero autonómico incumpla la LOPD.

Tres Comunidades Autónomas han hecho uso de la potestad de creación de una autoridad de control autonómica:

El Estatuto de Autonomía de Cataluña contempla en su artículo 31 tanto el derecho a la protección de datos personales como la necesidad de que una autoridad independiente designada por el Parlamento vele por el cumplimiento de este derecho, y el artículo 156 otorga a la Comunidad la competencia para crear dicha autoridad y registrar y controlar los ficheros de los organismos públicos de la Comunidad y los ficheros que sirvan para el ejercicio de funciones públicas. Con laLey 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos se crea dicha Autoridad, que es bastante parecida a la Agencia estatal: está presidida por un Directos apoyado por un Consejo Asesor, tiene facultad de inspección, de resolución de reclamaciones, y de sanción de infracciones. Tiene también un registro autonómico de ficheros. Sí existe una diferencia notable entre la autoridad catalana y la estatal: la primera circunscribe su actividad a las instituciones públicas y a las privadas controladas por el sector público directa o indirectamente[121].

El País Vasco también ha creado su propia Agencia de Protección de Datos. En síntesis, para evitar reiteraciones, es equivalente a la catalana en cuanto que tiene la misma estructura y funcionamiento que la AEPD y que únicamente opera en el ámbito de las instituciones públicas de la Comunidad.

Finalmente, la Comunidad Autónoma de Madrid también creó su Agencia mediante la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. A diferencia de los dos casos anteriores, esta Agencia ha dejado de existir, puesto que la citada Ley que la creó quedó derogada por la Ley8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas. Más concretamente, es el artículo 61 de esta segunda Ley el que extingue la Agencia autonómica, devolviendo a la estatal

[121] Por control indirecto ha de entenderse que los recursos económicos con los que cuente la institución en cuestión sean mayoritariamente públicos.

las competencias que se habían adquirido, y el que ordena a los responsables de la Agencia rendir cuentas de su actividad durante los 11 años de existencia del organismo.

III.- EVOLUCIÓN DEL DERECHO: PASADO, PRESENTE Y FUTURO

El pasado

El derecho a la autodeterminación informativa ha ido surgiendo conforme se han desarrollado las nuevas tecnologías, si bien éstas han ido siempre por delante. Debe darse mérito al carácter previsor en este sentido que tuvieron los impulsores de las primeras iniciativas de la protección de datos, que en Europa fueron los Gobiernos de Suecia y del *land* alemán de Hesse, primeros lugares en los que aparecieron leyes de protección de datos, y la Comisión Europea a mediados de los setenta.

El comienzo de la elaboración de este derecho no fue sencillo, ya que fue necesario declarar su autonomía del derecho a la intimidad. En efecto, lo que hoy en día se empieza a conocer como un bien jurídico independiente, los datos personales, solía incluirse en la esfera de la intimidad, y por ello no se les daba más importancia. En defensa de los que en un principio rechazaron la concepción de un nuevo derecho hay que recordar la velocidad a la que avanzan las nuevas tecnologías: hace cuarenta años era muy difícil intuir la revolución digital que se avecinaba y los riesgos que conllevaría. Solo el tiempo y la experiencia han acabado por dar la razón a los defensores de la protección de datos como derecho autónomo.

Las nuevas tecnologías a las que se hace referencia han sido principalmente los ordenadores, internet y los dispositivos móviles (teléfonos, *smartphones*, tabletas, entre otros). Desde la segunda mitad del siglo XX se han ido desarrollando ordenadores cada vez más potentes, que cobraron una importancia capital con la aparición y expansión de internet en los años setenta y ochenta, y que desde la aparición de los *smartphones* o teléfonos inteligentes han empezado a tener menos importancia como medio de comunicación en la sociedad.

Sin embargo no han sido únicamente las nuevas tecnologías las que han dado lugar a este nuevo derecho: también la globalización ha tomado parte. Y es que la existencia de cada vez más compañías internacionales, el aumento en las relaciones y comunicaciones supraestatales… hacen que el flujo global de datos se haya incrementado a su vez.

El resultado ha sido la elaboración de un concepto de datos personales como una extensión más de la personalidad de los ciudadanos que debe ser protegida en consecuencia, y esto se ha llevado a cabo tanto a nivel constitucional como legal.

En definitiva, la revolución tecnológica con la que concluyó el milenio pasado abonó el terreno por igual a nuevas oportunidades y riesgos, y tanto en Europa como en América, continentes pioneros en esta materia, los diferentes Estados y organismos supraestatales llevan varias décadas tratando de organizar y regular la nueva situación. En lo que a este Trabajo respecta, se ha puesto coto a la utilización de datos personales de forma indiscriminada. Por desgracia, ello ha pasado generalmente desapercibido para la ciudadanía.

Presente

El mensaje sobre la necesidad de proteger los datos personales no caló inmediatamente entre la población. Es un tópico recurrente el decir que cuando en internet se encuentra una casilla junto al texto "aceptar los términos y condiciones" se suele hacer click en aceptar sin pensarlo dos veces. Esto es un reflejo de la despreocupación con la que los ciudadanos se han comportado con sus datos personales en internet.

Al igual que anteriormente cuando se cuestionaba la necesidad de un nuevo derecho, también hay que decir que la situación es abismalmente diferente en la segunda década del siglo XXI a lo que era en los años noventa y principios del nuevo siglo, con el "boom" de internet. Actualmente la sociedad vive constantemente bajo la electrónica mirada de una pantalla, sea del aparato que sea. Prácticamente cualquier acción queda registrada y almacenada para un posterior análisis. La situación ha cambiado mucho en un periodo muy corto de tiempo, y es por ello que la sociedad ha tardado en adaptarse.

Han sido hechos como la revelación del espionaje del Caso Snowden, o el conflicto iniciado por Max Schrems[122] contra Facebook los que han hecho recapacitar a la gente.

[122] El austríaco Max Schrems es el activista fundador de Europe vs Facebook, la plataforma que demandó a, entre otras grandes empresas del mismo sector, Facebook. El pleito llegó al TJUE, y concluyó con la famosa sentencia que anula el acuerdo de "puerto seguro" ("*safeharbor*") entre Europa y Estados Unidos, acuerdo que permitía el libre intercambio de datos entre ambos continentes. Según alegó Schrems, la red social era utilizada por la Agencia Nacional de Seguridad estadounidense para recabar

Con la concienciación de la sociedad vienen inevitablemente los cambios legislativos, y en 2012 comenzó la elaboración del nuevo Reglamento General de Protección de Datos.

La normativa europea de protección de datos ha sido criticada por ser considerada muy burocrática y difícil de llevar a la práctica[123]. En efecto, han proliferado los supuestos de hecho que demandan una respuesta más rápida de la que ofrecen las normas de protección de datos; no ha de olvidarse que la cuestión principal en materia de protección de datos es que una vez se pierde el control de los mismos es muy difícil que vuelva a recuperarse, y el hecho de que los ciudadanos tengan distintos derechos que ejercitar ante un uso ilícito de sus datos personales (que por otro lado es un gran avance y algo a lo que debe darse mucho mérito) es insuficiente para proporcionar esa respuesta rápida, por muy eficiente que se sea en la tramitación de las solicitudes relativas a dichos derechos.

Dicho lo cual, también es de alabar la actuación de las autoridades de control, que han llevado y llevan a cabo sus labores (interpretación y control de la aplicación de las normas de protección de datos, publicidad a las mismas, facilitar a la población información y medios para proteger sus derechos…) con gran diligencia y eficacia.

En síntesis, actualmente el derecho a la autodeterminación informativa goza de autonomía, garantías e instrumentos de protección, y su desarrollo se concibe como un avance necesario en las sociedades modernas.

Futuro

En España y en Europa el futuro del derecho a la autodeterminación informativa pasa por el nuevo RGPD, que entrará en vigor en mayo de 2018. El tiempo dirá si responde a los objetivos por los que se inició su elaboración.

Si bien en principio supone una mejora sobre la mayoría de aspectos de la Directiva, ampliando el articulado y explicando mejor lo relativo a los mecanismos de protección de datos, precisamente el hecho de que sea un texto mucho mayor que la Directiva hará que sea más complejo de aplicar, y podría agravar el problema de lo poco práctico de las normas Europeas de protección de datos.

---

datos de sus usuarios, lo que llevó al TJUE a considerar que América no es un territorio seguro al que enviar datos de ciudadanos europeos.

[123] Ver nota al pie 89

En España el Gobierno que surja del interregno político de la primera mitad del año 2016 deberá modificar las leyes de protección de datos, esencialmente la LOPD y su Reglamento de desarrollo, para hacerlas más acorde con el nuevo Reglamento. También existe la posibilidad de elaborar una Ley nueva, lo que permitiría intentar mejorar la estructura de la actual. En cualquier caso, conviene actuar lo antes posible para estar preparados para la entrada en vigor del Reglamento.

A este respecto ya ha comenzado a actuar la AEPD, mediante la publicación de pequeñas guías que ayudan a entender qué aporta de nuevo el Reglamento y a qué deben prestar atención los responsables y encargados del tratamiento de datos, que al fin y al cabo son los que más medidas tendrán que llevar a cabo para adaptarse. Así, el 26 de mayo la AEPD publicó una serie de respuestas a las preguntas más frecuentes que pueden surgir sobre el Reglamento[124]; el 29 de junio tuvo lugar la 8ª Sesión Anual Abierta de la AEPD, en la que participaron entre otros el Ministro de Justicia y la Directora de la Agencia, y se trataron cuestiones generales sobre cuestión de datos y sobre la adaptación del RGPD[125]; también el 29 de junio se publicó una nota de prensa en la que se resumían las intervenciones relativas al Reglamento[126].

Además de la actividad de la Agencia y de la actualización de las normas legales y reglamentarias España puede avanzar en la regulación de la protección de datos de otra forma: la reforma constitucional. Como ya se ha mencionado en alguna ocasión, el artículo de la Constitución que sienta la base para la construcción de este derecho adolece de defectos importantes en su redacción, siendo uno destacable la confusión del derecho a la autodeterminación informativa con el derecho a la intimidad. Es por ello que debiera plantearse una reforma del artículo 18.4 que reflejase los avances producidos en estos casi cuarenta años que lleva en vigor la Norma Suprema. Por desgracia, nuevamente hay que hacer alusión a la incapacidad de los partidos políticos de nuestro país por superar sus diferencias para llevar a cabo actividades de esta envergadura, y si bien ello probablemente no sea una gran dificultad para la redacción

[124] Pueden encontrarse en el siguiente enlace: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php (visitado por última vez el 29 de junio).

[125] Puede verse la sesión completa en la página web de la AEPD, en este enlace: http://www.agpd.es/portalwebAGPD/jornadas/8_sesion_anual/index-ides-idphp.php (visitado el 29 de junio).

[126] Puede verse aquí: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_06_29_02-ides-idphp.php (visitado el 29 de junio).

de nuevas Leyes (o modificación de las existentes), sí supone un obstáculo casi insuperable para cambiar la Constitución, que es considerada como rígida por la dificultad y complejidad de su proceso de reforma[127].

[127] Al respecto, ver **García Cuadrado, Antonio M.***Principios de Derecho Constitucional.* León : Eolas, 2011, páginas 657 a 663, especialmente el parágrafo 492.

CONCLUSIONES

El derecho a la autodeterminación informativa pertenece a la última generación de derechos, surgidos en la segunda mitad del siglo XXI a consecuencia de los más modernos avances tecnológicos. La importancia de la protección de datos no fue objeto de una especial atención inicialmente, pero el tiempo ha puesto las cosas en su lugar y ahora forma parte del elenco de derechos constitucionales de los ciudadanos.

En Europa se ha hecho un esfuerzo por armonizar las legislaciones estatales en esta materia antes de que comenzasen a dispersarse, y se ha conseguido en gran medida, si bien ello ha hecho que la aplicabilidad de los mecanismos de protección de datos sea bastante compleja. En cualquier caso, la elaboración de la Directiva 95/46 y del RGPD es la prueba de que se reconoce la existencia de un riesgo y la voluntad de tomar medidas para minimizarlo.

Igualmente en nuestro país la adaptación de la normativa internacional en forma de la LORTAD y la LOPD, si bien hecha de forma tardía, es un síntoma de un avance en la dirección coherente con la dinámica actual. Aunque más que la redacción de estas leyes, que al fin y al cabo son prácticamente copias de la normativacomunitaria y no innovan en demasía, es importante la existencia y la labor de la AEPD, que es el organismo que efectivamente se encarga de velar por la seguridad de los ficheros de datos.

Desde el punto de vista constitucional, la deficiente redacción del artículo 18.4 CE ha ido en detrimento de la construcción del derecho a la autodeterminación informativa. Ha tenido que ser el TC en su labor de intérprete de la Norma Suprema el que se encargó de poner la protección de datos a la altura a la que debe estar. Esto debe ser motivo de reflexión, y es que la Constitución, aunque pilar fundamental de nuestro ordenamiento, no es un elemento inamovible del mismo, y su reforma, siendo no solo necesaria, sino también objetivamente positiva para la protección de los derechos de los ciudadanos, debe ser llevada a cabo para que no se vuelva a dudar de la existencia de este derecho.

Una posible reforma consistiría en la sustitución del actual punto cuarto del artículo 18 por un texto que diferenciase la autodeterminación informativa como un derecho autónomo, tal como el siguiente:

Se reconoce el derecho a la autodeterminación informativa y a la protección de los datos propios. No podrá hacerse uso de los mismos sin el consentimiento del interesado u otra base jurídica suficiente.

Reformas menos ambiciosas pudiesen optar en lugar del término "autodeterminación informativa" por una alusión únicamente a la protección de datos, pues en el fondo, como se ha dejado constancia en el análisis del derecho, su núcleo esencial radica en los mecanismos de protección de los datos personales.

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Portal Web de la Agencia Española de Protección de Datos. *Portal Web de la Agencia Española de Protección de Datos.* [En línea] 26 de mayo de 2016. [Citado el: 8 de junio de 2016.] http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php.

ALZAGA VILLAAMIL, ÓSCAR.*Comentario sistemático a la Constitución española de 1978.* Madrid : Ediciones del Foro, 1978. ISBN 84-85589-00-9.

DEL CASTILLO VÁZQUEZ, Isabel Cecilia.*Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar.* Primera edición. Pamplona : Aranzadi, 2007. pág. 740. ISBN 978-84-470-2858-0.

GARCÍA CUADRADO, Antonio M.*Principios de Derecho Constitucional.* León : Eolas, 2011. ISBN 978-84-938666-8-6.

HEREDERO HIGUERAS, Manuel.*La Directiva Comunitaria de Protección de los Datos de Carácter Personal.* Pamplona : Aranzadi, S.A., 1997. pág. 375. ISBN 84-8193-515-8.

—. *La Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentario y textos.* Madrid : Editorial Tecnos, 1996. ISBN 84-309-2824-3.

Informe anual de 2015 del Procurador del Común de Castilla y León. Procurador del Común de Castilla y León. León : s.n., 2015. pág. 766.

MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis.*El derecho a la audoterminación informativa.* Madrid : Fundación coloquio jurídico europeo, 2009. ISBN: 9788461334704.

MURILLO DE LA CUEVA, Pablo Lucas.*Informática y protección de datos personales. Estudio sobre la Ley Orgánica 5/1993, de regulación del tratamiento*

automatizado de los datos de carácter personal). Madrid : Centro de estudios constitucionales, 1993. ISBN 84-259-0940-6.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. European Data Protection Supervisor. *European Data Protection Supervisor.* [En línea] [Citado el: 8 de junio de 2016.] https://secure.edps.europa.eu/EDPSWEB/edps/lang/es/EDPS/cache/offonce.

The Right to Privacy. **WARREN, Samuel D. y BRANDEIS, Louis D.** 5, Cambridge, Massachusetts : The Harvard Law Review Association, diciembre de 1890, Harvard Law Review, Vol. IV.

VLADEK, David. Separated by common goals: A U.S: Perspective on narrowing the U.S.-EU privacy divide. [aut. libro] Artemi Rallo Lombarte y Rosario García Mahamut. *Hacia un nuevo derecho europeo de protección de datos.* Valencia : Tirant lo Blanch, 2015.

JURISPRUDENCIA CONSULTADA

Sentencias del Tribunal Constitucional:

- Sentencia núm. 254/1993 de 20 julio.
- Sentencia núm. 143/1994, de 9 de mayo.
- Sentenciasnúm. 11/1998 de 13 enero y 45/1999 de 22 de marzo, primera y última sentencias de la serie relativa al caso de la huelga de RENFE.
- Sentencia núm. 144/1999, de 22 de julio.
- Sentencia 290/2000, de 30 de noviembre de 2000.
- Sentencia 292/2000, de 30 de noviembre de 2000.
- Sentencia 2/1982, de 29 de enero de 1982.

Sentencias del Tribunal Supremo

- Sentencia núm. 2210/2005.
- Sentencia núm. 6689/2002.

Sentencias del Tribunal de Justicia de la Unión Europea

- Sentencia en el asunto C-101/01, B. *Lindqvist* contra Suecia, de 6 de noviembre de 2003.
- Sentencia en el asunto C-131/12, Google contra España, de 13 de mayo de 2014.

Sentencias de derecho comparado

- Sentencia del Tribunal Constitucional Federal Alemán 65, 1 [Censo de Población].

NORMATIVA UTILIZADA

Europea

- Convenio Europeo de los Derechos Europeos de 1950.
- Convenio 108 del Consejo de Europa de 1981.
- 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 datospersonales y a la libre circulación de estos datos.
- Reglamento (CE) Nº 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.
- Decisión nº 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 SupervisorEuropeo de Protección de Datos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Española

- Constitución de 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.
- Ley Orgánica 5/1992 de 29 de octubre de regulación del tratamiento automatizado de los datos de carácterpersonal.
- 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.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley del Procedimiento Administrativo Común de las Administraciones Públicas
- Ley 20/2011, de 21 de julio, del Registro Civil.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.
- Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña.
- Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.
- 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.

- Decreto 308/2005, de 18 de octubre, por el que se desarrolla 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.
- Decreto 309/2005, de 18 de octubre, por el que se aprueba el Estatuto de la Agencia Vasca de Protección de Datos.
- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.
- Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas.

Otras

- Constitución de Portugal de 1976
- Constitución de Brasil de 1988
- Constitución de la Provincia de Buenos Aires de 1994
- Ley Fundamental para la República Federal de Alemania de 1949
- Recomendaciones de la OCDE de 1980 sobre protección de la privacidad y flujos transfronterizos de datos personales.
- Declaración del Pleno del Tribunal Constitucional 1/2004, de 13 de diciembre de 2004. Requerimiento 6603-2004. Formulado por el Gobierno de la Nación, acerca de la constitucionalidad de los artículos I-6, II-111 y II-112 del Tratado por el que se establece una Constitución para Europa, firmado en Roma el 29 de octubre de 2004. Primacía del Derecho comunitario y alcance de la Carta de derechos fundamentales de laUnión Europea.