



Universidad de Jaén

Facultad de Ciencias Sociales
y Jurídicas

EL DERECHO A LA PROTECCIÓN DE DATOS, REGULACIÓN Y APLICACIÓN EN EUROPA Y ESPAÑA

ALUMNO: ARIEL GABRIEL PEÑAFIEL BURBANO

TUTORA: DRA. CATALINA RUIZ – RICO – RUIZ

MAYO, 2019

“El reconocimiento de la protección de datos como derecho fundamental cumple con el objetivo de mantener la relación entre la persona y su cuerpo, ya no enclaustrado en los confines de la fisicidad y en el secreto de lo psíquico, sino realmente dislocado, entregado a los infinitos bancos de datos que dicen al mundo quiénes somos”

Stefano Rodotà (2014)

ABREVIATURAS:

ARCO: Derechos de acceso, rectificación, cancelación y oposición

AEPD: Agencia Española de Protección de Datos

BOE: Boletín Oficial del Estado

CE: Constitución Española

CDFUE: Carta de los Derechos fundamentales de la Unión Europea

IP: Identificación Personal

NTIC: Nuevas tecnologías de la información y comunicación

LTAIPBG: Ley de transparencia, acceso a la información pública y buen gobierno

LOPDGDD: Ley Orgánica de protección de datos personales y garantía de los derechos digitales

LSSICE: Ley de servicios de la sociedad de la información y del comercio electrónico

LOPD: Ley Orgánica de Protección de datos de carácter personal

RGPD: Reglamento General de Protección de Datos

RLOPD: Reglamento de desarrollo de la Ley Orgánica de Protección de datos

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

STS: Sentencia Tribunal Supremo

STC: Sentencia Tribunal Constitucional

TFUE: Tratado sobre el Funcionamiento de la Unión Europea

TJUE: Tribunal de Justicia de la Unión Europea

TS: Tribunal Supremo

TC: Tribunal Constitucional

UE: Unión Europea

RESUMEN:

La última revolución industrial, que ha ido de la mano de la tecnología, marcó un antes y un después en la forma en que la sociedad ha funcionado y que funciona desde su surgimiento, afectando a todos sus ámbitos tanto académico, económico, profesional, social etc. De hecho la frase “Si no estás en Internet no existes” ha cobrado gran fuerza en la actualidad.

Situaciones que en el pasado requerían de un largo proceso, como la interacción social entre personas de distintos países, en la actualidad se realizan en cuestión de segundos, gracias al surgimiento del Internet que ha permitido el desarrollo de Redes sociales interactivas conectadas a la red – Facebook, Instagram, Twitter, whatsapp - aunque ciertamente la parte negativa de este gran avance, ha sido la exposición y en algunos casos pérdida consciente e inconsciente de nuestro derecho a la intimidad y privacidad (Art. 18 CE) y (Art. 8 CEDH), derechos ligados a la protección de los datos de carácter personal a través de los cuales nos definimos como personas – nombres, apellidos, etnia, estado de salud, nivel de estudios, nivel económico etc – y como ciudadanos de un determinado Estado.

Por ello, la Unión Europea ha sido pionera en la regulación y protección del Derecho fundamental a la Protección de datos de carácter personal que a partir del 25 de mayo de 2018, a través del Reglamento General de Protección de Datos (RGDP), lo regula, siendo plenamente aplicable en toda Europa.

En el presente trabajo abordaremos, por una parte la Regulación y aplicación del Derecho a la protección de datos de carácter personal centrándonos en el ámbito Europeo y vinculándolo con la normativa nacional vigente. Analizaremos el impacto del denominado Derecho al Olvido en la intimidad y privacidad de la persona y por último, conoceremos los mecanismos para la protección de este derecho a través de los denominados Derechos ARCO - acceso, rectificación, cancelación y oposición – su definición e impacto en la jurisprudencia europea, haciendo especial hincapié en el de acceso y rectificación.

PALABRAS CLAVE: Unión Europea, Protección de datos de carácter personal, Derecho al olvido, Red social, Internet, Intimidad, Privacidad, Libertad de expresión.

ABSTRACT:

The last industrial revolution, which has gone hand in hand with technology, marked a before and after in the way in which society has functioned and which works since its emergence, affecting all of its academic fields, economic, professional, social etc. In fact the phrase "If you are not on the Internet you do not exist" has gained great strength today.

Situations that in the past required a long process, such as social interaction between people from different countries, are currently taking place in a matter of seconds, thanks to the emergence of the Internet that has allowed the development of interactive social networks connected to the network – Facebook, Instagram, Twitter, Whatsapp - although certainly the negative part of this breakthrough, has been the exposure and in some cases loss of conscious and unconscious of our right to privacy and privacy (Art. 18 CE) and (Art. 8 CEDH) rights linked to the protection of personal data through which we define ourselves as persons – names, surnames, ethnicity, state of health, level of education, economic level etc – and as citizens of a given State.

Therefore, the European Union has been a pioneer in the regulation and protection of the fundamental right to the protection of personal data that from 25 May 2018, through the General Regulation on Data Protection (RGDP), regulates it, being fully applicable throughout Europe.

In this paper we will address, on the one hand, the Regulation and application of the Right to Personal Data Protection by focusing on the European level and linking it to existing national legislation. We will analyze the impact of the Right to Oblivion on the privacy and privacy of the person and finally, we will know the mechanisms for the protection of this right through the so-called Rights ARCO, access, rectification, cancellation and opposition; their definition and impact on European jurisprudence, with particular emphasis on access and rectification.

KEY WORDS: European Union, Protection of personal data, Right to oblivion, Social network, Internet, Privacy, Freedom of expression.

ÍNDICE

1.	INTRODUCCION.....	1
2.	OBJETIVOS.....	2
3.	LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL EN EL ÁMBITO NACIONAL Y DE LA UNIÓN EUROPEA.	3
3.1.	Las nuevas tecnologías y su impacto en la reglamentación del derecho a la protección de datos de carácter personal.....	3
3.2.	El derecho a la protección de datos como “nuevo” derecho y nueva solución a los retos de las NTIC.....	5
3.3.	Normativa de la Unión Europea, tratados internacionales y legislación Estatal sobre el Derecho a la protección de datos de carácter personal	7
a)	Consejo de Europa.....	7
b)	Unión Europea.....	8
c)	Derecho Español.....	10
3.4.	Los fundamentos del derecho a la protección de datos y su relación con otros derechos análogos	11
a)	Protección de Datos y Libertad de Expresión.....	15
b)	Naturaleza y alcance de la Directiva 95/46/CE	18
3.5.	Ley de transparencia y criterio de interés público: conflicto protección de datos y el interés público	
a)	Normativa sobre Transparencia y Protección de Datos.....	20
b)	Transparencia. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.....	21
c)	Jurisprudencia sobre Protección de Datos del Tribunal Europeo de Justicia.....	23
d)	Del Tribunal Constitucional	23
4.	DERECHO AL OLVIDO, REDES SOCIALES Y NUEVAS TECNOLOGIAS.....	25
4.1.	El régimen constitucional del derecho al olvido digital	25
4.2.	El Derecho a la Intimidad y su relación con otros derechos fundamentales	26
a)	El art.- 10.1 CE y el libre desarrollo de la personalidad.....	26
b)	La Titularidad y la delimitación del contenido y los límites del derecho al olvido.....	28
4.3.	La configuración del derecho al olvido digital.....	29
4.4.	Derecho al Olvido análisis Jurisprudencial	33
a)	La sentencia de la Gran Sala del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo de 2014. Google Spain S.L. y Google Inc frente al ciudadano español Sr. Costeja González y la Agencia Española de Protección de Datos.	34
b)	La Jurisprudencia del Tribunal Supremo	36
5.	LOS DERECHOS EN PROTECCIÓN DE DATOS	40
5.1.	Derechos ARCO	40

5.2.	Derecho de Acceso	43
5.3.	Derecho de Rectificación.....	46
5.4.	Derecho de Cancelación	47
5.5.	Derecho de Oposición	48
5.6.	Derecho de Indemnización.....	48
6.	CONCLUSIONES	49
6.	BIBLIOGRAFÍA	51

1. INTRODUCCION

La importancia que ha cobrado el desarrollo tecnológico es indudable, pero el almacenamiento, tratamiento y difusión masiva de la información presenta un riesgo potencial para los derechos fundamentales de las personas. Los avances tecnológicos ocurridos en los últimos años, así como la rápida y constante evolución del mundo digital, obligan a plantearse si la regulación jurídica actual de la red es eficaz. Por ello, es fácil entender la creciente preocupación por los usos potenciales de la información disponible en la red, en una época de acelerado desarrollo tecnológico y humano, de nuevas prácticas sociales y comerciales, en la que el acceso libre y directo a la web es una realidad casi insoslayable y en la que se da un uso masivo de esta.

En la actualidad, el derecho a la protección de datos de carácter personal sí que se ha reconocido como derecho fundamental a nivel de la Unión Europea (UE), consagrado explícitamente en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE) y ha sido desarrollado por la jurisprudencia del Tribunal de Justicia (TJUE), así como, en el ámbito del Consejo de Europa (CdE), en la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) de desarrollo del derecho a la vida privada y familiar artículo 8 del Convenio Europeo de Derechos Humanos (CEDH).

Este Derecho se ha venido definiendo como el derecho de toda persona a tener un control sobre el uso de sus datos personales. Esta potestad de control permite evitar que, a través del tratamiento de datos de carácter personal, se pueda llegar a disponer de información que afecte a la intimidad y demás derechos fundamentales y libertades públicas de las personas.

Una de estas amenazas, propia de la naturaleza del mundo digital, es la perennidad y universalidad de la información que se publica y se comparte en la web, lo cual supone una permanencia de datos potencialmente perjudiciales para cualquier persona, que son mundialmente accesibles por parte de cualesquiera usuarios de Internet, con total ausencia de límites espacio-temporales.

Por todo ello, la protección de datos es el nuevo objetivo de los legisladores. De hecho, el dato tiene hoy en día la consideración de bien económico, susceptible de valoración pecuniaria, lo que tiene como consecuencia la creación de normas comunitarias y el reforzamiento de las ya existentes nacionales así como su actualización al panorama actual, dado que vivimos en plena era de la información, a fin de proteger tanto al usuario español como europeo.

2. OBJETIVOS

Los objetivos que persigue el presente trabajo se pueden resumir de la siguiente forma:

1. Investigar y analizar el impacto que ha supuesto el desarrollo de las nuevas tecnologías de la información y comunicación (NTIC) en la vida de la sociedad actual y especialmente en la privacidad de la persona a través del estudio del Derecho fundamental a la Protección de Datos de Carácter personal tanto en el ámbito Estatal como a nivel Comunitario.
2. Realizar un análisis jurisprudencial en lo referente al conflicto en el que puede entrar este Derecho con otros derechos fundamentales como la libertad de expresión, el interés público, mediante un estudio de diferentes sentencias del Tribunal Europeo de Justicia.
3. Entender el surgimiento y alcance del Derecho al olvido digital, su regulación, aplicación y relación con otros derechos fundamentales mediante el estudio de legislación nacional y comunitaria, así como análisis de jurisprudencia. Que nos permita ubicar concretamente a este derecho a nivel Constitucional fundamental.
4. Determinar el contenido de los Derechos de acceso, rectificación, cancelación, oposición e indemnización en relación con la protección de datos.

En el trabajo se analiza la regulación de la Protección de Datos de carácter personal en Europa y España a través de una observación a las distintas normativas Comunitarias, tratados internacionales, legislación nacional y jurisprudencia.

Como punto de partida, debemos considerar la Protección de Datos de carácter personal del artículo 8 del Convenio Europeo de Derechos Humanos y de las Libertades fundamentales (CEDH) y el artículo 18.1 de la Constitución Española (CE) y su relación con el artículo 10 CE. Así como el estudio de las distintas sentencias emitidas por el Tribunal Europeo de Justicia y la aplicación de la ya derogada, Directiva 95/46/CE, pero no obstante vinculada y con efectos al Reglamento General de Protección de Datos de 25 de mayo de 2018.

Dichas sentencias son:

5. Sentencia de 6 de noviembre de 2003, caso Lindqvist, asunto C – 101/01.
6. Sentencia de 7 de mayo de 2009, caso Rijkeboer, asunto C – 553/07.
7. Sentencia de 20 de diciembre de 2017, caso Nowak, asunto C – 434716.

Seguidamente, estudiaremos el Derecho al olvido digital, su regulación constitucional, relación con otros derechos fundamentales, configuración y jurisprudencia.

Para terminar el trabajo se profundizara en los Derechos ARCO, como medio de protección de los datos de carácter personal, su regulación y aplicación.

3. LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL EN EL ÁMBITO NACIONAL Y DE LA UNIÓN EUROPEA.

3.1.Las nuevas tecnologías y su impacto en la reglamentación del derecho a la protección de datos de carácter personal

El ritmo acelerado de la llamada cuarta revolución industrial o tecnológica de las comunicaciones y de la informática (NTIC), han supuesto un giro de 360 grados para la economía y la sociedad. Este cambio se puede constatar de manera clara viendo el papel de los jugadores en el tablero económico y social: sólo existes si estás en Facebook, Twitter o Instagram; Wikipedia se ha comido la industria de las enciclopedias; YouTube y Netflix han cambiado drásticamente el modo en que vemos la televisión o vamos al cine; Airbnb ha perturbado significativamente la industria hotelera y Uber o Cabify están en proceso de distorsionar los clásicos servicios de taxi.

Por otro lado, vemos cómo las NTIC han abierto nuevos tipos de mercados, distintos a los tradicionales mercados de bienes y servicios: hablamos, efectivamente, de los mercados de datos personales (Acquisti, 2016). Y así, sucesivamente, vemos que la innovación tecnológica y la transformación digital han cambiado de manera radical todas las facetas de nuestra vida cotidiana. Todo lo cual ha marcado y cambiado radicalmente la escala y el modo en que se intercambian y se utilizan los datos.

A día de hoy, cabe destacar la desaparición de la distancia espacio temporal en la creación y difusión de los contenidos en la Web, las nuevas tendencias tecnológicas (incluyendo los avances del hardware, los avances del software, la creciente conectividad y ubicuidad, así como el desarrollo y proliferación de los motores de búsqueda), el auge de las libertades informativas y, sobre todo, la indeleble perennidad de la información en Internet.

Con respecto a los avances en el hardware, el aumento de la capacidad de almacenamiento se pone de manifiesto en la cantidad de información que puede ser recogida y almacenada, así como la velocidad con la que la misma puede ser analizada. Por otra parte, los avances en la conectividad del hardware, a través de las redes, aumentan el almacenaje y difusión de su contenido. Estos avances en el hardware han hecho posible, además, la creación y creciente establecimiento de empresas oferentes de información recopilada, analizada y correspondientemente agregada por ellas mismas.

Todo lo cual se ha desarrollado a través de los dispositivos de recopilación de datos, pasando de una generación analógica, simple y costosa, a una digital, especializada y barata con dispositivos ubicuos y comunes. Estas tendencias ponen de manifiesto, por un lado, el hecho de que cada dispositivo de hardware es un dispositivo de recopilación de datos y, por otro, el aumento de formas en que se utilizan las tecnologías de la información, tanto en la vida cotidiana como en la actividad profesional; pues, como dispositivo de red, los dispositivos de hardware avanzados se han convertido en un elemento importante para las interacciones sociales, para las transacciones financieras, y para la búsqueda y recopilación de información.

Con respecto al aumento de la interconectividad e ubicuidad, la expansión de la World Wide Web sigue desarrollándose a ritmo vertiginoso como mecanismo y fenómeno global para el intercambio y la búsqueda de información. Los ordenadores no se limitan a acceder en tiempo real a cantidades ingentes de datos almacenados en modo local, en sus discos duros y otros dispositivos de almacenamiento fijo o portátil, sino que están permanentemente conectados a la red. Así, junto con el aumento de la conectividad proporcionada por las redes, estas se han convertido en potentes mecanismos para el intercambio de datos. Además, la cantidad posible de datos transferidos por la red en un momento dado, o en otras palabras el ancho de banda, ha ido en aumento de forma exponencial.

Ya en el 2009, la humanidad había alcanzado 0,8 Zettabytes (ZB) de almacenamiento digital, ahora debemos estar rondando los 5 ZB y está previsto que lleguemos a los 44 ZB en 2020; 1 ZB equivale a la capacidad de almacenamiento de 250 mil millones de DVDs.

Ni siquiera Google puede abarcar este desbordamiento de información, solo tienen indexados el 0,004% de todo el conocimiento disponible. Cuantificar esa “explosión de datos” con exactitud es imposible, pero sus fuentes son bien conocidas: teléfonos móviles, GPSs, automóviles, POS, clientes, Smart meters, redes sociales, RFIDs, “el Internet de las cosas” ¹(por ejemplo electrodomésticos conectados a Internet), etc.

La explosión de datos, también de datos personales, a la que estamos asistiendo, es más importante que la misma ley de Moore, en virtud de la cual se establece que, aproximadamente cada dos años, se duplica el número de transistores en un microprocesador, *“el uso de determinados servicios en Internet puede ser potencialmente lesivo [...] para nuestros derechos fundamentales”*. Dentro de este grupo debe señalarse, en primer lugar, a las redes sociales, que ofrecen medios de interacción entre los usuarios basados en los perfiles que estos

¹ <https://www.samsung.com/es/a-fondo/smart-home/que-es-el-internet-de-las-cosas/>

misimos generan, formándose comunidades de personas que comparten determinados intereses de tipo profesional o personal, sobre actividades o aficiones, etc. A la información personal publicada en línea por el propio usuario, debe añadirse la relativa a sus acciones e interacciones. Su combinación permite la obtención de un perfil muy preciso de sus intereses y actividades y estos datos, el resultado de su procesamiento, podrán ser utilizados con distintos fines, sobre todo comerciales y de publicidad, pero pueden también implicar riesgos para esa persona como la suplantación de identidad, mermas económicas o de oportunidades de empleo [...] o finalmente, pueden propiciar ataques a la integridad física y moral” (Garrida Domínguez, 2016).

Por lo tanto, la capacidad de los buscadores de poner a disposición de cualquiera, con relativa facilidad, información que contiene datos personales, “puede suponer una hipoteca para el honor, la intimidad y el libre desarrollo de la personalidad” (Simon Castellano, 2012).

3.2. El derecho a la protección de datos como “nuevo” derecho y nueva solución a los retos de las NTIC

La forma en la que la sociedad actual entiende la vida y el día a día ha cambiado radicalmente: ya no es significativo, ni mucho menos fácil, distinguir entre lo offline y lo online en un mundo que tiende a estar constantemente conectado e interconectado. A su vez, las informaciones que se introducen en la World Wide Web, no son filtradas por profesionales ni por un código deontológico (Córdoba Castroverde, 2016), convirtiendo Internet en un medio independiente, complejo, descentralizado, abierto, e ilimitado de información. En este sentido, Internet, dotado de un incontrolable cúmulo de datos, habilita la búsqueda inmediata, puesta a disposición y relación de información, así como la creación de perfiles personales, poniendo en peligro la salvaguardia de los derechos de las personas.

El desafío para el Derecho de regular estas nuevas situaciones y proteger de manera más efectiva los derechos relacionados con la intimidad y la vida privada se ve, de manera clara, con el auge de las nuevas tecnologías: *“en etapas anteriores, el respeto a la vida privada podía realizarse mediante el uso de los sentidos [...] permanecía así dentro de los límites de las relaciones naturales. Los muros de una casa, la soledad de un lugar desierto, incluso el tono expresivo oral del susurro, eran suficientes para asegurar la protección de la intimidad y para excluir el conocimiento y la difusión de las acciones y de las palabras de un individuo [...] hoy es posible observar y escuchar a distancia, sin límites de tiempo, de espacio o de modo [...] estas circunstancias, en especial la utilización masiva de la informática, han determinado que*

para la opinión pública y el debate político de nuestro tiempo constituya un problema nodal el establecimiento de unas garantías que tutelen a los ciudadanos de la agresión tecnológica a su intimidad” (Pérez Luño, 2012).

Así pues, nos encontramos que el refugio que suponían las paredes, las puertas y los pensamientos, a día de hoy, ha sido ametrallado por infinitos cables, señales WiFi, cookies, nubes, y un sinfín de innovadoras maneras de almacenar y difundir información.

Ha surgido la obligación del legislador y del juez-intérprete de dar respuestas adecuadas a los riesgos existentes para la protección de los derechos fundamentales de las personas en la era del imparable avance de las NTIC, y, como apuntan algunos autores, a los riesgos relativos a una “expropiación sin precedentes de la privacidad” (Sancho López, 2017, pág. 5) El derecho a la protección de datos de carácter personal. Este derecho se ha venido definiendo como el derecho de toda persona a tener un control sobre el uso de sus datos personales. Esta potestad de control permite evitar que, a través del tratamiento de datos de carácter personal, se pueda llegar a disponer de información que afecte a la intimidad y demás derechos fundamentales y libertades públicas. Esta creación y reinención, convertida, como no podía ser de otra manera, en un derecho fundamental, se presenta como instrumento indispensable para el libre desarrollo de la personalidad y para la defensa de su dignidad.

El derecho fundamental a la protección de datos viene generando amplia discusión académica en lo relativo a su alcance y aplicación. Existen autores que sostienen la premisa de que este derecho, en todas sus facetas y como derecho individual, está subordinado a derechos que además presentan una vertiente institucional o colectiva, como pueden ser la libertad de expresión o al derecho a la información (Tourinho, 2014, pág. 68) Otros, además, sostienen que existe una “hiperprotección” de la privacidad bajo la premisa de limitar y vigilar la libertad de información (Dader, 2012, pág. 2)

La facultad de actuación jurídica insertada en el contenido de otros derechos ya reconocidos, como el derecho al honor, la intimidad y la propia imagen (Jódar Marín, 2010, pág. 159)) ha servido de justificación para el posicionamiento jurídico y para la consagración de la naturaleza del derecho a la protección de datos como derecho enfrentado con las libertades de información. La UE, y sus desarrollos normativos y jurisprudenciales, han ejercido una indudable influencia en el desarrollo de este derecho fundamental (Plaza Penadés, 2014, pág. 17).

3.3. Normativa de la Unión Europea, tratados internacionales y legislación Estatal sobre el Derecho a la protección de datos de carácter personal

El camino hasta el reconocimiento de la protección de datos personales como un derecho fundamental, primero como extensión del derecho a la intimidad o a la vida privada y después con carácter autónomo, se ha desarrollado de forma paralela a la preocupación por los peligros que se cernían sobre el uso de dichos datos. A medida que esta evolución tecnológica se ha ido desarrollando, se ha ido haciendo más patente la necesidad de proteger a los titulares de los datos y de dotarles del control sobre los mismos.

En este proceso de consolidación del derecho ha sido determinante la interacción entre los ordenamientos internacional, europeo y nacional y de sus respectivas jurisdicciones.

a) Consejo de Europa

El artículo 8 del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950, consagra el derecho al respeto de la vida privada y familiar. Con el fin de preservar este derecho en relación con los datos personales, se adoptó el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, único instrumento internacional jurídicamente vinculante en este ámbito.

Este tratado, aun adoptado mucho antes de la era de Internet y las comunicaciones electrónicas, contiene los principios rectores de la protección de datos personales y ha servido de fuente de inspiración para la elaboración del acervo comunitario en la materia. Sirve de ejemplo la redacción primigenia de su artículo 5, dedicado a la calidad de los datos, que exige que los mismos se obtengan y traten leal y legítimamente; se registren para finalidades determinadas y legítimas, evitando su utilización de forma incompatible con dichas finalidades; sean adecuados, pertinentes y no excesivos en relación con tales finalidades; sean exactos y, si fuera necesario, actualizados; y se conserven durante un tiempo que no exceda del necesario para la consecución de las finalidades que justificaron su registro.

A partir del referido instrumento internacional, el Tribunal Europeo de Derechos Humanos ha construido una aquilatada doctrina en la que la noción de «vida privada» ampara toda información relativa a una persona física identificada o identificable. En esta mutua interacción entre ordenamientos destaca la aprobación por el Comité de Ministros del Consejo de Europa en su 128ª sesión, celebrada el 18 de mayo de 2018 en Elsinor (Dinamarca), del Protocolo modificativo del Convenio para la protección de las personas con respecto al tratamiento

automatizado de datos de carácter personal (que ha dado lugar al conocido como Convenio 108 +), en el que cabe constatar la influencia del RGPD.

b) Unión Europea

El derecho de toda persona a la protección de los datos de carácter personal que la conciernan se reconoce en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, proclamada solemnemente por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza, y el artículo 16 del Tratado de Funcionamiento de la Unión Europea, en la redacción procedente del Tratado de Lisboa, firmado el 13 de diciembre de 2007.

El primero de estos preceptos, dotado de carácter jurídicamente vinculante, al igual que el resto de la Carta, en virtud del citado Tratado de Lisboa, exige que los datos personales sean tratados de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley, sujetándose el respeto de estas normas al control de una autoridad independiente. Por su parte, el segundo precepto citado habilita al Parlamento Europeo y al Consejo para establecer, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho europeo, y sobre la libre circulación de estos datos.

Aunque la consagración en el Derecho originario de la protección de datos como derecho no tuvo lugar, por ende, hasta este siglo, ya en la última década del anterior se adoptó la norma precedente del RGPD, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

El Tribunal de Justicia de la Unión Europea fue sentando las bases para la protección de los derechos personales, dado que las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que pueden atentar contra las libertades fundamentales y, en particular, contra el derecho a la intimidad, *«deben ser interpretados a la luz de los derechos fundamentales que, según una reiterada jurisprudencia, forman parte de los principios generales del Derecho cuyo respeto garantiza el Tribunal de Justicia»* (Sentencia de 20 de mayo de 2003, asunto *Rechnungshof*). Los pronunciamientos de este órgano en la

materia han ido adquiriendo un mayor peso, sobre todo a la luz de las consecuencias que han tenido tres de ellos:

8. La Sentencia de 8 de abril de 2014 (asunto Digital Rights), que declaró inválida la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, al considerar que constituía una injerencia en los derechos fundamentales.
9. La Sentencia de 13 de mayo de 2014 (asunto Google), que, respaldando la posición de la Agencia Española de Protección de Datos, estableció los elementos determinantes del llamado derecho al olvido.
10. La Sentencia de 6 de octubre de 2015 (asunto Shrems), que declaró inválida la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Por consiguiente, esta resolución judicial anuló el acuerdo conocido como «puerto seguro» o «safe harbour» sobre la base del cual se venían legitimando las transferencias internacionales de datos desde la Unión Europea a los Estados Unidos de América.

El proceso de asentamiento del derecho a la protección de los datos personales en la Unión Europea ha culminado con la aprobación del RGPD, cuyo artículo 1.2 menciona la garantía de este derecho como objeto de la norma. Con ella se aspira a asegurar en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea (considerando décimo).

Se trata del primer derecho fundamental cuya regulación está encabezada por una disposición europea directamente aplicable con el carácter complementario de la legislación interna, en clara demostración de la fuerza expansiva del ordenamiento comunitario y del catálogo de derechos incorporado a su Derecho originario.

c) Derecho Español

La exposición de motivos de la Ley Orgánica de Protección de datos personales y garantía de los derechos digitales (LOPDGDD) subraya en su primer párrafo el carácter pionero de la Constitución española en el reconocimiento del derecho fundamental a la protección de datos personales cuando su artículo 18.4 dispuso que *«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»*. El desarrollo de este derecho fundamental se hizo esperar hasta la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, después reemplazada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, mediante la que se completó la transposición a nuestro ordenamiento jurídico de la Directiva 95/46/CE.

Dos pronunciamientos del Tribunal Constitucional marcaron las pautas para dotar al derecho resultante del artículo 18.4 de la Constitución de un contenido propio:

11. La Sentencia 254/1993, de 20 de julio, en dicho precepto *«nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama “la informática”»*.
12. Mayor precisión, a la hora de configurar este derecho e identificar sus diferencias con el derecho a la intimidad, se desprende de la Sentencia 292/2000, de 30 de noviembre. Razonó en ella el Tribunal Constitucional que la función del derecho fundamental a la intimidad del artículo 18.1 de la Constitución *«es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad»*, mientras que *«el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado»*.

La adopción del RGPD ha tenido, una incidencia directa en nuestro marco normativo. Ello ha situado una norma europea en la cabecera del grupo normativo regulador del derecho fundamental a la protección de datos personales. Con la función de adaptar nuestro ordenamiento al RGPD y de procurar la seguridad jurídica depurando las previsiones legales incompatibles con él, se hizo necesaria la aprobación de una nueva norma, la LOPDGDD, sustitutiva de la anterior Ley Orgánica 15/1999.

En resumen, los más exigentes estándares de garantía del derecho fundamental han sido alcanzados gracias a la «fertilización recíproca» de los ordenamientos internacional, europeo y nacionales.

3.4. Los fundamentos del derecho a la protección de datos y su relación con otros derechos análogos

La dignidad humana supone un valor básico y fundamentador de los derechos humanos que tienden a concretar y satisfacer las necesidades de la persona en la esfera moral (*Pérez Luño, 2010, p. 234*). Y es, justamente esta especial conexión entre los derechos de la esfera moral o de la persona y la dignidad humana (*Prieto Álvarez, 2005, p. 162*) la que ha hecho que la doctrina clásica haya clasificado algunos de ellos como “derechos de la personalidad”, incluidos el derecho al honor, el derecho a la imagen, el derecho a la intimidad, el derecho al respeto a la vida privada y el más reciente derecho a la protección de datos.

El TC se pronuncia con respecto a ello estableciendo que: *“la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás”; o que la intimidad, como derecho “estrictamente vinculado a la propia personalidad y que deriva, sin duda, de la dignidad de la persona humana [...] [supone] la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario según las pautas de nuestra cultura para mantener una calidad de vida humana”*. Lo que significa afirmar la pretensión genérica de reconocer al individuo unos derechos que le corresponden por el mero, pero significativo, hecho de ser persona.

La consideración de la dignidad como fundamento principal de derechos personalísimos comporta una doble garantía para la persona: una garantía negativa que asegura que no deberá ser objeto de intromisiones y una garantía positiva que permita *“la preservación de la intimidad”* como *“punto de apoyo para el pleno desarrollo de la personalidad del individuo”*.

El entendimiento de la fundamentación de la protección de datos requiere un obligatorio acercamiento al derecho a la intimidad, el cual ha experimentado un desarrollo relativamente paralelo al del progreso tecnológico.

Se habla de la intimidad, en su sentido más objetivo, como el núcleo o la parte más interior que guarda la persona, dentro de un conjunto de esferas que cada individuo configura según su voluntad. Entendiendo la intimidad, en un sentido más subjetivo, como el derecho de autodeterminación informativa, a través del cual, la persona determina lo que debe o no debe quedar reservado al conocimiento genérico.

Los derechos personalísimos hacen referencia primariamente a un espacio específico de libre disposición individual para el libre desarrollo y configuración de la personalidad, lo que, inexorablemente, conlleva concretar una cierta potestad de control: *“la libertad informativa representa una nueva forma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del right of privacy [...] sino que consiste también en la libertad de informarse, es decir, de ejercer un control autónomo sobre los datos propios, sobre la propia identidad informática”* (Frosini, 1988, p. 23). No obstante, es una indudable verdad que la libertad, en una era como la digital, se ve coartada por el empleo de técnicas informáticas (ya sea de control individual o colectivo) que comprometen o menoscaban gravemente su práctica, en particular aquellas relativas al tratamiento de datos de carácter personal: *“el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de las personas provenientes del uso torticero del tratamiento automatizado de datos personales”* (Garriga, 2000, p. 305). La necesidad de revisar y reconocer derechos fundamentales viene dada, entre otras razones, por el progreso técnico, como remedio para evitar la indigencia de la persona (Bobbio, 1991, p. 18).

En efecto, debido a la revolución tecnológica y digital, vivimos en un mundo acompañado de una constante creación, almacenamiento e intercambio masivo de datos, en muchas ocasiones de carácter personal, que construyen identidades digitales y un cuerpo “electrónico” inseparable del cuerpo físico de la persona (Rodotà, 2014, p. 151).

El derecho a la protección de datos también se nutre del derecho a la intimidad (en este caso intimidad “informática”). El concepto de intimidad se identifica con un ámbito de plena disponibilidad por parte del individuo, siendo este el único que determina lo que debe o no quedar reservado del conocimiento general. No obstante, independientemente de la denominación por la que opte (derecho a la protección de datos personales, Habeas Data,

derecho a la autodeterminación informativa, libertad informática, etc.) los fundamentos de este “nuevo” derecho a la protección de datos de carácter personal lo que protege, originariamente, es la dignidad de la persona y se engloba en un ámbito de libertad individual (Rebollo, 2008, p. 40 y 101).

Así pues, con independencia de su denominación, vista su fundamentación, la protección de datos se puede definir como el derecho a mantener el control sobre las informaciones propias y a determinar las modalidades de construcción de la propia identidad y vida privada.

“Esta singularización del derecho a la protección de datos obedece a una pretensión clara, una mayor protección del individuo. A esta circunstancia hay que añadir [...] la respuesta del derecho a las posibilidades técnicas. Si como hemos visto aquellos prácticamente en cincuenta años han tenido una evolución vertiginosa, el derecho no ha tenido otro remedio que adecuarse a esta celeridad. Por ello, el derecho a la intimidad ha permanecido estable, sin modificaciones conceptuales, normativas o jurisprudenciales, significativas. Por el contrario, el derecho a la protección de datos es una de las áreas del derecho, y de forma concreta de los derechos fundamentales, más evolucionado, mejor normado y con más medios de garantía y protección, tanto a nivel estatal como europeo” (Rebollo Delgado, 2008, pág. 102).

El derecho a la protección de datos, se regula en el artículo 8 CDFUE como derecho autónomo y difiere de otro derecho protegido por la misma, el derecho a la vida privada (artículo 7 CDFUE). Justamente en esta distinción del articulado que lo regula encontramos la justificación de su autonomía e independencia. A pesar de que el artículo 8 CDFUE no define qué es el derecho a la protección de datos, sí que establece que toda persona tiene derecho a la protección de sus datos personales y asienta unos principios básicos para garantizar su protección.

En efecto, el concepto intimidad o privacy, en el que, según algunos autores, se podría insertar la protección de datos personales, *“exige una respuesta acorde a una sociedad avanzada en la que la intimidad no tiene sólo una faceta negativa o de abstención de injerencia de los poderes públicos. La protección de datos ha sido objeto de trato específico en la Carta de Niza, superando incluso el propio derecho al respeto de la vida privada y familiar que consagra en el Convenio de Roma, para contemplar una dimensión activa que se traduce en todo un haz de facultades que permitirían al sujeto titular del derecho ejercer el control y gobierno de sus propios datos personales, así como defenderlos ante autoridades independientes”* (Tur Ausina, 2006, pág. 229).

Efectivamente, parece no haber duda en que el objeto del derecho a la protección de datos es más amplio que el del derecho a la intimidad, ya que extiende su garantía no solo a la intimidad en su dimensión jurídicamente (constitucionalmente) protegida, sino también a aquellos derechos personalísimos análogos que pertenecen, de alguna manera u otra, al ámbito de la vida privada en la era actual, todos ellos unidos a la dignidad humana.

El derecho a la protección de datos de carácter personal representa el reconocimiento de un derecho que se desarrolla en el contexto de la revolución y evolución tecnológica. La intimidad, el honor, y, de manera más genérica la dignidad del individuo, deben ser resguardados de potenciales y posibles usos indebidos derivados del tratamiento de información personal almacenada electrónicamente que les vincula.

Los datos de carácter personal están definidos por el Derecho de la UE *“como toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”*

Lo que otorga el derecho a la protección de datos es el derecho a conocer quién, qué, cómo y hasta cuándo datos de carácter personal son recogidos, tratados, conservados, utilizados, y transferidos además del derecho a acceder, modificar, actualizar y solicitar su supresión en determinados supuestos. En otras palabras, el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre datos de carácter personal, mediante la posibilidad del interesado de decidir oponerse, permitir y establecer los límites del acceso y uso de los mismos. Hablamos de una suerte de autodeterminación informativa reforzada y ampliada con el fin de dotar a los individuos de una cobertura jurídica, con una suerte de instituto de garantía (Serna Bilbao, 2011, p. 7), frente a los riesgos que supone el tratamiento de los datos de carácter personal para la dignidad de la persona.

Naturalmente, existen diversos derechos ligados y en juego dentro del prisma del procesamiento y la protección de datos personales, entre ellos, la libertad de expresión, el derecho de información, el derecho a la propiedad privada, la libertad de empresa y el derecho a un recurso efectivo, entre otros. Dado que todos los derechos reconocidos por la CDFUE tienen el mismo rango, la prevalencia absoluta de uno sobre el otro sería inaceptable, pues no existe supremacía

entre derechos. Así, la propia CDFUE ha aclarado que el derecho a la protección de datos, al igual que la libertad de expresión o cualquier otro derecho, no constituyen una prerrogativa exclusiva y deben ser considerados desde la perspectiva de su función social, y por ende, podrán ser limitados si se reúnen ciertas condiciones. Así pues, existen límites para ambos en función, básicamente, del examen exhaustivo del principio de proporcionalidad.

En este sentido, el TJUE se ha encargado de analizar y examinar en qué casos y bajo qué condiciones se pueden limitar unos derechos y otros. En el caso del derecho a la protección de datos frente a la libertad de expresión, tanto el Derecho derivado como las interpretaciones y aclaraciones del TJUE han establecido limitaciones al primero a través de conceptos como el “interés general” o “con fines periodísticos” y al segundo a través de consideraciones tales como la necesidad de cautela para prevenir vulneraciones serias a la identidad persona.

a) Protección de Datos y Libertad de Expresión

Es necesario recordar que el derecho fundamental a la libertad de expresión está enunciado en el artículo 11 de la Carta de Derechos Fundamentales de la Unión Europea, bajo el título “Libertad de expresión y de información”, en los siguientes términos:

“1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

.2. Se respetan la libertad de los medios de comunicación y su pluralismo”.

Ya por lo que se refiere a la jurisprudencia, el Tribunal de Justicia se ha manifestado, entre otras, en una de las más importantes sentencias de las que en materia de protección de datos ha dictado, no solo por ser de las primeras sino también por las apreciaciones hechas en la misma, que con posterioridad van a ser citadas en otras sentencias del propio Tribunal de Justicia, además de en las conclusiones de los abogados generales. Nos referimos a la Sentencia de 6 de noviembre de 2003, caso *Lindqvist*, asunto C – 101/01.

En este caso, la Sra. Lindqvist desempeñaba funciones de catequista en la parroquia de Alseda (Suecia). Hizo un curso de informática en el que, entre otras cosas, tenía que crear una página web en internet. A finales de 1998, la Sra. Lindqvist creó, en su domicilio y con su ordenador personal, varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaran.

A petición suya, el administrador del sitio Internet de la iglesia de Suecia creó un enlace entre las citadas páginas y dicho sitio. Las páginas web de que se trata contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre completo o, en ocasiones, solo su nombre de pila. Además la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional.

Asimismo, señalo que una de sus compañeras se había lesionado un pie y se encontraba en situación de baja parcial por enfermedad. La Sra. Lindqvist no había informado a sus compañeros de la existencia de estas páginas web, no había solicitado su consentimiento, ni tampoco había comunicado su iniciativa a la Datainspektion (Organismo público para la protección de los datos transmitidos por vía informática). En cuanto supo que algunos de sus compañeros no apreciaban las páginas web controvertidas, las suprimió. El Ministerio fiscal inició un proceso penal contra la Sra. Lindqvist por infracción de la Ley sueca de Protección de Datos (*Personuppgifslag, SFS 1998, núm. 204, en lo sucesivo "PUL"*) y solicitó que se le condenara por:

- Haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito a la Datainspektion (artículo 36 de la PUL);
- Haber tratado sin autorización datos personales delicados, como los relativos a la lesión de un pie y a la baja parcial por enfermedad (artículo 13 de la PUL);
- Haber transferido datos de carácter personal a países terceros sin autorización (artículo 33 de la PUL).

La Sra. Lindqvist reconoció los hechos, pero negó que hubiera cometido una infracción. El EKJO TINGSRATT (Suecia) la condenó al pago de una multa; la Sra. Lindqvist recurrió en apelación esta resolución ante el órgano jurisdiccional remitente.

Dado que albergaba dudas sobre la interpretación del Derecho comunitario aplicable al caso, en concreto, de la Directiva 95/46/CE, el órgano jurisdiccional decidió suspender el procedimiento y plantear al Tribunal de Justicia diversas cuestiones prejudiciales. En particular, la sexta cuestión era del siguiente tenor:

“¿Puede considerarse en un caso como el presente que las disposiciones de la Directiva 95/46 implican una restricción contraria al principio general de libertad de expresión, o a otras libertades y Derechos vigentes en la Unión Europea y que tienen su equivalente, entre otros,

en el artículo 10 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales?”.

Lo que se plantea es si la Directiva 95/46, en sí misma, implica una restricción al derecho a la libertad de expresión. Para realizar una ponderación de los diferentes derechos e intereses, existen disposiciones en la propia Directiva y deben tenerse en cuenta asimismo las disposiciones nacionales.

En cuanto a la propia Directiva 95/46/CE, sus disposiciones, han de ser relativamente generales, dado que deben aplicarse a un gran número de situaciones muy distintas. Por tanto, el justo equilibrio entre los derechos e intereses en juego debe buscarse en el ámbito nacional, al aplicar a los casos concretos la normativa que adapta el Derecho interno a la Directiva 95/46/CE. En consecuencia, el Tribunal estima que las disposiciones de la Directiva no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión o a otros derechos y libertades vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 CEDH.

Admitido lo anterior, el Tribunal declara que *“incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los Derechos e intereses en juego, incluidos los Derechos fundamentales tutelados por el ordenamiento jurídico comunitario”*. Para ello deberán tener en cuenta los criterios que se encuentran en la propia Directiva al establecer *“normas que determinan en que situaciones y en qué medida es lícito el tratamiento de datos personales y cuál es la tutela que debe dispensarse”*, así como las disposiciones que garantizan la adaptación del Derecho interno a dicha Directiva.

“Es cierto – continua el Tribunal – que los Estados miembros disponen en muchos aspectos de un margen de apreciación para adaptar su Derecho interno a la Directiva 95/46. No obstante, nada permite considerar que el régimen que establece esta carezca de previsibilidad o que sus disposiciones sean, por sí mismas, contrarias a los principios generales del Derecho comunitario y, en particular, a los Derechos fundamentales que tutela el ordenamiento jurídico comunitario. Por tanto, el justo equilibrio entre los Derechos e intereses en juego debe buscarse más bien en el ámbito nacional, al aplicar los casos concretos la normativa que adapta el Derecho interno a la Directiva 95/46”.

b) Naturaleza y alcance de la Directiva 95/46/CE

Asimismo, en la sentencia de 6 de noviembre de 2003, caso Lindqvist, en su séptima cuestión, el órgano jurisdiccional remitente preguntaba, en esencia, si los Estados miembros pueden establecer una protección más rigurosa de los datos personales o un ámbito de aplicación más amplio que los que resultan de la Directiva 95/46/CE.

Las posiciones de las partes intervinientes en el recurso fueron muy dispares. El Gobierno sueco señaló que la Directiva 95/46/CE no se contenta con fijar requisitos mínimos para proteger los datos personales. En su opinión, los Estados miembros, al adaptar su Derecho interno a dicha Directiva, están obligados a alcanzar el nivel de protección que determina esta última y no pueden establecer ni una protección más rigurosa ni una protección menor.

Sin embargo, el Gobierno holandés sostuvo que la Directiva 95/46 no se opone a que los Estados miembros establezcan una protección más rigurosa en algunos ámbitos. Además, los Estados miembros son libres de aplicar igualmente los principios de la Directiva 95/46 a actividades que no están comprendidas en el ámbito de aplicación de esta última. En fin, la Comisión alegó que un Estado miembro no puede establecer una protección más rigurosa de los datos personales o un ámbito de aplicación más amplio que los que resultan de la citada Directiva.²

El Tribunal de Justicia, partiendo del texto de los considerandos octavo³ y décimo⁴ de la Directiva afirma que *“la armonización de las legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa. La Directiva 95/46 trata de asegurar la libre circulación de datos personales, garantizando al mismo tiempo un alto nivel de protección de los Derechos e intereses de las personas titulares de dichos datos”*. Es cierto, continua, *“que la Directiva 95/46 reconoce a los Estados miembros*

² Apartado 92 a 94.

³ *“Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones”*.

⁴ *“Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad”*.

un margen de apreciación en ciertos aspectos y que les permite mantener o establecer regímenes particulares para situaciones específicas tal y como demuestra un gran número de disposiciones. No obstante, dichas posibilidades deben emplearse tal y como dispone la Directiva y de conformidad con su objetivo, que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del Derecho a la intimidad”.

En cambio, concluye, “nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello”. En consecuencia, “las medidas adoptadas por los Estados miembros para garantizar la protección de datos personales deben atenerse tanto a las disposiciones de la Directiva 95/46/CE como a su objetivo, que consiste en mantener el equilibrio entre la libre circulación de datos personales y la tutela del Derecho a la intimidad. En cambio, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva 95/46 a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello”.

En conclusión, los Estados miembros son libres de adoptar y modificar el modelo institucional que consideren más adecuado para sus autoridades de control, si bien, deberán velar por que no se limite la independencia de la autoridad de control exigida por el artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46. Por lo tanto, una armonización completa no obsta a que los Estados miembros tengan reconocido un cierto margen de maniobra, siempre y cuando se garanticen las obligaciones establecidas en la Directiva 95/846/CE.

3.5. Ley de transparencia y criterio de interés público: conflicto protección de datos y el interés público

Partiendo del texto constitucional, el artículo 20.d) reconoce el derecho fundamental a *comunicar o recibir libremente información veraz por cualquier medio de difusión*, y el artículo 105.b) establece que *“la ley regulará 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”*. De este último precepto se deriva que el derecho de acceso del administrado a los registros públicos no es absoluto, sino que cede ante la preponderancia de otros intereses legítimos también merecedores de protección.

La transparencia es fundamental en un estado de derecho para que los ciudadanos puedan tener un conocimiento global de los asuntos públicos que redundan en su persona y en la sociedad en general, y poder decidir con libertad la identidad de sus dirigentes de entre las opciones posibles.

a) Normativa sobre Transparencia y Protección de Datos

La plasmación legal en nuestro ordenamiento jurídico del reconocimiento constitucional del derecho a la información vino a reflejarse inicialmente en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, resultando una regulación muy laxa, pues únicamente venía a reconocer el acceso de los ciudadanos a los archivos y registros públicos.

El desarrollo legal posterior vino motivado por directivas comunitarias que instaban a los estados miembros a procurar el acceso de los ciudadanos a la información y a la justicia en materia medioambiental, y a garantizar la reutilización de la información elaborada o custodiada por las Administraciones y organismos públicos. Posteriormente, en el año 2007, con la aprobación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, cuando se produjo el primer intento de instauración de la Administración electrónica, con el objeto de implantar la sociedad de la información en las relaciones entre particulares y entes públicos, y entre éstos entre sí.

Finalmente, la norma más reciente en materia de acceso a la información la constituye *la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno*, que regula el acceso de la ciudadanía a la labor de los servidores públicos, establece los principios éticos y de actuación de los miembros del gobierno, y plasma mecanismos de control para procurar el cumplimiento de la Ley.

De otro lado, una regulación legal más amplia que la ofrecida por la Ley 30/1992, de 26 de noviembre, del acceso de los ciudadanos a los registros públicos la constituye la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que nació con vocación de ofrecer a los ciudadanos la comunicación electrónica en sus relaciones con las Administraciones Públicas. Se trata de lograr la optimización de las relaciones ciudadano-Administración, posibilitando un acceso eficaz y dinámico del interesado, de cualquier interesado, independientemente de sus condicionantes territoriales, temporales, espaciales, intelectuales, físicos, psicológicos u otros.

Posteriormente, la referida ley fue objeto de desarrollo por el Real Decreto 1671/2009, de 6 de noviembre. Asimismo, conviene traer también a colación la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información en el sector público, que tuvo su origen en la Directiva comunitaria 2003/98 CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo.

Como regulación más reciente del reconocimiento legal de acceso de los ciudadanos a la información, la constituye la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que viene a perseguir, como así se refleja en su exposición de motivos y en el objeto de la ley, la publicidad de la actividad del sector público, el acceso de los ciudadanos a la información pública y la exigencia a los miembros del Gobierno y altos cargos de una buena conducta, con el efecto de aplicarles unas consecuencias al incumplimiento de sus obligaciones como garantes del buen gobierno.

En lo referente a los límites al principio de transparencia, es imprescindible mencionar la regulación legal del derecho a la protección de datos, íntimamente relacionado con el derecho a la intimidad de las personas, que por su naturaleza de derecho fundamental, se encuentra regulado por ley orgánica, en concreto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, habiendo sido objeto de desarrollo por el Real Decreto 1720/2007, de 21 de diciembre.

b) Transparencia. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

La Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (en adelante, LTAIPBG) nace con una vocación de procurar y acrecentar la transparencia en los asuntos de la cosa pública, tratando de facilitar en mayor medida el acceso del ciudadano a dicha información, procurándole, de este modo, una participación más efectiva en tales asuntos, así como, trata de garantizar dicha ley los principios del buen gobierno, al establecer un código de conducta a los miembros del Gobierno y altos cargos, de la misma forma, que unas consecuencias a su inobservancia.

La aplicación subjetiva de la Ley (artículo 2.1) se muestra amplia, pues incluye como sujetos destinatarios de la transparencia de la actividad pública, no sólo las Administraciones Públicas Territoriales (Administración General del Estado, Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla, así como, las entidades que integran la Administración Local), sino también la Administración Pública Institucional (entidades

gestoras y servicios comunes de la Seguridad Social, organismos autónomos, Agencias Estatales, entidades públicas empresariales, entidades y corporaciones de Derecho Público, sociedades y fundaciones públicas, así como asociaciones constituidas por los citados entes), estableciéndose también como sujetos destinatarios de la transparencia y por tanto, objeto de control, las instituciones de la Casa del Rey, el Congreso, el Senado, el Tribunal Constitucional, el Consejo General del Poder Judicial, el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en sus acciones sujetas a Derecho Administrativo.

Es clara la tendencia de la LTAIPBG a garantizar la publicidad de la actividad pública, extendiendo esa transparencia al concepto amplio de Administración Pública, pues se dilata su ámbito de aplicación subjetiva no sólo a la actividad de los gestores públicos pura y dura, sino también a la de órganos públicos decisores, consultivos o puramente representativos, acogiendo incluso dentro de ese aura de control a entes privados relacionados con la actividad pública, manifestando un claro propósito de no dejar vía alguna de escape al control.

Con respecto a los sujetos con derecho de acceso a la información, el artículo 12 menciona *todas las personas, en los términos previstos en el artículo 105. b) de la Constitución*, entendiendo por información pública (artículo 13), *los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones*. De lo anterior se deduce que cualquier información, expresada en cualquier formato, que emane de un organismo público en el ejercicio de sus funciones propias, es objeto de publicidad y el ciudadano puede acceder a ella.

Esa parece ser la regla general, si bien, en los preceptos que le suceden vienen a establecerse algunos límites. Así, el artículo 14.1 menciona los siguientes:

la seguridad nacional, la defensa, las relaciones exteriores, la seguridad pública, la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios, la igualdad de las partes en los procesos judiciales y la tutela judicial efectiva, las funciones administrativas de vigilancia, inspección y control, los intereses económicos y comerciales, la política económica y monetaria, el secreto profesional y la propiedad intelectual e industrial, la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión o la protección del medio ambiente. Pero incluso el apartado 2 de ese precepto viene a exigir la realización de un juicio de ponderación, pues la aplicación de tales límites se supedita al *objeto*

y finalidad de la protección y considerando las circunstancias del caso concreto, especialmente la concurrencia de un interés público o privado superior que justifique el acceso.

c) Jurisprudencia sobre Protección de Datos del Tribunal Europeo de Justicia

En el ámbito del Derecho Europeo, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como la Carta de los Derechos Fundamentales de la Unión Europea, han resultado objeto de variadas sentencias del Tribunal Europeo de Justicia.

En tales pronunciamientos judiciales, motivados principalmente por la aparición y cada vez mayor influencia de la tecnología en la transacción de la información, se han venido a sopesar intereses contrastados; el derecho a la intimidad y protección de los datos personales con el derecho de acceso a la información. Resulta destacable, a propósito del alcance de los límites al tratamiento automatizado de datos personales y del acceso por parte de terceros a esa información, la Sentencia del Tribunal de Justicia, (Gran Sala), de 13 de mayo de 2014, asunto C-131/12, Google Spain, S.L., Google Inc. y Agencia Española de Protección de Datos, Mario Costeja González, que declaraba la responsabilidad de los gestores de motores de búsqueda sobre el tratamiento de datos personales, concediendo al interesado la posibilidad de solicitar que la información de la lista de resultados vinculada a su nombre se retirara de su disposición al público, haciendo prevalecer ese derecho frente al *interés económico del gestor* y frente al interés público de acceso a esa información, justificándose, a sensu contrario, la intrusión en el derecho a la intimidad de aquellas personas con relevancia pública, sobre las que pudiera concurrir un interés público en acceder a la información relativa a las mismas.

d) Del Tribunal Constitucional

En cuanto al derecho a la intimidad, garantizado en el artículo 18.1 de la Constitución, ha sido predicado por el Tribunal Constitucional como un derecho producto de la dignidad de la persona, plasmado en el artículo 10.1 de la Constitución y que implica la garantía de la persona a salvaguardar *un ámbito de su vida propio y reservado frente a la acción y el conocimiento de terceros, sean éstos poderes públicos o simples particulares* (Sentencias del Tribunal Constitucional (en adelante, SSTC) 73/1982, 110/1984, 107/1987, 231/1988, 197/1991, 143/1994 y 15/1997, 70/2002, 10/2002, de 17 de enero, 185/2002, de 14 de octubre, 85/2003, de 8 de mayo, 127/2003, de 30 de junio; 189/2004, de 2 de noviembre, 159/2009, de 29 de junio o 93/2013, de 23 de abril). Traduce esa protección en un poder de disposición de que goza la

persona sobre los datos de su ámbito personal y familiar, que le habilita a mantenerlos protegidos de la injerencia de otros. También impide que los poderes públicos se conviertan en *fuentes de esa información* sin consideración de las necesarias garantías, teniendo la obligación de evitar daños consecuencia del acceso o transmisión ilícitos de dichos datos.

El derecho a la intimidad no sólo se predica en el sentido de evitar que personas ajenas accedan a la parte íntima que el individuo se reserva respecto de la interferencia de terceros, sino que también implica el impedimento al hecho de que ajenos puedan utilizar, transmitir y extender esos datos sin consentimiento del afectado (a tal efecto, *STC 173/2011, de 7 de noviembre* o *STC 241/2012, de 17 de diciembre*, que se remite a las *SSTC 98/2000, de 10 de abril* o *186/2000, de 10 de julio*).

Sin embargo, el derecho a la intimidad no tiene el carácter de absoluto, sino que se encuentra sometido a unos límites, marcados por los demás derechos fundamentales y bienes jurídicos garantizados por la Constitución (*SSTC 73/1982, 110/1984, 170/1987, 231/1988, 143/1994, 151/1997, STC 156/2001, de 2 de julio, 70/2002, de 3 de abril, 115/2013, de 9 de mayo*).

En este sentido, ha establecido la jurisprudencia constitucional elementos para delimitar la intromisión o no en el derecho a la intimidad, a saber, que concurra un *fin constitucionalmente legítimo* (*SSTC 37/1989, de 15 de febrero; 142/1993, de 22 de abril; 7/1994, de 17 de enero; 57/1994, de 28 de febrero; 207/1996, de 16 diciembre; 234/1997, de 18 de diciembre; 70/2002, de 3 de abril*); que la injerencia en el derecho esté contemplada en la ley (*STC 37/1989, de 15 de febrero, STC 7/1994, de 17 de enero, STC 95/1999, de 31 de mayo, STC 207/1996, de 16 de diciembre, STC 234/1997, de 18 de diciembre, STC 70/2002, de 3 de abril, STC 25/2005, de 14 de febrero*); que la entrometimiento en el ámbito de la vida privada constitucionalmente salvaguardada se acuerde en resolución judicial motivada (*STC 71/2002, de 3 de abril*); y que se garantice el principio de proporcionalidad, esto es, que la medida adoptada sea idónea para alcanzar el fin constitucionalmente legítimo perseguido con ella (juicio de idoneidad), que sea imprescindible al efecto (juicio de necesidad) y que sea proporcionada en sentido estricto (equilibrada, por implicar más beneficios para el interés general que perjuicios sobre otros bienes en conflicto) (*SSTC 66/1995, de 8 de mayo; 55/1996, de 28 de marzo; 270/1996, de 16 de diciembre; 37/1998, de 17 de febrero; 186/2000, de 10 de julio y 70/2002, de 3 de abril*).

En definitiva, el derecho a la intimidad se encuentra estrechamente relacionado con el derecho a la protección de datos, que ha definido el Tribunal Constitucional como un *derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona*

provenientes de un uso ilegítimo del tratamiento mecanizado de datos (SSTC 254/1993 y 11/1998) y define la *libertad informática* como un derecho a controlar los datos contenidos en un programa informático, que incluye evitar que esos datos sean utilizados para fines diferentes de aquel lícito que motivó su recopilación. Esa posibilidad de fiscalización se traduce en que de modo previo a la compilación y uso de datos personales se exija la aquiescencia del afectado, que éste sea informado sobre el fin dado a los datos, así como, incluye el derecho del individuo al acceso, rectificación y cancelación de esos datos (ATC 29/2008, de 28 de enero, que se remite a la STC 292/2000, de 30 de noviembre o STC 254/1993). A tal efecto, la citada STC 292/2000 declaró inconstitucionales el último inciso del apartado 1 del artículo 21 de la Ley 15/1999, al no establecerse en la ley los supuestos en los que podía consentirse la transmisión de datos entre Administraciones Públicas, pues quedaba esa decisión a la discrecionalidad del responsable del fichero, así como un inciso del apartado 1 del artículo 24, y su apartado 2, pues imponía como una de las limitaciones al derecho a la protección de datos, una mera decisión administrativa. (Expósito, 2019)

4. DERECHO AL OLVIDO, REDES SOCIALES Y NUEVAS TECNOLOGIAS

4.1. El régimen constitucional del derecho al olvido digital

Los problemas que plantean las nuevas tecnologías, han hecho permanentes y universalmente accesibles informaciones perjudiciales para la reputación de las personas. Consecuencia de ello se ha producido una reacción que ha empezado a plantear en el debate público la conveniencia de regular el «*derecho al olvido*», en este supuesto el ordenamiento jurídico intervendría para forzar lo que antes se producía de manera natural gracias al paso del tiempo y las dificultades prácticas para acceder y dar difusión a la información. La configuración del derecho al olvido comporta entonces la determinación de los preceptos constitucionales a los que puede vincularse, pero también una dimensión negativa, de restricción de los derechos que facilitan el acceso y la circulación de la información para dar garantía al derecho al olvido.

Es decir, el ciudadano tendría la posibilidad de exigir la supresión, ocultación o cancelación de determinada información o la constancia de hechos (no sólo datos personales, sino también noticias pasadas que puedan afectar al futuro de las personas) que han sido publicados —prensa, boletines y diarios oficiales, resoluciones judiciales, etc. — en un determinado momento del pasado. Con ello lo que se pretende es encontrar un equilibrio entre todo lo que forma parte del ámbito de la vida privada de las personas —intimidad, honor, propia imagen, datos personales—, y lo que es público—contenido de las resoluciones judiciales—, con la

anonimización se busca una correcta ponderación entre dos bienes jurídicos constitucionalmente protegidos —vida privada y publicidad de la actuación de los poderes estatales—.

4.2. El Derecho a la Intimidad y su relación con otros derechos fundamentales

Nuestro ordenamiento jurídico contempla varias situaciones en las que se exige el olvido de hechos pasados, ya que su recuerdo supondría una hipoteca para el futuro de determinadas personas. Por ejemplo, los individuos que en el pasado delinquieron tienen un interés real y legítimo de cancelar sus antecedentes; un derecho a que se olvide su pasado para reintegrarse en la sociedad y edificar sin trabas su futuro. Con todo, la protección del olvido también se podría enmarcar dentro de los derechos, valores y principios que la CE recoge.

a) El art.- 10.1 CE y el libre desarrollo de la personalidad

La carta magna contiene valores, principios jurídicos y derechos fundamentales que inspiran todo el ordenamiento. La dignidad humana, recogida en el art. 10.1 de la norma suprema, supone la consagración constitucional de la protección de la dignidad de la persona, individualmente considerada, y de los derechos que le son inherentes, que son fundamentos del orden político y de la paz social. Precisamente, el libre desarrollo de la personalidad está incluido dentro del precepto constitucional que reconoce el valor dignidad personal:

«La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamento del orden político y de la paz social» (Art. 10.1 CE).

El TC ha entendido que no es casualidad que la dignidad humana esté contemplada en el art. 10 CE, al frente del título destinado a tratar los derechos y deberes fundamentales, buena muestra que el legislador constitucional la consideró *«como el punto de arranque, como el prius lógico y ontológico para la existencia y especificación de los demás derechos»*.⁵

El art. 10.1 CE reconoce la autonomía del individuo, su libertad de actuar y decidir libremente su proyecto vital, así como la posibilidad de alterarlo, modificarlo e innovarlo tantas veces como quiera, e incluso, no tenerlo. Así, el citado precepto recoge un bien jurídico que la carta magna pretende tutelar.

Para comprender cuál es el alcance del derecho al olvido, y determinar con exactitud cuál es el bien jurídico que se protege con el mismo. Hay que recordar que la dignidad humana tiene una

⁵ STC 53/1985, de 11 de abril, FJ 3.

conexión inextricable con los derechos de la personalidad, esto es, con el honor, la propia imagen, la intimidad y la protección de los datos personales. En concreto, el TC ha detallado que los derechos reconocidos en el art. 18 de la CE aparecen como «*derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda alguna de la dignidad de la persona que reconoce el artículo 10 de la CE*»⁶.

Así, los derechos de la personalidad que eventualmente se pueden ver afectados por el recordatorio constante de noticias pasadas, están enlazados intrínsecamente a la dignidad humana. De hecho, se les ha catalogado como derechos de libertad y autonomía⁷ (Alvarez Conde, 2003), porque fueron concebidos para garantizar una esfera reservada al individuo frente a la acción de los demás.

De este modo el derecho al olvido nace como un derecho a la autodeterminación informativa⁸ (P. Lucas Murillo, 2007), esto es, un derecho a tener el control sobre tus datos personales —habeas data—, a decidir cuáles pueden ser tratados y consultados por ojos extraños. La conexión del libre desarrollo de la personalidad con el derecho fundamental a la protección de datos es indudable.

Es indiferente si la información publicada en el pasado era pública o privada. En la hipótesis de divulgación de informaciones privadas que no se enmarcan dentro de los límites de las libertades informativas, su difusión y publicación, tanto en el pasado como en el presente, significaría una lesión de los derechos de la personalidad. Evidentemente, dependiendo del tipo de información privada, ésta podría suponer un daño al honor, a la intimidad, a la propia imagen o al derecho a la protección de datos personales.

El recuerdo constante de la información privada, además de afectar el libre desarrollo de la personalidad, también vulneraría los derechos de la personalidad. El bien jurídico protegido con

⁶ STC 231/1988, de 2 de diciembre, FJ 3.

⁷ Vid. por todos E. ÁLVAREZ CONDE: Curso de derecho constitucional: El Estado constitucional. El sistema de fuentes. Los derechos y libertades, Vol. I, 4a ed., Tecnos, Madrid, 2003, pág. 336.

⁸ «En ese empeño, no hay que olvidar que el derecho a la autodeterminación informativa es un derecho fundamental. Que se dirige a satisfacer una necesidad básica de toda persona: el control de la información que le concierne. Que no consiste en una exquisitez jurídica ni en un capricho, sino en una pretensión esencial en la sociedad en la que vivimos. Sin ese control, sin los límites que comporta para los poderes públicos y para los sujetos privados, ya sean los gobernantes, ya sean las empresas u otras entidades privadas, contarán no sólo con un conocimiento potencialmente pleno de la vida de cada uno de nosotros, sino que lo utilizarán para tomar decisiones que nos afectarán directa o indirectamente pero siempre de manera decisiva. El resultado será que estará en peligro el libre desenvolvimiento de nuestra vida e, incluso, nuestra propia identidad». P. LUCAS MURILLO DE LA CUEVA: «Perspectivas del derecho a la autodeterminación informativa», Revista Internet, Dret i Política, núm. 5 (2007): 18-32, pág. 30.

el derecho al olvido sería el libre desarrollo de la personalidad, que está recogido en el art. 10.1 de la carta magna.

Puede ubicarse el derecho al olvido, que se manifiesta en determinadas normativas —prescripción de los antecedentes penales⁹, anonimización de las sentencias— y puede derivarse implícitamente del art. 10.1 de la CE, esto es, de la dignidad humana y del libre desarrollo de la personalidad.

b) La Titularidad y la delimitación del contenido y los límites del derecho al olvido

El derecho al olvido se configuraría como un derecho subjetivo, de titularidad individual. Hay que especificar, sin embargo, que cuando se usa el vocablo «*persona*» se hace referencia a personas físicas, no a personas jurídicas, pues la dignidad de la persona recogida en el art. 10.1 de la CE hace exclusiva referencia a la dignidad del ser humano.

El contenido del derecho al olvido sobrepasaría el ámbito de protección de la vida privada, y comprendería el recuerdo de informaciones pasadas —hechos, noticias, vídeos, comentarios, etc.— que pueden afectar el futuro y el libre desarrollo de la personalidad, con independencia de si aquella información tiene carácter público o privado.

Por tanto resulta fundamental establecer cuáles son sus límites:

La eventual confrontación se daría entre el bien jurídico protegido por el derecho al olvido y las libertades informativas reconocidas ex arts. 20.1.a) y d) de la CE. La divulgación de información que contiene datos personales, a pesar de ser veraz, si no responde a un interés público, no está protegida por el art. 20.1 de la CE¹⁰.

Utilizando el mismo criterio que han establecido nuestros tribunales para la ponderación de las libertades informativas con otros derechos, la difusión de una información del pasado que pueda afectar el derecho al olvido, aunque sea veraz, no estaría protegida por el contenido del art. 20.1

⁹ Precisamente, en referencia al hecho que la difusión de los antecedentes penales afecta a la intimidad de las personas, J. M. ALVAREZ-CIENFUEGOS razona que «la definición de lo que constituye «la intimidad personal y familiar» se nos revela cada vez más amplia y más precisa, más rica de contenido y más próxima al ciudadano, amparando esferas de la personalidad hasta ahora desconocidas. Nace, por tanto, una nueva sensibilidad hacia espacios de la intimidad que aparecen vedados para la curiosidad ajena y reservados a lo que configura la construcción de la propia vida privada». J. M. ALVAREZ-CIENFUEGOS SUÁREZ, citado, págs. 4 y 5.

¹⁰ «Ninguna objeción puede hacerse a la finalidad que persigue el derecho a la libertad de información veraz, pero dicho derecho fundamental no es un derecho absoluto, sino que hay que ponerlo en relación con otros derechos fundamentales, como lo es en este caso, el derecho fundamental a la protección de datos al que se refiere la STC 292/2000, de 30 de noviembre de 2000». SAN (Sala Contenciosa) núm. 5062/2006, de 10 de noviembre de 2006, FJ 5.

de la carta magna. En cambio, el ejercicio de divulgar hechos pasados que gozan de una relevancia pública actual, se enmarcaría dentro de los límites de las libertades informativas, y el derecho al olvido decaería frente a estos¹¹.

- A modo de ejemplo el supuesto en el que un diario autonómico divulga una información relativa a Juan, alcalde de una ciudad capital de provincia, en la que se menciona que el mismo fue condenado hace quince años por un delito de tráfico de influencias, cuando era concejal de un pequeño municipio. Evidentemente, los hechos gozan de relevancia pública, porque el personaje ocupa un cargo público y la ciudadanía tiene un interés real en conocer esa información. Las libertades informativas harían decaer, en este caso, el derecho al olvido.

El contenido esencial del derecho al olvido estaría integrado por la garantía individual frente a la divulgación de hechos pasados, que no responden a un interés público actual, y que pueden condicionar el libre desarrollo del proyecto vital. Más concretamente, en referencia a informaciones contenidas en expedientes de antecedentes penales, indultos, sanciones administrativas, sanciones disciplinarias, resoluciones judiciales, concesiones de ayudas en casos de exclusión social y paro recibidas, las deudas pasadas y vencidas, etc. Aunque tengan la consideración de «hechos pasados» que pueden condicionar el libre desarrollo de la personalidad, el derecho al olvido tendría que decaer, en sentido general, en caso que los hechos comunicados se consideren de relevancia pública actual, hipótesis donde las libertades informativas prevalecerían.

4.3. La configuración del derecho al olvido digital

Hoy, las nuevas tecnologías, especialmente Internet, ponen al alcance de los ciudadanos plataformas en las cuales es posible transmitir información y acceder a la misma con facilidad. El procesamiento informático y la digitalización de la información contrastan con la fragilidad de la memoria humana. Por ejemplo, el efecto multiplicador de los motores de búsqueda web

¹¹ Un supuesto similar ocurre con la ponderación entre el derecho a la intimidad y las libertades informativas, un juicio en el que la veracidad es irrelevante: *«la exceptio veritatis carece de trascendencia en el ámbito del derecho a la intimidad, como sí la tiene en el del derecho al honor (...). Si se trata de intimidad, la veracidad de la información no excluye la ilegitimidad de la intromisión, pues la veracidad no sólo es irrelevante, sino que, por el contrario es presupuesto de la intromisión, y lo determinante de que la divulgación no sea ilegítima es únicamente la relevancia pública de los hechos íntimos divulgados, es decir, que su comunicación a la opinión pública, aun siendo verdadera, resulte ser necesaria en función del interés público del asunto sobre el que se informa, respecto de lo cual debe deslindarse el ámbito de lo público de lo que sólo suscita la curiosidad ajena»*. V. DEL CARPIO FIESTAS, pág. 9.

en relación a la constancia y visibilidad de los hechos pasados. En ese sentido, Internet puede significar el fin del olvido.

Este hecho ha desembocado en un debate que se ha producido tanto en los países que responden a la tradición jurídica civilista cómo a los que responden al common law. En Francia, un proyecto de Ley, que ya ha sido aprobado por el Senado pero que (todavía) no ha recibido la aprobación de la Asamblea, reconoce explícitamente la existencia de un derecho al olvido digital.

Lo que se pretende en Francia es dotar de mayor efectividad a este derecho, especialmente frente a las ingentes facultades que Internet otorga a los individuos, especialmente gracias a los buscadores, de acceder a información pasada que se perpetúa en las páginas web. Esta protección se enmarcaría dentro del derecho a la protección de datos personales, que exige que los mismos no puedan ser tratados sin consentimiento previo de su titular.

Además, estas preocupaciones son compartidas por la Comisión Europea, que prepara una iniciativa para limitar las potencialidades de la web, regulando un derecho al olvido que permita a los ciudadanos exigir a los proveedores de los servicios de Internet y a los buscadores web la eliminación de sus datos personales cuando estos dejen de ser necesarios para la finalidad con la que fueron recabados y publicados.¹²

- El derecho a la protección de datos de carácter personal (Art. 18.4 CE) como fundamento de la existencia de un derecho al olvido en internet

En España, la problemática ha aparecido a raíz de las quejas ciudadanas dirigidas a la AEPD, que ha exigido a los buscadores, especialmente a Google, que dejen de indexar informaciones que contienen datos personales, y que afectan a la dignidad personal de los individuos. En concreto, en la memoria de la AEPD del año 2009 se informa que:

« (...) en 2009 ha emergido una nueva preocupación para los ciudadanos, que se traduce en más solicitudes de tutelas de derechos ante la AEPD, en relación al derecho al olvido en Internet. En concreto, las solicitudes de ciudadanos pidiendo que se cancelen sus datos en páginas de Internet de diversa índole, u oponiéndose a que éstos sean recopilados y difundidos por buscadores de Internet se han incrementado un 200% en 2009, pasando de 18 en 2008 a 57 en 2009 (en 2007 se registraron tan sólo 3). Este dato revela que crece el interés de los

¹² Véase la noticia titulada «Bruselas quiere regular el ‘derecho al olvido’ en las redes sociales como Facebook», publicada en el diario 20 minutos, con fecha de 5 de noviembre de 2010, disponible en Internet: <http://bit.ly/aiwVSw> (17 de noviembre de 2010).

ciudadanos por evitar que sus datos aparezcan en los resultados de buscadores de Internet a partir de los datos identificativos de una persona»¹³.

Ante esta problemática, la AEPD ha recordado que los individuos no tienen que resignarse ni tienen que verse expuestos eternamente al tratamiento de sus datos personales, muchas veces contenidos en noticias del pasado que se mantienen perennes en la web, cuando las noticias o los hechos no tengan relevancia pública o no versen sobre un personaje público.

En este marco, la AEPD ha entendido que los ciudadanos pueden ejercer un derecho de oposición frente al tratamiento que los buscadores web realizan de los datos personales, es decir, además de la cancelación —la desindexación por parte de los motores de búsqueda de la información pasada—, se exige que el buscador encuentre medios para que la información no vuelva a aparecer en el futuro¹⁴. La protección del olvido en Internet ha sido enmarcada por la AEPD dentro del derecho fundamental a la protección de datos.

Hay que precisar que por «dato personal» se entiende cualquier información referente a personas físicas identificadas o identificables (art. 3.a) de la LOPD). Esta definición tan amplia¹⁵ de dato personal engloba toda aquella información que permite identificar a una persona: nombres y apellidos, el número del Documento Nacional de Identidad, la dirección física, la dirección de correo electrónico, la dirección IP, fotografías, vídeos, etc. O dicho en otros términos, toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquiera otro tipo susceptible de ser recogida, registrada, tratada o transmitida, y que permita la identificación de una persona física (art. 5.1.f) RLOPD).

En segundo lugar, por «tratamiento de datos personales» se entiende cualquier operación o procedimiento técnico de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación de datos (art. 3.c) de la LOPD).

Sin embargo no hay que olvidar el papel que juegan los motores de búsqueda web que indexan información que se encuentra disponible en la web, y por lo tanto, ponen al alcance de los

¹³Memoria de la AEPD correspondiente al año 2009, pág. 11, disponible en Internet: https://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2009/common/AEPD_memoria_2009.pdf (21 de junio de 2011).

¹⁴Vid. Resolución TD/00463/2007 de la AEPD.

¹⁵ «(...) la amplitud de esta definición facilita su adaptación a la constante evolución de la informática y permite hacer frente a uno de los peligros de ésta. En efecto, la acumulación de datos, su cruce, entrelazamiento, permite conocer, a partir de datos que aisladamente puedan parecer intrascendentes por no afectar a la intimidad, particularidades que pertenecen al ámbito protegido por la misma o que afectan al honor o estima de una persona». M. VIZCAÍNO CALDERÓN: Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas, Madrid, 2001, pág. 72.

ciudadanos un sistema para acceder, recoger, conservar y modificar información que eventualmente contiene datos personales, siendo perfectamente viable una interpretación que entienda que la actividad de los buscadores supone un tratamiento de datos personales¹⁶.

No hay daño al bien jurídico protegido por el art. 10.1 CE si no se puede identificar al individuo que se ve identificado por estos motores de búsqueda; no se puede lesionar su libertad de actuar ni su dignidad personal. Sin embargo, para que la legislación de protección de datos pueda proteger a los individuos de la divulgación de hechos pasados, hace falta que estos reciban un «tratamiento» acorde con la definición de la LOPD¹⁷.

Y la actividad que realizan los motores de búsqueda ha sido interpretada por la AEPD como un tratamiento de datos de carácter personal¹⁸. Por eso, el derecho al olvido digital estaría protegido por las garantías del derecho fundamental a la protección de datos; los individuos disfrutarían de los mecanismos de tutela recogidos en la LOPD frente toda información del pasado que contenga datos personales y esté sometida a un «tratamiento», siempre que su publicación no responda a un interés público actual.

La AEPD ha basado la existencia del derecho al olvido digital en dos principios recogidos en la LOPD:

- El primero es el principio del consentimiento del afectado, según el cual el tratamiento de datos de carácter personal exige el consentimiento inequívoco del afectado, a no ser que la ley disponga otra cosa —art. 6.1 LOPD—. Con ello se traspone el art. 7.a) de la Directiva 95/46/CE, que establece que *«los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si el interesado ha dado su consentimiento de forma inequívoca»*.
- El segundo principio que se invoca, el de finalidad¹⁹ establece que los datos personales serán cancelados cuando hayan dejado de ser necesarios para la finalidad

¹⁶ Vid. Resoluciones TD/01335/2008 y TD/00627/2009 de la AEPD.

¹⁷ «Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias». Art. 3.c) de la LOPD.

¹⁸ «Por ello, los afectados podrán ejercitar el mencionado derecho [al olvido] ante los buscadores, en cuyo caso concurren todos los requisitos necesarios para que atiendan tal petición». Informe 0214/2010 del Gabinete Jurídico de la AEPD, pág. 3, disponible en Internet: <http://bit.ly/eGO4Fw> (15 de marzo de 2011). Vid. también Resolución TD/01589/2008 de la AEPD.

¹⁹ El principio de finalidad se recoge por vez primera en el Convenio núm. 108 del Consejo de Europa. En concreto, el art. 5.e) del Convenio establece que los datos de carácter personal que sean objeto de un tratamiento automatizado *«se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado»*.

con la que se registraron (art. 4.5 de la LOPD). Más concretamente, el art. 4.5 de la LOPD establece que:

«Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados».

Así, se ha interpretado que el principio de finalidad permite que las informaciones pasadas, que contienen datos personales y están sometidas a tratamiento (por ejemplo, en un buscador web), se puedan cancelar desde el momento en que estos han dejado de ser necesarios a la finalidad por la cual fueron publicados. El derecho al olvido actuaría así como un instrumento que persigue el efectivo cumplimiento del principio de finalidad, que exige que los datos personales tan sólo se puedan utilizar para la finalidad concreta por la cual fueron registrados, y una vez ya no son necesarios a tal efecto se puede producir su cancelación. Se deduce, entonces, que la cancelación de los datos garantizaría el derecho al olvido digital.

4.4. Derecho al Olvido análisis Jurisprudencial

Al “derecho al olvido” se ha referido también el Tribunal de Justicia tanto en el caso Google Spain y Google, al analizar el alcance de la responsabilidad del gestor de un motor de búsqueda, en virtud de la Directiva 95/46/CE; como en el caso *Manni*²⁰, por lo que se refiere a su aplicación a datos personales publicados en el registro de sociedades.

Con respecto al caso Google Spain, este se inicia cuando el demandante, el Sr. Costeja, con fecha 5 de marzo de 2010, presento ante la Agencia Española de Protección de Datos (AEPD), una reclamación contra la Vanguardia Ediciones, S.L., un periódico de gran difusión, concretamente en Cataluña, y contra Google Spain y Google Inc., ya que cuando se hacía una búsqueda utilizando su nombre y apellidos a través del motor de búsqueda Google (“Google Search”), aparecían como resultados el anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social que en la actualidad ya se habían resuelto, de manera que la información carecía de relevancia.

Cabe mencionar, y considerar, también que el anuncio al que se hace referencia había sido publicado en dos ejemplares de la edición impresa del periódico de 1998, que posteriormente fueron digitalizados lo que hizo posible que estuvieran disponibles en internet.

²⁰ <https://legal.gruposca.com/inexistencia-derecho-al-olvido-mundo-empresarial/>

En concreto, lo que solicitada el Sr. Costeja era *“por un lado, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitaba que se exigiese a Google Spain o Google Inc, que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia”*.

La AEPD desestimo la reclamación contra La Vanguardia *“al considerar que la publicación que esta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores”*. Por el contrario, si estimo la reclamación contra Google Spain y Google Ins., considerando que *“quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información. La AEPD considero que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros. La AEPD estimo que este requerimiento puede dirigirse directamente a los explotadores de motores de búsqueda, sin suprimir los datos o la información de la página donde inicialmente está alojada e, incluso cuando el mantenimiento de esta información en dicha página esté justificado por una norma legal”*.

a) La sentencia de la Gran Sala del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo de 2014. Google Spain S.L. y Google Inc frente al ciudadano español Sr. Costeja González y la Agencia Española de Protección de Datos.

Con independencia de algunos pronunciamientos anteriores en orden a la aplicación de la Directiva 95/46/CE del Parlamento y el Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas respecto del tratamiento de datos personales y la libre circulación de estos datos y al art. 8 de la Carta de derechos fundamentales de la Unión Europea, se dicta una sentencia pionera y de gran calado, que ha producido una enorme repercusión en el ámbito de la protección de datos, la doctrina y la jurisprudencia relativas a dicho derecho.

La sentencia no es otra que la acordada por la Gran Sala del Tribunal de Justicia de la Unión Europea en fecha 13 de mayo de 2014. Dicha sentencia resuelve el litigio existente entre Google Spain S.L. y Google Inc frente al ciudadano español Sr. Costeja González y la Agencia Española de Protección de Datos, en cuanto esta última resolvió favorablemente la reclamación formulada por dicho Sr. contra los buscadores de internet a los que se ha hecho referencia y la empresa La Vanguardia Ediciones S.L. Se trata de una cuestión prejudicial que resuelve la sentencia.

El Tribunal considera que al explorar internet de manera automatizada, el gestor de los motores de búsqueda recoge los datos que extrae, registra y organiza posteriormente en el marco de sus programas de indexación, conserva en sus servidores, y en su caso facilita el acceso a sus usuarios en forma de lista de resultados de búsqueda. Y declara que dicha actividad tiene la consideración de “tratamiento de datos personales” cuando la información ofrecida contiene datos personales, y el gestor del motor de búsqueda debe considerarse responsable de dicho tratamiento en el sentido del art. 2, letra b) de la Directiva 95/46/CE.

Los puntos 72, 91, 92, 98 y 99 de la sentencia vienen a fijar las características del derecho al olvido, al que cita expresamente en el apartado 91, considerando que dicho derecho se define por las siguientes connotaciones:

1. Los datos personales pueden ser conservados solo de forma que permitan la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.
2. Un tratamiento inicialmente lícito de datos exactos puede devenir con el tiempo incompatible con la directiva 95/46/CE cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron.
3. El particular tiene derecho a que una información relativa a su persona ya no esté vinculada a su nombre por una lista de resultados obtenida en una búsqueda efectuada a partir de su nombre. Y ello aún en el caso de que la citada información no cause perjuicio al interesado (apartados. 96 y 99).
4. El derecho al olvido no prevalece en los supuestos en que la información pueda referirse al papel del interesado en la vida pública o se imponga su conservación con fines históricos, estadísticos o científicos.

De lo anterior, se deduce que el derecho al olvido se pueda definir como aquel que posee el particular para suprimir sus datos personales de los resultados obtenidos por los motores de búsqueda de internet, cuando el transcurso del tiempo hace innecesaria su conservación y dichos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron, salvo que posean un interés histórico, estadístico, científico o relativo a la vida pública del interesado.

A partir de esta sentencia, Google estableció un procedimiento de solicitud de retirada de resultados de búsqueda, también discutido, puesto que, por ejemplo, la retirada de enlaces solo se haría en búsquedas que incluyan el nombre del afectado, y no en búsquedas para otras palabras.

En el ámbito periodístico, algunos medios de comunicación en internet han comenzado a ensayar respuestas para garantizar el derecho al olvido, como es el caso del diario El País, en su libro de estilo, el cual señala que las informaciones archivadas y con acceso desde elpais.com que den cuenta de imputaciones, acusaciones o detenciones, encarcelamientos o condenas que hayan sido revocados por una decisión policial o judicial posterior, deberán contener una advertencia al respecto y un enlace con la última información disponible.

También dispone que nunca se procederá al borrado de archivos digitales de El País, pero se puede considerar la posibilidad de ocultar esa información en los buscadores de internet. Además la información debe haber sido publicada más de quince años atrás respecto del momento en que se reclama su borrado.²¹

b) La Jurisprudencia del Tribunal Supremo

La sentencia de fecha 5 de abril de 2016 de la Sala I de lo Civil del Tribunal Supremo en Pleno, (Recurso nº 3269/2014) que fija y resume la construcción del derecho al olvido, relacionándolo con el ordenamiento español se trata de la demanda formulada por un ciudadano contra Google Spain, Yahoo Iberia, S.L y Telefónica de España, S.A.U. en la que solicitaba se dictara sentencia que declarase que los demandados habían cometido una intromisión en el derecho a la intimidad personal y familiar, a la imagen y al honor del demandante y que se retirase igualmente la información personal de las indexaciones y cachés, en el cual consta publicado el Real Decreto 1396/1999, de 27 de agosto de 1999, por el que se indulta a Don Alfonso por un delito cometido en 1981; y que en adelante, se prohíban y cesen las citadas indexaciones.

Para la resolución de la cuestión planteada, razona el Tribunal Supremo que:

²¹ Véase: “Libro de Estilo de El País”. Madrid, Santillana 2014.

“Una vez transcurrido un plazo razonable, el tratamiento de datos consistente en que cada vez que se realiza una consulta en un motor de búsqueda generalista de Internet como es Google, utilizando datos personales, como son el nombre y apellidos de una determinada persona, aparezca entre los primeros resultados el enlace a la página web donde se publica el indulto que le fue concedido, deja de ser lícito porque es inadecuado para la finalidad con la que se hizo el tratamiento, y el daño provocado a los derechos de la personalidad del afectado, tales como el honor y la intimidad, resulta desproporcionado en relación al interés público que ampara el tratamiento de esos datos, cuando el demandante no es una persona de relevancia pública, ni los hechos presentan un interés histórico.”

Añade que “Hay que tomar en consideración que Internet es una herramienta de información y de comunicación con una enorme capacidad para almacenar y difundir información. Esta red electrónica, que comunica a millones de usuarios por todo el mundo, hace posible que la información sea accesible a millones de usuarios durante un tiempo indefinido. El riesgo de provocar daños en el ejercicio y goce de los derechos fundamentales y las libertades públicas, particularmente el derecho al respeto de la vida privada, que representa el contenido y las comunicaciones en Internet es enorme, y se ve potenciado por la actuación de los motores de búsqueda.”

En relación con la sentencia del TJUE razona que: “Como declara el apartado 80 de la STJUE del caso Google, el tratamiento de datos personales que realizan estos motores de búsqueda «permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate. Además, el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo».

Analizando el caso concreto acuerda que, el tratamiento, en el año 2010, de los datos personales del demandante con relación al indulto que le fue concedido en 1999 por un delito cometido en 1981, en un motor de búsqueda en Internet como es Google, una vez que el afectado requirió a Google Spain para que cancelara dicho tratamiento de datos, debe considerarse ilícito por

inadecuado y desproporcionado a la finalidad del tratamiento, a causa del plazo transcurrido desde que sucedieron los hechos a que se refiere el tratamiento de datos.

Transcurrido ese tiempo, el derecho a la información y el control de la actividad gubernamental justifica que esos datos puedan ser accesibles para una búsqueda específica, en la página web en la que se publican oficialmente los indultos, la del BOE, porque la posibilidad de investigar sobre la política de indultos llevada a cabo por el Gobierno, incluso en tiempos pasados, o comprobar si una persona que se presenta a un cargo público ha sido indultada en el pasado, reviste interés general y justifica la afectación de derechos de la persona indultada que supone tal posibilidad de búsqueda.

Pero no está justificado un tratamiento como el que realiza Google, que supone que cada vez que alguien efectúa una búsqueda con cualquier finalidad (elaboración de informes comerciales, selección para un puesto de trabajo, búsqueda por clientes, conocidos o familiares, del teléfono o de la dirección de una persona, simple cotilleo, etc.) aparezca entre los primeros enlaces el que informa sobre los hechos delictivos que cometió una persona en un pasado lejano, aunque sea indirectamente, a través de la información sobre el indulto que le fue concedido.

Ratifica la sentencia de la Audiencia dictada en segunda instancia manteniendo que la ponderación que ha realizado la Audiencia entre los derechos al honor, a la intimidad y a la protección frente al tratamiento de datos de carácter personal del demandante, y la libertad de información que ampara la obtención de información sobre la concesión de indultos por el Gobierno a personas condenadas por la comisión de delitos, ha sido adecuada.

La gravedad del daño que se le causa al afectado, que muchos años después todavía debe sufrir el estigma social de haber sido condenado por un delito, no encuentra justificación en el ejercicio de una libertad de información como la que supone la actividad de un buscador generalista de Internet, cuando el interés público de la información se ha visto considerablemente mermado por el transcurso de un extenso periodo de tiempo.

Se razona además que no puede exigirse al gestor de un motor de búsqueda que por su propia iniciativa depure estos datos, porque ello supondría un sacrificio desproporcionado para la libertad de información, a la vista de las múltiples variables que debería tomar en consideración y de la ingente cantidad de información objeto de procesamiento y tratamiento por esos motores de búsqueda (como podría desprenderse de la STJUE).

Pero sí puede exigírsele que dé una respuesta adecuada a los afectados que ejerciten sus derechos de cancelación y oposición al tratamiento de datos, y que cancele el tratamiento de sus datos personales cuando haya transcurrido un periodo de tiempo que haga inadecuado el tratamiento, por carecer las personas afectadas de relevancia pública, y no tener interés histórico la vinculación de la información con sus datos personales.

Contextualizando el derecho al olvido razona que: “El llamado derecho al olvido digital”, que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales (no le da en principio autonomía al derecho al olvido por tanto), no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos.

Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículum a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, “posicionando” a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones.

“Pero dicho derecho (el derecho al olvido) sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse a un tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad, inserción que se vería obstaculizada por el rechazo que determinadas informaciones pueden causar en sus conciudadanos.”

Otra cuestión que aborda la sentencia es la consideración de Google Spain S.L. como responsable del tratamiento de datos a los que se refiere el recurso, concluyendo que dicha sociedad es responsable, contradiciendo así las sentencias de la Sala de lo Contencioso Administrativo del Tribunal Supremo de fecha inmediata anterior (STS, Sala III de 14-03-2016), en sendos recursos interpuestos contra las sentencias dictadas por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, que a su vez resolvían los recursos interpuestos por Google Spain S.L. contra las resoluciones del Director de la AEPD y , en las

que la Sala de lo Contencioso- Administrativo del Tribunal Supremo estimaban la excepción de falta de legitimación pasiva alegada por Google Spain S.L.y que solo consideran como responsable a Google Inc. Radicada en EEUU.

Y razona también la Sala I, que el reforzamiento de los derechos de los ciudadanos frente a la intromisión en sus datos personales de los buscadores de internet, operado por la directiva 1995/46/CE quedaría carente de contenido si se hubiesen de instar procedimientos judiciales en países extranjeros muy alejados de España, con las dificultades y el coste que ello entrañaría, añadiendo que la sentencia del TSJUE Google vs AEPD y Mario Costeja, así lo determinaba.

Cabe mencionar que en España, los recursos presentados por Google Spain, respectivamente, contra la resolución de la Agencia Española de Protección de Datos y una sentencia de la Audiencia Provincial de Barcelona²², dio lugar a pronunciamientos dispares por las Salas de lo Civil y la Sala de lo Contencioso – Administrativo del Tribunal Supremo²³.

5. LOS DERECHOS EN PROTECCIÓN DE DATOS

5.1. Derechos ARCO

La denominación “Derechos ARCO” proviene de la reducción de las siglas de los cuatro derechos, en este caso derecho de acceso, de rectificación, de cancelación y de oposición. También existe el derecho de indemnización, si bien no se incluye en estas siglas porque su procedimiento se realiza como consecuencia del incumplimiento de alguna norma legal por parte del responsable o del encargado sobre los datos del propio interesado.

Como afirma Álvarez Hernando²⁴ las personas físicas titulares de sus datos personales, pueden ejercer ante el responsable del tratamiento, o ante el encargado de tratamiento, los derechos ARCO (acceso, rectificación, cancelación y oposición). Estos derechos guardan relación con el derecho de información previa, ya que cuando se obtengan datos del interesado, éste debe ser informado previamente de forma expresa, para así poder ejercer los derechos ARCO que crea convenientes.

²² Véase la Sentencia núm. 210/2016, de la Sala de lo Civil del Tribunal Supremo, de 5 abril de 2016, en virtud de la que “Google Spain puede ser considerada, en un sentido amplio, como responsable del tratamiento de datos que realiza el buscador Google Search en su versión española (www.google.es), conjuntamente con su matriz Google Inc., y está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten sus derechos de acceso, rectificación, cancelación y oposición, y exijan responsabilidad por la ilicitud del tratamiento de datos personales realizando por el buscador Google en su versión”.

²³ Véase la Sentencia núm. 574/2016, de la Sala de lo Contencioso Administrativo del Tribunal Supremo, de 14 de marzo de 2016.

²⁴ ÁLVAREZ HERNÁNDO, J. (2011), *Guía práctica sobre Protección de datos: Cuestiones y formularios*, Valladolid: LEX NOVA, pp. 199-201.

Además, estos derechos no son absolutos, ya que el artículo 25.7 del RLOPD establece que: *“El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes”*. Entendiendo por derecho absoluto, aquel derecho que pertenece a una persona y debe ser respetado por todos los demás.

Tanto la LOPD como el RLOPD, en su artículo 24, establecen que el ejercicio de los derechos debe realizarse de forma gratuita, quedando prohibida la exigencia de una contraprestación al interesado por parte del responsable o del encargado del tratamiento, a no ser que se trate de una excepción como establece el artículo 28.3 del RLOPD: *“Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección”*.

El artículo 23 de RLOPD establece cómo se ejercen los derechos y quien los ejerce en cada caso:

“1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que la misma actúa en representación de aquel”.

Por otro lado, el artículo 24 del RLOPD establece las condiciones generales que deben darse en todos los derechos para que se puedan ejercer correctamente:

“1.Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la LOPD, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aun cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente”.

Seguidamente la LOPD en su artículo 25 establece de forma general el procedimiento que se utilizará para ejercer los derechos. Consiste en un procedimiento igual para todos los derechos.

Y por último, el artículo 26 del RLOPD establece cómo debe actuar el responsable o encargado del tratamiento ante un interesado que solicite ejercer sus derechos. El artículo 26 dispone lo siguiente:

“Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición”.

5.2. Derecho de Acceso

El Tribunal de Justicia se pronunció sobre el derecho de acceso en su sentencia de 7 de mayo de 2009, caso RijKeboer. En este caso, que tiene por objeto responder una cuestión prejudicial planteada por el Raad van State de los Países Bajos, el Tribunal de Justicia tiene que interpretar, por primera vez, el artículo 12 de la Directiva 95/46/CE.²⁵

En este caso, la cuestión prejudicial se plantea en el marco de un litigio entre el Sr. RijKeboer y el College van burgemeester en wethouders van Rotterdam ya que este último había desestimado parcialmente una solicitud de acceso a la información presentado por aquel, con fecha de 26 de octubre de 2005, sobre sus datos personales comunicados a terceros durante los dos años anteriores a dicha solicitud. El motivo de la desestimación parcial de la solicitud hecha por el Sr. RijKboer era que los datos personales anteriores en más de un año a la fecha de la

²⁵ Dicho artículo es como sigue:

“Artículo 12. Derecho de acceso.

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

- a) Libremente, sin restricciones y con un periodicidad razonable y sin retrasos ni gastos excesivos:
 - La confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;
 - La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda información disponible sobre el origen de los datos;
 - El conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;
- b) En su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;
- c) La notificación a los terceros a quienes se haya comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.”

solicitud habían sido cancelados automáticamente, lo que implica que no pueda ejercerse el derecho de cancelación con respecto a los mismos.

En relación con lo anterior, el Raad van State presenta al Tribunal de Justicia la siguiente cuestión prejudicial sobre el artículo 12, letra a), de la Directiva 95/46/CE:

*“La limitación legal de la comunicación de datos al año anterior a la solicitud, ¿es compatible con el artículo 12 letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos y a la libre circulación, interpretando en relación con el artículo 6, apartado 1, letra e), de la citada Directiva, y con el Principio de proporcionalidad”?*²⁶

Al respecto, el Abogado General comienza sus conclusiones mencionando que *“los titulares de los datos tratados pueden velar por su buen uso, ejerciendo el llamado “derecho de acceso”.*” Y añade también que el *“derecho a la protección se estructura en el artículo 12, pues el acceso representa la auténtica dimensión subjetiva de la Directiva, que, en suma, permite al individuo reaccionar en defensa de sus intereses”.*²⁷

En concreto, el caso se centra en determinar si una vez borrados los datos *“por mandato de la Directiva 95/46, se cierra la puerta al derecho de acceso, pues no cabe pedir una información que ya no existe”.*²⁸

En su Sentencia, el Tribunal de Justicia analiza el artículo 12, letra a), de la Directiva 95/46/CE conforme a los objetivos de la misma. En lo esencial, el Tribunal de Justicia manifiesta que el *“citado derecho debe necesariamente afectar al pasado. De no ser así, el interesado no estaría en condiciones de ejercer eficazmente su derecho a exigir la rectificación, la supresión o el bloqueo de los datos que presume ilícitos o incorrectos, ni de interponer un recurso judicial y obtener la compensación por el daño sufrido”.*²⁹

Sobre el derecho de acceso, el Tribunal indica que se trata de una obligación de los Estados miembros *“de establecer que el responsable del tratamiento ha de dar a la persona afectada acceso a la información relativa a los destinatarios o categorías de destinatarios y a los datos comunicados, si dicho interesado decide ejercer el derecho de acceso que le confiere el artículo 12, letra a), de la Directiva”.*

²⁶ Apartado 29.

²⁷ Punto 29.

²⁸ Punto 16.

²⁹ Apartado 59.

Por lo que se refiere a este derecho de acceso, el Tribunal de Justicia concluye que *“el artículo 12, letra a), de la Directiva obliga a los Estados miembros a garantizar un derecho de acceso a la información sobre los destinatarios a quienes se comunican los datos y al contenido de la información comunicada, no solo para el presente, sino también para el pasado. Corresponde a los Estados miembros fijar un plazo de conservación de dicha información, así como el acceso correlativo a esta, guardando un justo equilibrio entre, por un lado, el interés del afectado en proteger su intimidad, concretamente a través de las distintas vías de intervención y de recurso previstas por la Directiva, por otro, la carga que la obligación de dicha información puede representar para el responsable del tratamiento”*.³⁰

Otra Sentencia sobre el derecho de acceso es la del caso Nowak, en la que el Tribunal de Justicia indica que el derecho de acceso *“es indispensable, en particular, para permitir al interesado obtener, en su caso, del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de esos datos y, en consecuencia, ejercer el derecho que se contempla en el artículo 12, letra b), de dicha Directiva”*.³¹

Aclara el Tribunal de Justicia que *“los derechos de acceso y rectificación, con arreglo al artículo 12, letra a) y b), de la Directiva 95/46/CE, no incluyen las preguntas del examen, que por su propia naturaleza no son datos personales del candidato”*.³²

El Tribunal se refiere también, por último, a los límites al derecho de acceso, estableciendo que el Reglamento general de protección de datos *“amplia la lista de los motivos de limitación, actualmente establecida en el artículo 13, apartado 1, de la Directiva 95/46 a “otros objetivos importantes de interés público general de la Unión o de un Estado miembro”*. Además, el artículo 15 del Reglamento 2016/679, que trata del derecho de acceso del interesado, establece en su apartado 4 que el derecho a obtener copia de los datos personales no afectará negativamente a los derechos y libertades de otros”.³³

Así mismo dentro de nuestra legislación, la Ley Orgánica de Protección de datos de carácter personal con respecto al derecho de acceso, establece en su articulado:

Artículo 15.1 qué es el derecho de acceso de la siguiente forma: *“El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a*

³⁰ Apartado 70.

³¹ Sentencia de 17 de julio de 2014, YS y otros, C – 141/12 y C – 372/12, EU:C: 2014:2081, apartado 41.

³² Apartado 58.

³³ Apartado 61.

tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos". Mientras que el 27.1 del RLOPD amplía un poco esta definición estableciendo el derecho de acceso como: *"el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos"*.

Por otra parte, la Agencia Española de Protección de Datos establece que *"el derecho de acceso es uno de los derechos que la LOPD reconoce a los ciudadanos para que el ciudadano pueda controlar por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a obtener información sobre si éstos están siendo objeto de tratamiento y, en su caso, la finalidad del mismo, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos"*.

5.3. Derecho de Rectificación

En relación con el derecho de Rectificación previsto en el artículo 12, letra b), de la Directiva 95/46/CE, el Tribunal de Justicia se ha pronunciado en el caso Nowak, antes mencionado, indicando que este derecho *"no permite obviamente a un aspirante ampararse en el para "rectificar" a posteriori las respuestas "incorrectas".*" Y señala también que, por lo que se refiere a este derecho, *"el carácter exacto y completo de los datos personales debe ser apreciado atendiendo a los fines para los que fueron recabados. En lo que se refiere a las respuestas de un aspirante en un examen, tales fines consisten en poder valorar la amplitud de sus conocimientos y competencias en la fecha del examen"*.

Esto determina, tal como explica el Tribunal, que *"tales errores no son en modo alguno una inexactitud, a efectos de la Directiva 95/46/CE, que legitime un derecho de rectificación con arreglo a su artículo 12, letra b)"*.

Y el Tribunal de Justicia afirma, que *"los derechos de acceso y rectificación, con arreglo al artículo 12, letra b), de la Directiva 95/46, no incluyen las preguntas del examen, que por su propia naturaleza no son datos personales del candidato"*. Y siendo una de las primeras sentencias que cita el Reglamento General de Protección de Datos, recuerda también que *"tanto la Directiva 95/46 como el Reglamento 2016/679, que sustituyó a dicha Directiva, establecen determinadas limitaciones a esos derechos"*.

Este derecho se encuentra definido en el RLOPD, en él el artículo 31.1 establece que: *“El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos”*.

Del mismo modo la AEPD establece que, el derecho de rectificación es un derecho que la LOPD reconoce a los ciudadanos para defender su privacidad controlando por sí mismos el uso que se hace de sus datos personales, y el derecho a que éstos se modifiquen cuando resulten inexactos o incompletos.

5.4. Derecho de Cancelación

La LOPD en el artículo 16, citado anteriormente, regula junto con el derecho de rectificación el derecho de cancelación, de modo que la regulación del derecho es la misma para ambos. En el apartado 3 del artículo se regula a que dará lugar el derecho de cancelación exclusivamente, estableciendo lo siguiente: *“La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”*.

El artículo 31 del RLOPD, a diferencia de la LOPD, sí que establece una diferenciación entre dos derechos, de este modo, el artículo 31.2 del RLOPD amplía lo regulado en el artículo 16 de la LOPD sobre el derecho de cancelación de la siguiente forma: *“El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento”*.

Ante las definiciones conjuntas de la LOPD de ambos derechos, el RLOPD en su artículo 5.1,b) define “cancelación” como “el procedimiento en virtud del cual el responsable cesa en el uso de los datos”. Y como consecuencia, ello implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

Por su parte, la AEPD establece que, de igual modo que el derecho de rectificación, el derecho de cancelación sirve para que los ciudadanos puedan defender su privacidad controlando por sí mismos el uso que se hace de sus datos personales, con la diferencia de que en el derecho de cancelación se puede solicitar la eliminación de los datos cuando sean inexactos o excesivos.

5.5. Derecho de Oposición

En la LOPD no se regula en que consiste el derecho de oposición, solamente se regula en el artículo 17 el procedimiento para ejercerlo. Es el RLOPD el que en el artículo 34.1 expone en que consiste el derecho de oposición, regulándolo como:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento”.

La AEPD, igual que el reglamento, define el derecho de oposición, como un derecho que se utiliza para que, según la LOPD, en primer lugar, no se lleve a cabo el tratamiento de los datos personales o para que se cese este tratamiento de datos cuando no sea necesario el consentimiento del afectado para el tratamiento por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.

También se podrá ejercer cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial. Y por último, cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y esté basada en un tratamiento automatizado de sus datos de carácter personal.

5.6. Derecho de Indemnización

El derecho de indemnización solamente se regula en la LOPD, en el RLOPD no se hace ningún tipo de referencia a este derecho. En la LOPD encontramos el derecho de indemnización en el artículo 19.1, en él se regula cuando existe derecho de indemnización de la siguiente manera:

“Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados”.

Como indica la AEPD las indemnizaciones tendrán lugar de dos formas distintas; en primer lugar, cuando se trate de un fichero de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. Y en segundo lugar, si se trata de ficheros de titularidad privada, el derecho se ejercerá ante los órganos de la jurisdicción ordinaria. Hay que añadir que la AEPD no tiene capacidad para establecer la cuantía de la indemnización.

6. CONCLUSIONES

Bienes jurídicos como la privacidad (art. 18 CE), la libertad de expresión (Art. 20 CE), el libre desarrollo de la personalidad (Art. 10 CE) y más recientemente y debido al desarrollo digital sin precedentes que vivimos, ha surgido la así llamada *huella digital* de la mano del derecho a la supresión (Art. 17 RGDP) más conocido como al olvido, es decir, al anonimato digital, todos ellos íntimamente vinculados con el Derecho a la protección de datos de carácter personal (Art. 8 CDFEU) y (Art. 1 LOPDGDD) han sido bienes que se han visto vulnerados debido al boom tecnológico, *la cuarta revolución industrial*, hecho que ha ido de la mano del desarrollo sin precedentes del internet, a través de la cual estamos constantemente interconectados, esto ha supuesto la ruptura de varios muros sociales, ideológicos, culturales, comunicativos, y el avance de la humanidad así como el desarrollo en la protección de los derechos y la modernización de las Leyes Internacionales, Comunitarias y Estatales.

Se nos ha abierto un mundo nuevo donde la información es “gratis”, pero también ha supuesto una intromisión y en muchos casos violación de nuestros derechos más personales. Por ejemplo para poder acceder a una red social su precio justo supone la entrega de nuestros datos personales, de igual manera si deseamos adquirir un producto que esté de moda a través de la Web el primer paso es la aceptación de recopilación de nuestros datos.

La tendencia es a que este desarrollo tecnológico siga en auge, de hecho muchos sitios de importancia como periódicos, entes públicos, empresas de renombre, ya se encuentran posicionadas en la nube, han apostado por la digitalización completa de toda su información, el ejemplo más claro han sido los medios de comunicación escritos, que han traspuesto toda la información recabada en los últimos 40 o 50 años a disposición de los usuarios, esto es beneficioso, pero también es perjudicial, porque el hecho de encontrarse esta información al alcance de todos con un simple clic, puede suponer y de hecho ha supuesto el conocimiento de información delicada por desconocidos así como la violación de derechos fundamentales, que

además han entrado en conflicto con otros de la misma índole – derecho a la protección de datos vs libertad de expresión –.

Llegados a este punto la Comunidad Europea y España han sido pioneros en la regulación y protección de todos los derechos ligados a la privacidad del sujeto legislando y reconociendo como derecho fundamental el Derecho a la protección de datos de carácter personal y estableciendo y adecuando mecanismos de protección ya existentes como los denominados Derechos ARCO.

Es claro que este desarrollo continuara y por tanto la Ley deberá ir modernizándose a la par de este progreso con el objetivo final de preservar y proteger la privacidad de las personas en un mundo donde cada vez esta tarea es más difícil.

6. BIBLIOGRAFÍA

- Acquisti, A. T. (2016). "The economics of privacy".
- Alfonso Galan Muñoz, M. A. (2014). *La Protección Jurídica de la intimidad y de los datos de carácter personal frente a las Nuevas tecnologías informáticas y de la comunicación*. Tirant Lo Blanch - Derecho y TIC'S.
- Alvarez Conde, E. (2003). *El Estado Constitucional. El sistema de Fuentes. Los Derechos y libertades*. Madrid: Tecnos - Vol. I, 4ed.
- Carbonell, M. (2016). *La Vida en línea: el impacto de las redes sociales en todo lo que hacemos*. Tirant Lo Blanch.
- Castellano, P. S. (2012). *El Régimen Constitucional del Derecho al Olvido Digital*. Tirant Lo blanch.
- Córdoba Castroverde, D. y.-G. (2016). Reflexiones sobre los retos de la Protección de la privacidad en un entorno tecnológico. En *En cuadernos y debates Nº248: El derecho a la privacidad en un nuevo entorno tecnológico* (págs. 99 - 110). Madrid: Centro de Estudios Políticos y Constitucionales .
- Dader, J. L. (2012). La privacidad como excusa para restringir la información de interés público. *Revista general de Derecho Constitucional*, 2.
- Expósito, G. M. (9 de mayo de 2019). *elderecho.com*. Obtenido de <https://elderecho.com/transparencia-versus-proteccion-de-datos-i>: <https://elderecho.com/transparencia-versus-proteccion-de-datos-i>
- Garrida Dominguez, A. (2016). Nuevos retos para la protección de datos personales en la era del Big Data y la Computación ubicua. Madrid: Dykinson.
- Gayo, J. L. (2018). *El Derecho a la protección de datos en la Jurisprudencia del Tribunal de Justicia de la Unión Europea*. Wolters Kluwer - La Ley.
- Jódar Marín, J. Á. (2010). La era digital:nuevos medios, nuevos usuarios y nuevas profesiones. *Razón y Palabra Revista Electrónica en América Latina especializada en comunicación*, 159.
- P. Lucas Murillo, d. I. (2007). Perspectivas del Derecho a la autodeterminación informativa. *Revista internet, Dret i Política nº5* , 18 - 32.
- Pérez Luño, A. -E. (2012). Los Derechos Humanos en la sociedad Tecnológica. Madrid: Universitas.
- Plaza Penadés, J. (2014). Doctrina del Tribunal de Justicia de la Unión Europea sobre protección de datos y derecho al olvido. *Revista Aranzandi de derecho y nuevas tecnologías*, 17.
- Rebollo Delgado, L. S. (2008). Introducción a la Protección de Datos . Madrid: Dykinson S.L.
- Sáez, M. M. (2018). *Una revisión del derecho fundamental a la protección de datos de carácter personal*. Tirant Lo Blanch.
- Sancho López, M. (2017). Nuevas amenazas para la Protección de datos en el contexto del Big Data. *Revista Aranzandi de Nuevas tecnologías*, nº43, 1-21.
- Simon Castellano, P. (2012). *El Régimen Constitucional del Derecho al Olvido Digital*. Valencia: Tirant Lo Blanch.
- Touriño, A. (2014). El derecho al olvido y a la intimidad en internet. Madrid: Los libros de la Catarata.

Tur Ausina, R. (2006). "Cooperación en materia de terrorismo, transferencia de datos personales y privacidad. *Revista Europea de Derechos Fundamentales*, 229.

Waldo, J. L. (s.f.). *Engaging Privacy and information Technology and Digital Age*. Obtenido de (Whashington D.C. Nation Academic press:
<http://people.csail.mit.edu/rivest/pubs/WLM07.pdf>