FACULTAD DE LAS CIENCIAS SOCIALES, JURÍDICAS Y DE LA COMUNICACIÓN.

Campus María Zambrano, Segovia.

GRADO EN DERECHO

TRABAJO DE FIN DE GRADO:

"EL DERECHO AL OLVIDO DIGITAL"

AUTORA: Helena Martin del Valle.

TUTORA: Isabel Palomino Díez.

CURSO ACADÉMICO 2019/2020.

RESUMEN.

El objeto del presente trabajo es conocer la regulación de la protección de los datos personales, sus principios inspiradores, así como la evolución de la normativa en esta materia, tanto a nivel nacional como europeo, centrándonos en el reconocimiento del derecho al olvido digital derivado de la llegada de Internet, su conexión con otros derechos personalísimos y su construcción jurisprudencial. Se realizará también un estudio detallado de la sentencia que reconoció por primera vez el derecho al olvido digital.

PALABRAS CLAVE.

Indexar, calidad de los datos, derechos ARCO, protección de datos, tratamiento automatizado.

ABSTRACT.

The purpose of this work is to know the regulation of the protection of personal data, its inspiring principles, as well as the evolution of regulations in this area, both at national and European level, focusing on the recognition of the right to digital oblivion derived from the arrival of the Internet, its connection with other very personal rights and its jurisprudential construction. There will also be a detailed study of the judgment that recognized the right to digital forgetfulness for the first time.

KEYWORDS.

Indexing, data quality, ARCO rights, data protection, automated treatment.

LISTADO DE ABREVIATURAS UTILIZADAS.

AEPD: Agencia Española de protección de datos.

ARCO: Acceso, Rectificación, Cancelación y Oposición.

ART: Artículo.

CDFUE: Carta de los Derechos Fundamentales de la Unión Europea.

CE: Constitución Española.

DPO: Delegado de Protección de Datos.

LOPD: Ley Orgánica de Protección de Datos.

LORTAD: Ley Orgánica de Regulación del Tratamiento automatizado de Datos.

LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

OCDE: Organización para la Cooperación y el Desarrollo Económico.

RGPD: Reglamento de Protección de Datos.

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea.

STC: Sentencia del Tribunal Constitucional.

TC: Tribunal Constitucional.

TFUE: Tratado de Funcionamiento de la Unión Europea.

TJUE: Tribunal de Justicia de la Unión Europea.

UE: Unión Europea.

1. INTRODUCCIÓN

El derecho al olvido constituye una novedad, no solo desde el punto de vista de su regulación sino de su reconocimiento, que tuvo lugar por primera vez en virtud de una sentencia del Tribunal de Justicia de la Unión Europea. Veremos cómo este derecho se vincula con otros derechos constitucionales, como el honor, la intimidad, la propia imagen, la libertad de información, la libertad expresión etc.

Con la llegada de Internet, el derecho a la privacidad se ve mermado y hace que las personas se vean afectadas por una serie de intromisiones a su intimidad por ejemplo con la divulgación de información personal incorrecta o desactualizada. Por todo ello, se refuerza al afectado con una serie de mecanismos para hacer valer su derecho a la protección de datos, especialmente a través de los derechos ARCO.

Las leyes aprobadas en nuestro país, especialmente la Ley Orgánica 3/2018, de 5 de diciembre, hacen hincapié en los principios de protección de datos, cuidando que la exactitud, la adecuación con la finalidad para la que fueron recogidos, la veracidad, el consentimiento y la minimización de datos se cumplan por parte del responsable del tratamiento de datos personales. Con la aprobación del RGPD, se unifica en gran medida toda la normativa en materia de protección de datos y se hace extensiva su aplicación obligatoria en todo el territorio europeo, como veremos a lo largo del presente trabajo.

2. LA PROTECCIÓN DE DATOS.

2.1. Marco general de la protección de datos.

2.1.1. Derecho a la privacidad y a la intimidad personal.

La privacidad es aquella parte de la vida de una persona que se desarrolla en un ambiente estrictamente íntimo, lo que se denomina esfera personal, siendo por ello inaccesible al resto de las personas. Por tanto, cualquier individuo tiene derecho a mantener su privacidad fuera del control de los demás, asegurándose la no injerencia de estos en su vida privada.

Los conceptos de intimidad y privacidad se encuentran interrelacionados, pero con matices. La privacidad se ha venido considerando como un derecho inherente a cada ser humano, independiente, intransmisible e irrenunciable. De todos los derechos fundamentales, el respeto a la intimidad es el que más ligado está al concepto de

privacidad. Cualquier intromisión ilegítima en la privacidad de una persona está atentando contra su intimidad. Y, aparte, también podría repercutir negativamente en su honor y en su imagen.

El concepto de intimidad encuentra su fundamento y significado en la *idea de dignidad* de la persona y la tutela de su personalidad. Podríamos definirlo como un derecho a decidir por uno mismo en qué medida quiero compartir con otras personas mis pensamientos, sentimientos, inquietudes, etc. Por tanto, el derecho a la intimidad puede entenderse derivado de la personalidad del individuo, que se establece para mantener unas condiciones mínimas de desarrollo de la libertad individual de cada persona[1].

La intimidad es un derecho constitucionalmente protegido en el artículo 18.1 y, como se comentará más adelante, se establece un límite, en su apartado cuatro, relativo al uso de la informática[2]. La privacidad es un concepto más amplio que el de la intimidad o vida privada, y está conectado con la protección de datos de carácter personal. De esta forma, la protección de los datos (de la privacidad) es algo más, y distinto, que la protección al honor, la intimidad y la propia imagen, puesto que lo que se valora en la protección de los datos personales es el poder de disposición que tiene el individuo sobre su información y sus datos personales.

La amplitud del concepto *dato personal* [3] y *tratamiento de datos*, implica que su tutela se haya convertido en un tema clave, especialmente desde la existencia de la sociedad digital, y el tratamiento de la información y los datos personales de forma global e intemporal. La STC 292/2000, de 30 de noviembre, adelantándose al devenir de los tiempos actuales, consideró el derecho a la protección de datos como un verdadero derecho fundamental autónomo y distinto de los derechos a la intimidad personal y familiar. Esto se traduce en la necesidad de proporcionar a las personas un poder de disposición y control absoluto sobre sus datos personales, así como su utilización y

---

[1] HERRÁN ORTIZ, A.I. "El derecho a la protección de datos en la sociedad de la información". *Cuadernos de Deusto de Derechos humanos*, nº 26, 2003, pp. 9-11.

[2] Constitución Española. BOE nº 311, 29-12-1978.

[3] Se ha considerado como datos personales el nombre y apellidos, la voz, la imagen de una persona, su número de identificación fiscal, DNI, cuentas bancarias, su historial clínico, el número de fax, las direcciones de email, las direcciones IP, "puesto que proporcionan una información sobre una persona física identificada o identificable".

destino, con el fin de impedir su uso o tráfico ilícito y lesivo para su dignidad y derechos del afectado[4].

Esta sentencia es clave puesto que se introduce el concepto de libertad informática o habeas data como un derecho fundamental en sí mismo y autónomo del derecho a la intimidad personal[5]. Por tanto, el derecho a la protección de datos es mucho más amplio que el derecho a la intimidad, pues su objeto de protección son los datos personales; datos que no tienen por qué ser íntimos o que puedan suponer una amenaza, pero que pueden ser objeto de creación de perfiles en base a unos determinados parámetros[6]. Como es lógico, dada la estrecha relación existente entre los datos personales, el derecho fundamental a la intimidad y, más ampliamente, a la dignidad personal, la regla fundamental que se utiliza para poder tratar los datos personales es el consentimiento de una persona.

La jurisprudencia viene reconociendo un límite tradicional a los derechos al honor, intimidad y propia imagen, y es la existencia de un derecho de libertad de información; limitación especialmente reforzada cuando es ejercida por profesionales de medios de comunicación, puesto que constituyen un elemento

---

[4] El TC afirma en su FJ Sexto: "La singularidad del derecho a la protección de datos, es por un lado su objeto más amplio que el del derecho a la intimidad, ya que el derecho a la protección de datos extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 C.E , sino a lo que este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inexorablemente unidos al respeto a la dignidad personal. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos de la constitucionales y sean o no relativos al honor, ideología, la intimidad personal y familiar y cualquier otro bien constitucionalmente amparado". Vid. SIMÓN CASTELLANO, P. *El reconocimiento del derecho al olvido digital en España y la U.E. Efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015, pp.185.

[5] MURGA FERNÁNDEZ, J. "La protección de datos y los motores de búsqueda en Internet: Cuestiones actuales y perspectiva de futuro acerca del derecho al olvido". *Revista de Derecho Civil*, nº4, vol. IV, 2017 pp. 185-187.

[6] Un ejemplo de la magnitud de los datos personales que pueden afectar a la privacidad, los encontramos en las redes sociales. Un artículo del País en el que se explicaba la creación de perfiles en Internet con un simple me gusta en la red social Facebook: https://elpais.com/sociedad/2013/03/11/actualidad/1363020389_803146.html

imprescindible en la creación de una sociedad democrática y de una opinión libre. Es necesario valorar, por una parte, el nivel de injerencia en el derecho fundamental a la protección de datos personales derivado de la clase de dato personal a la que se va a tener acceso y, por otra parte, el interés público real en el acceso y en la publicación de la información que contiene datos personales[7].

2.1.2. Criterios generales de la protección de datos.

El derecho a la protección de datos es un derecho a la autodeterminación informativa, es decir, la persona decide qué contar y cómo contarlo, o, por el contrario, decide no divulgar sus datos personales, o también el supuesto en el que los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados. Hay que recordar que la protección de datos personales nace como un derecho a controlar la información personal de los tratamientos masivos. Para determinar cuándo hay un interés objetivo en que determinados datos personales sean tratados, o mantenidos, en el tiempo exige un análisis, por un lado, desde una vertiente positiva, en donde se estudian los aspectos objetivos de los datos personales como pueden ser el contenido de la información, qué tipo de datos se publican, etc. y, por otro, los aspectos subjetivos relacionados con las circunstancias del afectado en cuestión y especialmente con su notoriedad pública. A todo esto, hay que añadir un juicio de proporcionalidad para valorar si la conservación o difusión de dichos datos personales, con o sin el consentimiento de su titular e, incluso, en contra de este, es pertinente, necesario e idóneo[8].

Desde una vertiente negativa, hay que tener en consideración el factor tiempo, elemento decisivo; habrá que ponderar la permanencia de ese interés en el tiempo, puesto que, aunque el uso de esos datos esté justificado en un principio, el transcurso del tiempo ha podido hacerlo desaparecer, concretamente cuando los datos ya no son necesarios para los fines para los que fueron recogidos o tratados. Puede ocurrir que la información y los datos que incorpora dejen de ser relevantes y que

---

[7] TRONCOSO REIGADA, A. "Los límites de acceso a la información". *Revista iberoamericana de Derecho informático*, nº1, 2016, pp. 45-53.

[8] Pertinente, necesario e idóneo: para el caso de que no exista una medida menos lesiva que la propuesta para cumplir el mismo fin o idónea, si es otra medida, pero sirve para cumplir el mismo fin.

desaparezca el interés público que generó su inicial difusión. Es precisamente esta "falta de interés" la que resulta especialmente importante por el paso del tiempo y el deseo del afectado de que determinados datos personales no sigan siendo accesibles al conocimiento público, unido a la intemporalidad de los datos personales en Internet, hace que surja un derecho de protección de los datos personales o, más concretamente, un derecho al olvido.

Por lo tanto, la protección de la privacidad de los ciudadanos tendría las siguientes notas:

- Limitación de la finalidad: Los datos personales serán recogidos con fines *determinados, explícitos y legítimos*, y no serán tratados de manera incompatible con dichos fines. No se considerará incompatible con ellos, el tratamiento posterior de los datos con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos. Principio derivado directamente del RGPD, en su artículo 5.

-El consentimiento: El tratamiento de los datos personales está basado en el consentimiento del afectado de acuerdo con el artículo 6 de la LO 3/2018[9].

-La veracidad y exactitud: los datos serán exactos y, si fuere necesario, actualizados (artículo 4 de la LO 3/2018).

-Confidencialidad: Todas las personas que realicen cualquier tratamiento de datos personales están sujetas al deber de confidencialidad (artículo 5 de la LO 3/2018)[10].

-Calidad: Este criterio se estableció ya en el Convenio nº 108, de 28 de enero de 1981, del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Actualmente, se incluyen

---

[9] Art 6 LO 3/2018 de 5 de diciembre:

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

[10] Art 5 LO 3/2018 de 5 de diciembre*:*

1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

tanto los automatizados como los no automatizados. Tanto unos como otros se tratarán de la siguiente forma:

a) Se obtendrán de forma lícita y se tratarán de forma leal y legítima.

b) Se tratarán para finalidades determinadas y legítimas, es decir, que no se utilizarán de forma incompatible con estas características.

c) Serán adecuados, necesarios, pertinente se hayan recabado, es decir, que no sean abusivos.

d) Serán exactos y, si fuera necesario, serán puestos al día, es decir, actualizados.

e) Se conservarán bajo una forma que posibilite la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se han tratado.

Como se comentaba en el inicio de este epígrafe, el factor tiempo es un elemento clave, que hasta hace poco no había sido tenido en cuenta al tiempo de evaluar si se había lesionado, o no, el derecho a la protección de los datos personales. Pues bien, ahora los tiempos son otros; con la llegada de Internet, la información puede ser localizada fácilmente y lo más importante, no se olvida, permanece indefinidamente en las redes. El factor tiempo tiene una importancia fundamental en esta cuestión puesto que las características anteriormente citadas (necesario, adecuado, pertinente, exactitud) deben cumplirse no solo en el momento inicial de recogida y tratamiento de la información, sino durante todo el tiempo en el que dicha información sea tratada. Por tanto, la existencia de esta nueva sociedad digital supone un peligro añadido a todos los anteriores, y que afecta de forma grave a la privacidad de las personas. En el supuesto de una información exacta desde un principio, puede ocurrir que, transcurrido un lapso de tiempo, esa información no se corresponda con la realidad porque haya cambiado o porque ha dejado de existir o porque no esté actualizada. O también puede ocurrir que esa información haya sido superada por acontecimientos posteriores que la desvirtúan o dejan en un segundo plano. Pero

lo que no cambia es el hecho de teclear el nombre de una persona en un buscador y recordar ese acontecimiento o esa información relacionada con ella.

2.1.3. El principio de calidad de los datos personales.

Cuando hablamos de calidad de los datos personales, ello entra en conexión con el artículo 5 RGPD, donde se recogen los principios relativos a los datos personales. Las premisas que regula el RGPD son:

-No podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos.

-Los datos serán exactos y actualizados en todo el momento.

-Si son inexactos, serán cancelados o sustituidos por los correspondientes datos rectificados o completados.

-La rectificación y cancelación notificada tiene que resolverse y notificarse al cesionario en el plazo de 10 días.

-Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido recabados.

-Podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una obligación jurídica o de ejecución de contrato, etc.

-Los datos de carácter personal serán almacenados de forma que permitan el ejercicio de derecho de acceso, salvo que sean cancelados.

-Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Como regla general, el responsable de un determinado servicio (por ejemplo, Facebook o Google) no puede conservar copias de los perfiles de los usuarios que han abandonado dicha plataforma, para sus propias finalidades o intereses espurios y mucho menos por un tiempo indeterminado. En definitiva, la conservación de las

copias de los datos personales por un tiempo indefinido no es aceptable[11]. Se establece, por tanto, un principio de prohibición del exceso de los datos -un principio de minimización-, que obliga a que los mismos sean limitados al mínimo necesario en relación con los fines para los que fueron recogidos y de esta forma los prestadores de servicios de Internet tienen la obligación de limitar la recogida de datos al mínimo.

2.2 Marco normativo de protección de datos en la Unión Europea.

2.2.1. Principales novedades del Reglamento Europeo de Protección de datos.

El primer gran hito a nivel normativo fue la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que vio la luz el 24 de octubre de 1995. Esta Directiva tenía como fin principal asegurar un alto nivel de protección al tratamiento de datos personales en el territorio de la Unión Europea. Se fijan así una serie de barreras que impidiesen la libre circulación de información, así como, por primera vez, se constituye un derecho de oposición por razones legítimas; derecho que, más tarde, veremos cómo ha ido evolucionando a lo largo de los años, y también un derecho de rectificación[12].

Más de 20 años después de la aprobación 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos, la Unión Europea ha aprobado el Reglamento (UE) 2016/679, de 27 de abril de 2016, con el mismo título y conocido también como Reglamento General de Protección de Datos, que comenzó a ser aplicado en el año 2018 y que sustituye y deroga la citada Directiva.

---

[11] El Grupo de Trabajo del artículo 29, en su Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, emitido el 4 de abril de 2008, señala que la retención de datos por estos no debía superar los seis meses.

[12] PÉREZ GÓMEZ, A.M. "El Derecho al olvido digital en Europa, una lucha de titanes". *Revista la Propiedad Inmaterial*, nº22, 2016, pp.173-186.

La Directiva de 1995 fue creada con el objetivo de, por un lado, defender el derecho fundamental a la protección de datos y, por otro, garantizar la libre circulación de los mismos. El contexto en el que fue aprobada era totalmente distinto al actual en términos de avance tecnológico, Internet y globalización. Es, por ello, que se plantearon, por parte de la Comisión, algunas propuestas sobre protección de datos, entre ellas, la propuesta de sustituir la Directiva 95/46/CE por el actual Reglamento. En conclusión, llegaron al consenso de que aquélla no resolvía los problemas o, mejor dicho, no se adaptaba a las nuevas realidades ni estaba a la altura de los retos tecnológicos del momento. Fue el 5 de octubre de 2010 cuando se celebró una reunión de alto nivel para tomar una decisión y se consultó así mismo al Grupo de Trabajo sobre Protección de Datos del artículo 29[13]. Por tanto, como ya se venía adelantando, se llegó a la conclusión de que la Directiva era insuficiente no sólo para adaptarse a los momentos actuales, sino también para la protección del derecho fundamental a la protección de datos. En esa reunión, se remarcó el hecho de crear un marco jurídico común, es decir, tratar de obtener una armonización de todas las normativas de los distintos Estados miembros de la Unión Europea[14].

Durante este tiempo, la libertad informática y, sobre todo, la llegada de las nuevas tecnologías han supuesto cambios en la sociedad y han planteado distintas realidades, por lo que la normativa, como es lógico, tiene que adaptarse a estas nuevas realidades, no previstas ni contempladas en las distintas legislaciones. Uno de los elementos claves de esa evolución lo constituye el paso de considerar el habeas data como un instituto de protección de otros derechos, principalmente la intimidad, a entenderlo como un derecho autónomo e independiente con su propia configuración y lógica internas. Si hacemos una comparativa de la Directiva y el nuevo Reglamento, vemos, por ejemplo, como el artículo primero de aquélla señala que su objetivo es garantizar «la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales». Por su parte, el Reglamento

---

[13] El Grupo de Trabajo del artículo 29 (GT Art. 29) es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD).

[14] CHÉLIZ INGLÉS, M. C. "El derecho al olvido digital. Una exigencia de las tecnologías recogido en el Reglamento general de protección de datos", nº5, agosto 2016, pp. 260-261.

señala en el mismo ordinal: «El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales». En otras palabras, durante este largo periodo el derecho a la libertad informática se ha independizado del derecho a la intimidad, constituyendo ahora un derecho fundamental autónomo, como comentábamos en el epígrafe introductorio sobre la protección de datos. En este sentido ha jugado un papel fundamental el legislador comunitario y los tribunales de los Estados miembros[15].

El reconocimiento de este derecho a la protección de los datos personales no solo aparece en las Directivas y Reglamentos de la Unión Europea, o en las normativas de los distintos Estados miembros, sino también cobra una especial relevancia en este reconocimiento el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea: y el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE); ambos artículos dicen lo mismo: *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen.*

Como comentábamos anteriormente, la ley necesitaba adaptarse a las nuevas realidades. El objetivo de las regulaciones normativas no ha cambiado, sigue siendo el mismo, simplemente hay que adaptarse a los nuevos tiempos y seguir insistiendo, por un lado, en la necesaria protección de un derecho humano (derecho de protección de los datos personales) y, por otro, en la importancia económica que tiene el flujo de datos personales, lo que más tarde abordaremos. Uno de los aspectos que cambia sustancialmente es la intensidad; si bien el objetivo del RGPD es el mismo que el de la Directiva, cambia notablemente la protección, precisamente por la llegada de las nuevas tecnologías, el Big Data, la comercialización de nuestros datos personales por empresas con fines comerciales, el alto grado de filtración y exposición de nuestra vida privada, etc. Si el flujo de datos e información personal tenía relevancia económica en 1995, no ha hecho más que multiplicar esa relevancia en los últimos años. La economía digital parece haberse convertido en un objetivo prioritario de la Unión Europea y los propios Considerandos del Reglamento declaran la importancia «de generar confianza que permita a la economía digital desarrollarse en todo el mercado interior» (7). Desde el punto de vista de la protección de las personas, los retos y los riesgos también se han vuelto mayores,

[15] Vid., por ejemplo, dentro de nuestro ordenamiento, la STC 292/2000, de 30 de noviembre.

pues el uso de datos personales por parte de las organizaciones públicas y privadas se realiza ahora «en una escala sin precedentes» en comparación a hace 15 años, puesto que no se comercializaba con nuestros datos de la forma en la que se hace ahora, además de que, para la gran mayoría de empresas o entidades públicas, el tratamiento de nuestros datos personales es una fuente de poder y de negocio[16].

Por otro lado, en el periodo transcurrido, el derecho a la libertad informática se ha convertido en un elemento muy destacado y visible del proyecto europeo. Las sucesivas sentencias del Tribunal de Justicia de la Unión Europea sobre la materia han ido formando su contenido y lo han hecho llegar a lugares antes insospechados, puesto que se plantean situaciones que, hasta hace unos años, eran impensables[17]. De este modo, la normativa sobre protección de datos se ha convertido en un símbolo de los altos estándares de calidad del Derecho europeo y de su capacidad para imponerlos en el ámbito internacional, especialmente en las complejas relaciones Europa-Estados Unidos.

Si nos fijamos en los intereses del consumidor y de las empresas, son generalmente opuestos. Es decir, hoy por hoy el tratamiento de los datos de carácter personal para una empresa tiene un fin puramente comercial, mientras que, para el usuario, el hecho de ceder sus datos a terceros, por ejemplo, en una página web, es únicamente para acceder a los servicios de dicha página; es más, si no proporciona sus datos, incluso se le puede denegar el uso de ese servicio, es, por tanto, en muchos casos, una obligación impuesta. Esta oposición de intereses puede generar muchos inconvenientes a la hora de hacer respetar los derechos de ambas partes. Y volvemos al problema de la llegada de las nuevas tecnologías, las herramientas digitales tienen una aplicación global y su restricción está limitada territorialmente por las legislaciones pertinentes a nivel nacional. De este modo, la utilización y visualización de los datos de carácter personal es global, pero la regulación legislativa es limitada.

Como consecuencia de todo esto, los legisladores, tanto europeos como nacionales, pretenden dotar de una serie de herramientas al consumidor a fin de tener un cierto control sobre sus datos personales. El resultado de estas herramientas implica la

---

[16] FERNÁNDEZ VILLAZÓN, L.A. "El Nuevo Reglamento Europeo de Datos". *Foro Nueva Época*, vol. 19, nº 1, 2016, pp. 395-411.

[17] Por ejemplo, la utilización de información tal cual fue publicada en los medios de comunicación, STJUE, de 18 diciembre de 2008, caso C-73/07, Tietosuojavaltuutettu y Satakunnan Markkinapörssi Oy, Sata media Oy.

instauración de una serie de límites al responsable del tratamiento de dicha información personal, por ejemplo, un servidor de Internet.

El nuevo Reglamento aporta precisamente todo eso y es que, pasar de una Directiva a un Reglamento, instrumento que podemos considerar como auténtica ley europea, implica el paso de una regulación más flexible y abierta para los Estados miembros a otra de aplicación más uniforme y sólida en el conjunto de la Unión. Se pretendían superar los obstáculos, como son los avances tecnológicos y la globalización, y, para ello, ha sido clave un elemento que es la denominada "ejecución estricta". El objetivo no es otro que garantizar una mayor seguridad jurídica en toda la Unión Europea. Esta preocupación se advierte claramente en el Documento de Trabajo de la Comisión que sirvió de base para la elaboración del Reglamento y otras disposiciones que conforman el llamado «paquete de protección de datos». En dicho documento, se ponen de relieve las barreras que, para los negocios y la actividad de las autoridades públicas, derivan de la fragmentación de la normativa de protección de datos, la inseguridad jurídica y la falta de consistencia en la vigilancia de su cumplimiento.

Ciertamente, se ha pretendido un marco normativo común en el cual se llevarán a cabo actuaciones comunes en todo el territorio europeo. Sin embargo, con la Directiva se dejaba la puerta abierta a los Estados a la hora de ejecutar esas actuaciones, lo que se tradujo en un amplio margen a la acción de aquéllos. Por tanto, aquí es donde surge el primer problema, puede ocurrir que, en un Estado miembro, el tratamiento de un determinado dato personal sea lícito y, en otro, no lo sea. Esto desembocó, como era evidente, en disparidad de problemas de interpretación y planes de actuación diferentes en cada Estado miembro. La Comisión, como era lógico, detectó faltas de coherencia en la definición del consentimiento, en la regulación de las categorías de datos sensibles, en las reglas sobre notificación previa de los tratamientos, o en las transferencias de datos a terceros países, etc.[18].

La Comisión insiste en superar estos hechos, es decir, solventar esos problemas de interpretación y las actuaciones llevadas a cabo. Quizá el error fue en dejar la puerta abierta a los Estados miembros a la hora de regular ciertos puntos. Ese era el elemento que presenta más inconvenientes; la Directiva es mucho más abierta, flexible con los Estados miembros, legislativamente hablando. En cambio, el

[18] Documento de Trabajo de la Comisión de 25 de enero de 2012 [SEC (2012) 72 final], pp. 12-15.

Reglamento es una herramienta legislativa más coherente, sólida, restrictiva y está dotada de una mayor ejecución en todo el territorio europeo. Una regulación más uniforme para toda Europa permitiría superar tales inconvenientes. La Comisión insiste también en que las diferencias de criterio de las distintas autoridades nacionales de protección de datos a la hora de exigir el cumplimiento de la Directiva, y las grandes diferencias existentes entre los distintos sistemas sancionadores en caso de incumplimiento, constituyen otras tantas «incoherencias» del sistema que pretenden salvarse con el nuevo Reglamento.

Por lo tanto, vistos los errores que supuso flexibilizar la normativa y dejarla al criterio de los Estados miembros, con el nuevo Reglamento se pretende resolver este problema, pero logrando un punto intermedio, es decir, lograr una normativa sólida, coherente, común y de ejecución inmediata, y, a la vez, permitir la interpretación y aplicación al criterio de los Estados miembros, eso sí de forma más limitada, reduciendo su margen de actuación. Una regulación más sólida parece haber implicado también una normativa más estricta, al querer dejar menos espacios a la aplicación e interpretación de los Estados; el Reglamento se ve obligado a abordar con mucho más detalle, rigor y exhaustividad los diferentes aspectos del tratamiento de datos de carácter personal.

Por primera vez en la historia, todos los países de la Unión Europea quedan sometidos a una misma regulación en protección de datos personales, por tanto, se moderniza y unifica el derecho a la protección de datos, teniendo en cuenta, como ya se ha comentado anteriormente, el nuevo escenario tecnológico, y la disparidad de criterios y las discrepancias existentes entre los Estados miembros debidas principalmente a la gran cantidad de cláusulas abiertas que contenía la Directiva (open-ended-principales). Queda constatada la voluntad integradora, sólida y coherente del nuevo Reglamento, dispuesta a superar los problemas existentes en los criterios dispares de interpretación de la regulación, que en nada favorecía la protección del derecho fundamental a la protección de los datos personales[19].

El Reglamento General de Protección de Datos ha incluido importantes novedades en el apartado de derechos del afectado. La nueva normativa asume como pilar fundamental que nuestra información personal debe estar sometida a nuestro propio criterio, como ya venía haciendo la Directiva, al dotar de una serie de herramientas

[19] SANCHO LÓPEZ, M. "Garantías legales del concepto de privacidad: entre el derecho al olvido y el nuevo Reglamento de Protección de Datos", nº9, 2018, pp.:185-187.

de control al interesado para hacer valer su derecho; un ejemplo de ellos es el derecho de rectificación. El conjunto de facultades que se conceden al afectado siempre se han entendido como parte del contenido esencial de la autodeterminación informativa. En este sentido, la nueva normativa ha supuesto un cambio radical en materia de protección de datos, ya que ahora se facilita al titular de los mismos la gestión de su propia información personal en base a sus preferencias, así como somete a empresas privadas y Administraciones Públicas al interés del ciudadano, obligándoles a adoptar políticas activas de protección de datos, cambiando las reglas del juego existentes hasta el momento. Por tanto, el eje central ahora es el consumidor y su protección en caso de vulneración del derecho a la protección de datos.

Por otro lado, el Reglamento se hace eco de la doctrina del Tribunal de Justicia, que, durante estas décadas, ha realizado una nada desdeñable labor de precisión y concreción de conceptos, a veces regulados con excesiva ambigüedad en la Directiva. Por otra parte, algunas modificaciones responden a la necesidad de adaptarse a los cambios tecnológicos y sociales que han tenido lugar en los últimos años, especialmente con la llegada de globalización, siempre con la premisa de conseguir una normativa de protección «tecnológicamente neutra».

Otro aspecto importante que hay que valorar, es la prestación del consentimiento. El Reglamento desarrolla ahora, en su artículo 7, las condiciones que ha de reunir la prestación del consentimiento para ser válido y exige «que el responsable deberá ser capaz de demostrar que aquél (el interesado) consintió el tratamiento de sus datos personales». Nótese que el consentimiento puede seguir siendo tácito, salvo cuando se trata de categorías especiales de datos, donde se exige que sea explícito. Por tanto, la necesidad de probar su existencia hace que algunas prácticas frecuentes hasta ahora, basadas en la simple inactividad del interesado, resulten más difíciles de aceptar bajo la nueva regulación. Una adecuada demostración de que se ha prestado dicho consentimiento va a requerir una conducta más activa, más directa del afectado, aunque sea tácita.

Por otra parte, el acceso cada vez más frecuente de los menores a los servicios de la sociedad de la información ha obligado a dedicar el artículo 8 del Reglamento a regular su consentimiento mediante unas condiciones especiales[20]. Básicamente, la

[20] Art 8.1 REGLAMENTO (UE) 2016/679: *Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los*

nueva normativa fija una especie de «mayoría de edad» informática que da validez al consentimiento dado por las personas mayores de dieciséis años (aunque los Estados miembros pueden rebajar hasta los trece). Como se puede deducir, el uso de los servicios de la sociedad de la información por parte de un menor que esté por debajo de la edad anteriormente citada, queda vinculado a la autorización de quien ostente la patria potestad o la tutela del mismo.

Otro derecho afectado y que está íntimamente relacionado con los anteriores, es el recogido en el artículo 22, el derecho a no ser sometidos a decisiones automatizadas. Si bien este derecho fue recogido en la Directiva, no se llegó a prever la importancia que iba a alcanzar la elaboración de perfiles por parte de empresas privadas sobre la base del tratamiento masivo de datos personales a través de técnicas como la del Big Data. Estas técnicas comerciales suelen ser utilizadas por empresas de marketing y publicidad para elaborar perfiles, pero su utilidad puede extenderse más allá de los fines comerciales, por ejemplo para la predicción del rendimiento en el trabajo, la situación económica, la salud, la fiabilidad, el comportamiento, etc. El número de datos que pueden manejarse y el número de personas afectadas han aumentado en la actualidad, además, en una escala impensable en 1995.

No se trata con todo esto de limitar ni de prohibir este tipo de prácticas comerciales dedicadas a elaborar perfiles (éstas han abierto unas expectativas económicas que la UE no parece dispuesta a desaprovechar), sino de garantizar, como mínimo, el derecho del afectado a «tener intervención humana», a «expresar su punto de vista» y a «impugnar la decisión», es decir, que el interesado tiene derecho a conocer los fines del tratamiento de su información personal, así como a mostrar su punto de vista, retirar su consentimiento o, incluso, rectificar la información que considere necesaria.

Con relevantes modificaciones, se regulan los tradicionales Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), que, con el nuevo Reglamento, se transforman en los derechos de Transparencia, Información, Acceso, Rectificación, Cancelación, Oposición, Limitación del Tratamiento y Portabilidad. El artículo 16 simplifica las fórmulas para facilitar al interesado ejercitar su derecho de rectificación

---

datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

de la información personal.[21] Como se comentaba anteriormente, se flexibiliza el derecho de acceso a la información al interesado y se va un poco más allá puesto que se facilita que de todo interesado pueda obtener una copia de los datos personales que han sido objeto de tratamiento[22].

Se prevé también la posibilidad de limitar el tratamiento de los datos personales en el artículo 18, se trata de una especie de garantía pre-procesal que puede funcionar en interés del interesado a la hora de poner un límite al tratamiento de su información. Cuando se ejercita este derecho, los datos no se suprimen, pero dejan de ser tratados y se conservan para facilitar la formulación, la defensa o el ejercicio de reclamaciones. De esta manera, se ataja el perjuicio que el proceso de la información pudiera estar provocando, a la vez que se permite su posterior revisión en caso de conflicto.

La limitación está prevista en cuatro supuestos. En primer lugar, cuando el interesado haya impugnado la exactitud de los datos personales; se limita entonces el tratamiento de éstos como garantía provisional «en un plazo que permita al responsable verificar la exactitud de los mismos». En segundo lugar, cuando el interesado se haya opuesto al tratamiento y el responsable haya alegado motivos legítimos imperiosos para continuarlo. También procede entonces la limitación provisional, en tanto se evalúa si esos motivos legítimos prevalecen sobre los intereses o las libertades del interesado. En tercer lugar, procede la limitación cuando el tratamiento de datos es ilícito y el interesado opta porque aquéllos no sean suprimidos. Finalmente, cuando los datos no son ya necesarios para el tratamiento porque la información ha dejado de ser relevante para el objetivo con el que fue recogida, o porque la misma ha cambiado. La regla general es que deben ser cancelados. No obstante, el interesado que los necesite para la formulación, el ejercicio o la defensa de reclamaciones puede obtener en su lugar la limitación; una medida práctica que trata de paliar efectos indeseados para los interesados.

---

[21] Art 16.1 REGLAMENTO (UE) 2016/679: *El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le concierne. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.*

[22] Art 15 REGLAMENTO (UE) 2016/679: *El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.*

Para proporcionar una mayor virtualidad al control por los interesados de su propia información personal, se reconoce expresamente el derecho a la portabilidad de los datos personales (artículo 20). Más que la libertad informática, lo que está en juego aquí es la libre competencia. Piense el usuario de Internet en la gran cantidad de datos personales que ponemos hoy en día en manos de las empresas que operan en la sociedad de la información (teléfonos, direcciones, fotografías, vídeos, etc.). Cuando ese volumen llega a cierto nivel, por ejemplo, se ha introducido información personal en muchas páginas webs o servicios de Internet, existe el miedo a perderla o a tener que volver a introducirla manualmente, lo que puede actuar como fuerte elemento disuasorio si nos estamos planteando cambiar de servicio o de compañía. Es decir, que el usuario puede tener miedo de perder toda la información que ha introducido en un determinado servicio de Internet, o bien puede querer desvincularse de ese servicio. Pues bien, el Reglamento reconoce nuestro derecho a recibir los datos personales que nos incumban «en un formato estructurado de uso común y lectura mecánica» y transmitirlos a otro responsable del tratamiento sin que el primero pueda oponerse. Es más, la norma europea reconoce el derecho a que los datos «se transmitan directamente de responsable a responsable» cuando sea técnicamente posible. Se deduce también de este artículo que el interesado puede, en cualquier momento, retirar de un determinado servicio de Internet la información que ya no sea necesaria para el fin inicial para el que fue recogida.

Se refuerza así mismo el derecho de oposición recogido en el artículo 21, introduciendo nuevos motivos para su ejercicio como la elaboración de perfiles, lo que se conecta con el ya citado artículo 22. Cito textualmente: "*El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones".*

Entre los derechos de nueva incorporación, destaca el recogido en el artículo 17, el denominado derecho de supresión, o también conocido como derecho al olvido, que será abordado en el siguiente epígrafe.

Para facilitar las facultades de acceso de los interesados, se dispone que los responsables del tratamiento de la información de carácter personal, posibiliten la

presentación de solicitudes por medio de canales electrónicos[23]. También hay que hacer referencia a que el ejercicio de este derecho y los otros citados anteriormente serán preeminentemente gratuitos.

Así mismo, el Reglamento incorpora algunos mecanismos como el cifrado o la seudonimización de los datos personales (artículo 32). Entre las principales novedades que atañen especialmente a los consumidores, es preciso destacar la incentivación del uso de datos personales seudonimizados. Lo que se pretende con estas herramientas es evitar, de forma irreversible, la identificación de los sujetos, así como la confidencialidad e integridad de los datos personales de los particulares[24]. La seudonimización como tal es un concepto novedoso que consiste en una información que, sin incluir los datos denominativos de un sujeto afectado permiten, a través de la asociación con información adicional, determinar quién es el individuo que está detrás de los datos seudonimizados.

Para todo esto, se tienen en cuenta múltiples variables como son la naturaleza, el contexto, el alcance y los fines de tratamiento de la información personal que se maneja, sumado todo ello a los riesgos graves que puedan afectar a los derechos y libertades de los interesados. El fundamento es reducir estos riesgos y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos.

Enlazado con lo anterior, se establece la obligación de realizar una evaluación de impacto[25], también conocida como Privacy Impact Assessment, cuando se lleve a cabo un tratamiento de datos que pueda conllevar algún riesgo para los derechos y libertades de las personas físicas, o mediante la aplicación de otro tipo de

---

[23] Art 15.3 REGLAMENTO (UE) 2016/679: *Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.*

[24] Art 32.1 b REGLAMENTO (UE) 2016/679*: La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.*

[25] Art 35.1 REGLAMENTO (UE) 2016/679: *Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.*

operaciones encargadas de determinar el alcance de los riesgos del tratamiento de los datos personales[26].

Por último, se contemplan actuaciones preventivas cuyo objetivo es cumplir con las disposiciones de su articulado, como se deduce de la inclusión de la protección de datos como orientación de las políticas y decisiones empresariales que deben cumplir los responsables cuando tratan información personal, como regla general desde el momento inicial del tratamiento hasta el final del mismo[27].

Otro ejemplo claro de la extensión de las obligaciones de los encargados del tratamiento de la información es el concepto de "responsabilidad activa" (*accountability*) por el que se les obliga a que adopten medidas necesarias para cumplir con los principios, derechos y garantías que se recogen en el RGPD, estableciendo así mismo responsabilidades derivadas de su incumplimiento reguladas en el artículo 24 del RGPD.

El Reglamento exige que haya responsabilidad proactiva tanto en el cumplimiento como en su demostración. Para ello, el responsable del tratamiento deberá establecer procedimientos a través de los cuales:

- Pueda garantizar la aplicación de la normativa de protección de datos.
- Pueda demostrar frente a terceros la efectiva aplicación y el cumplimiento de la normativa de protección de datos.

[26] El RGPD no diferencia entre ficheros de nivel básico, medio o alto, sino que impone medidas de seguridad en base al estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y las libertades/derechos concretos de las personas físicas.

[27] Art 25.1 REGLAMENTO (UE) 2016/679: *Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.*

El concepto como tal aparece mencionado en el artículo 5, apartado 2, del RGPD[28]. Todo ello seguido de numerosas obligaciones encaminadas a la protección de los derechos de los usuarios[29]. Citamos algunas de ellas:

- Nueva figura del Delegado de Protección de Datos (DPO).
- Medidas de protección de datos desde el diseño y por defecto.
- Registro de actividades de tratamiento.
- Análisis de riesgo.
- Medidas de seguridad.
- Evaluación de impacto en la protección de datos.
- Notificación de quiebras por seguridad.

La novedad, quizá más importante y esperada, es la derivada del principio de territorialidad. Pues bien, comenzaremos explicando el origen del problema sobre la aplicación de este principio de territorialidad. En los comienzos del desarrollo de la actividad en la red se debatía qué normativa iba a ser aplicable para regular las relaciones jurídicas que se establecen y la jurisdicción competente para solucionar los eventuales conflictos. Digamos que la territorialidad es consustancial al ejercicio de la jurisdicción, pero el fenómeno de Internet es una realidad virtual en la que no existen espacios físicos, es decir, no entiende de territorios. Como sabemos, Internet es una plataforma global que va más allá de las fronteras físicas entre países.
Poniendo un ejemplo práctico sobre esto, si nos remontamos al año 1996, John P. Barlow colgaba en la Red la llamada "Declaración de Independencia del Ciberespacio", que ya predecía esta idea: "*En el Ciberespacio no tenemos gobierno electo ni es probable que lo tengamos, de ahí que me dirija a ustedes, Gobierno del Mundo industrializado con no mayor autoridad que aquella con la que habla la propia libertad. Yo declaro que el espacio social global que estamos construyendo es por naturaleza independiente de las tiranías que ustedes pretenden imponernos. Ustedes no tienen ningún derecho a gobernarnos ni poseen método alguno de coerción que debamos temer con fundamento…Sus conceptos jurídicos de propiedad, libertad de*

[28] Art 5.2 REGLAMENTO (UE) 2016/679: *El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»*).

[29] SANCHO LÓPEZ, M. "Garantías legales del concepto de privacidad: entre el derecho al olvido y el nuevo Reglamento de Protección de Datos", nº 9, 2018, pp.186.

expresión, derecho a la identidad, libertad de circulación y contexto no nos es aplicable. Se basan en la materia. Aquí en el ciberespacio no hay materia".

Como vemos, estas expresiones son claramente exageradas, pero tienen un sustrato real: el ciberespacio es un ámbito virtual en el que los límites territoriales poco importan, porque no existen; además, las jurisdicciones y las competencias territoriales de los tribunales no son funcionales[30]. Pero los litigios que surgen deben ser resueltos por órganos jurisdiccionales con base territorial. Por ello, los principales problemas que se producían, y se siguen produciendo, son los que tienen que ver con la protección de datos en este entorno global, dominado por empresas que ubican sus sedes en terceros Estados, pero que prestan sus servicios a ciudadanos de todo el mundo a través de Internet. La clave de la cuestión es la determinación de la normativa a la que quedan sujetas las reclamaciones que los usuarios plantean contra las mismas y, consustancialmente, los tribunales competentes para la resolución de esas reclamaciones.

El parámetro que se solía utilizar era el establecimiento, es decir, donde se encontraba ubicado el centro de operaciones de la empresa, atendiendo a criterios como la estabilidad de la instalación, la efectividad del desarrollo de actividades en ese Estado, la naturaleza especifica de las actividades económicas y de las prestaciones de servicios (sobre todo en el caso de servicios prestados exclusivamente a través de Internet). Y ello aunque la actividad ejercida fuese mínima, puesto que bastaba con que la actividad fuese real y efectiva, y ejercida mediante una instalación estable. Esta solución no tiene mucha eficacia puesto que, hoy en día, las empresas que operan en Internet utilizan soportes técnicos que pueden estar centralizados en distintos países y sus servidores pueden estar ubicados en sitios remotos o, incluso, secretos. Con lo cual, pueden prescindir de crear un establecimiento al uso. Por tanto, lograr una protección eficaz de los datos personales del ciudadano, queda claro que no puede depender de donde esté ubicado el centro de los medios técnicos de la empresa, es decir, su establecimiento.

Es frecuente el uso de soportes técnicos inmateriales, que permiten prestar los servicios "desubicados" del territorio al que van dirigidos, fruto del alcance global de Internet, y, en muchos casos, sin contar con medios ubicados en dicho territorio. Aquí es donde se encuentra el principal problema a la hora de lograr una tutela

---

[30] CÓRDOBA CASTROVERDE, D. "Los retos de la protección de datos en Internet. Caso Google Spain y Derecho al Olvido". *Afduam*, 21, 2017, pp.: 228-229.

efectiva de la protección de datos cuando se produzcan eventuales lesiones en el ciberespacio. Otro peligro añadido es la estratagema empleada por muchas empresas para eludir la aplicación de la normativa europea o nacional, suprimiendo los establecimientos y medios, o, incluso, cambiando el centro de gestión de recursos y ubicándolo en otros países que tengan otra normativa más permisiva.

Por todo ello, el Reglamento aborda esta cuestión con mucha sensatez y eficacia, estableciendo un criterio de conexión más amplio y mejorado. En su artículo 3.2 establece lo siguiente: *El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:*

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o;

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Como vemos, el criterio de conexión es muy acertado y, sobre todo, ajustado con la realidad tecnológica y la problemática de la desubicación de los medios y establecimientos en el tratamiento de datos de carácter personal. Hasta ahora, si una empresa tenía fuera de la Unión Europea su sede, no tenía establecimiento o no designaba responsable alguno, quedaba excluida del ámbito de aplicación de la normativa europea, aunque estuviese tratando datos de ciudadanos de la UE y el foco de conflicto de intereses estuviese ubicado allí. El artículo 3.2 del RGPD solventa el problema de la territorialidad a través de la extensión de la aplicabilidad hacia los responsables que no estén establecidos en la UE cuando las actividades de tratamiento de datos personales estén relacionadas con la oferta de bienes y servicios a interesados que residan en suelo europeo o ejerzan su actividad en este[31].

La tutela judicial de la privacidad permite por tanto que todo interesado pueda presentar una reclamación ante la autoridad de control de cualquier Estado miembro en el que tenga su residencia habitual, lugar de trabajo, o lugar de la supuesta infracción. Se debe mencionar también la regulación establecida para el derecho a un recurso judicial contra el responsable o encargado, que se puede ejercitar ante los órganos jurisdiccionales del Estado miembro en el que aquél tenga un

[31] Art 3.1 REGLAMENTO (UE) 2016/679: *El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.*

establecimiento, o donde el interesado tenga su residencia habitual; solo hay un excepción y es que el responsable sea una autoridad pública que actúe en el ejercicio de su potestades; en este caso, se entiende que el recurso debe presentarse en el Estado miembro donde se encuentre dicha autoridad[32]. Se acaba por fin con la disparidad de criterios entre los distintos órganos jurisdiccionales respecto de cuestiones tan fundamentales como la legitimidad pasiva de los intervinientes.

También se subsanan las trabas a la actuación de los poderes legislativo y judicial, y se pone fin a la práctica más que asentada entre las corporaciones de Internet, de establecer sus sedes en países cuyas legislaciones permiten, sin demasiados problemas, la mercantilización de la información de carácter personal, ignorando reiteradamente la legislación nacional y europea sobre esta materia y obstaculizando el ejercicio eficaz de los derechos de los ciudadanos, que se encontraban en una clara situación jurídica de indefensión. Así pues, se obliga a estas empresas a someterse al Derecho de la Unión y de los tribunales nacionales de los Estados miembros cuando ofrezcan sus servicios en suelo europeo.

2.2.2. Especial mención al artículo 17 del RGPD: el derecho de supresión.

Como ya se ha hecho mención, el derecho de supresión constituye una de las principales novedades introducidas por el RGPD. Se configura como tal en el artículo 17, y se entiende como una derivación del derecho a la intimidad y propia imagen y como una extensión del derecho al honor. Este artículo lo define como *el derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le concierne, el cual estará obligado a suprimir sin dilación indebida los datos personales* cuando concurran determinadas circunstancias. Pero, cuidado, no hay que entender este derecho como un derecho a configurar un pasado hecho a nuestra medida, obligando a editores de páginas web a borrar información de nuestro pasado que no queremos que se conozca, o porque carece de importancia. Para poder solicitar su supresión, han de revelarse de alguna manera ilícitos en función de las circunstancias concurrentes. Lo que supone el derecho al olvido digital es un límite, una barrera, a la memoria interna de Internet donde el tiempo es lineal, real y no distingue entre pasado, presente o futuro, lo que provoca, en muchos casos, por la

[32] Vid. art. 79.2 REGLAMENTO (UE) 2016/679.

descontextualización, una vulneración de los derechos fundamentales del afectado, perjudicando su integridad y dignidad personal.

Se debe examinar, junto con este nuevo derecho, el concepto *habeas data*, el derecho a la protección de datos personales desde la vertiente de la potestad del interesado, que, como ya comentábamos en epígrafes anteriores, ha pasado a tener un control sobre sus datos, la denominada autodeterminación informativa. Esto se debe en gran medida a la extensión que ha hecho el Reglamento de los derechos ARCO, especialmente los relacionados con el derecho de cancelación y oposición en el ámbito de Internet; conceptos más que aceptados hoy en día por todas las legislaciones, doctrina y jurisprudencia. La naturaleza jurídica del derecho al olvido digital tiene su origen, como bien sabemos, en el derecho a la intimidad, a la vida privada y, sobre todo, a la protección de datos. Por tanto, está íntimamente conectado con la propia personalidad del ser humano y su desarrollo.

Como ya apuntábamos en el comienzo de este epígrafe, el legislador europeo no considera el derecho al olvido como autónomo o diferenciado de los derechos ARCO, sino como una consecuencia de los mismos. Por ello, se dice que es también una potestad otorgada a los ciudadanos para reclamar que sus datos o información personal sean suprimidos de Internet cuando puedan afectar a su intimidad o al libre desarrollo de ciertos derechos fundamentales. Esta potestad se ejercita solicitando a los responsables de los ficheros que los datos sean suprimidos, eso sí siempre que concurra una serie de circunstancias que establece el propio artículo 17 RGPD:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

Como vemos, todo este articulado, así como la doctrina existente en esta materia, se ha adaptado a los nuevos tiempos de la tecnología y al nuevo marco social[33]. Como decía ya Diez Picazo en el año 1979, *cuando aún ni se atisbaba el reflejo de la futura era digital, la publicación de la biografía de una persona todavía viva exige su consentimiento y por ello debe exigir cualquier investigación sobre su vida anterior, el apoderamiento de sus datos y el archivo de estos*[34].

2.3. Marco normativo de la protección de datos en España.

2.3.1. Legislación nacional anterior y posterior al Reglamento General de Protección de Datos.

El primer desarrollo legislativo que se realizó sobre el derecho fundamental a la protección de datos se llevó a cabo a través de Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[35]. Su aprobación tuvo en cuenta el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981[36].

El citado Convenio supuso un hito en la regulación de la materia de protección de datos en el ámbito europeo y determinó la aprobación sucesiva de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, ya

---

[33] SANCHO LÓPEZ, M. "Garantías legales del concepto de privacidad: entre el derecho al olvido y el nuevo Reglamento de Protección de Datos" *Revista Actualidad Jurídica Iberoamericana*, nº9, 2018 pp. 233-239.

[34] DÍEZ PICAZO, L. *Derecho y Masificación social. Tecnología y derecho privado (dos esbozos)*. Madrid: Civitas, 1979, pp.114.

[35] BOE Nº 262, 31 de octubre de 1992.

[36] BOE Nº 274, de 15 de noviembre de 1985.

citada anteriormente, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

Estas normativas y, adicionalmente otras dos Directivas europeas[37], se incorporaron al Derecho nacional con la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que derogó la citada LO 5/1992. Esta regulación de 1999 ha sido sustituida, tras la aprobación del RGPD 2016/679, que entró en vigor el 25 de mayo de 2018, por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), que adecua la normativa española al citado RGPD y se convierte en la norma actualmente vigente en nuestro país.

Como comentábamos al inicio de este epígrafe, el primer gran desarrollo legislativo sobre la protección de datos fue en el año 1992. A comienzos de los años 90, los primeros avances tecnológicos necesitaban una respuesta rápida para hacer frente al vacío legal que existía en torno a la protección de datos. El Derecho no podía quedar impasible ante este nuevo fenómeno. Constatado el peligro que suponía un uso arbitrario e indiscriminado de los datos personales por parte de instituciones, empresas, comunicaciones, etc., nacieron las primeras iniciativas legislativas para establecer un sistema de garantías de los derechos y libertades de las personas. Surgen así las denominadas generaciones de leyes de protección de datos personales[38].

Nos remontamos en el tiempo pues a la LO 5/1992, de 29 de octubre, también conocida como LORTAD (Ley Orgánica de tratamiento automatizado de los datos de carácter personal), que culminó un proceso de elaboración doctrinal y normativa que se remonta a 1976. Con esta Ley, el Reino de España cumplía, además, el compromiso asumido con la ratificación del Convenio 108 del Consejo de Europa[39],

---

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

[38] PÉREZ LUÑO, A.E: *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Tecnos, 4ª ed., 1991.

[39] Convenio del Consejo de Europa, abierto a la firma el 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (B.O.E. de 15 de noviembre de 1985).

cuyo artículo 4 obligaba a los Estados parte a dotarse de una ley interna de protección de datos dentro del plazo que el propio Convenio (artículo 22) preveía para su entrada en vigor. La entrada en vigor de esta Ley respondía así mismo a las exigencias derivadas de los Acuerdos de Schengen de 1985, cuyo artículo 117 imponía a los Estados parte la obligación de dotarse de una legislación interna de protección de datos de un nivel como mínimo igual al del Convenio 108[40] y a la Recomendación (87) 15, de 17 de septiembre.

La LORTAD se completó con dos normas reglamentarias: el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal y el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. Se confeccionó también otro Real Decreto, en el año 1999, como desarrollo legislativo de la LO 5/1992, con la finalidad de establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal. Es el denominado Real Decreto 994/1999, de 11 de junio, de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, hoy, lógicamente, derogado.

La Exposición de Motivos de la Ley Orgánica 5/1992 deja entrever la tibia llegada de la tecnología en aquellos años, lo que se denominaba como "recolección y tratamiento de datos", fenómenos, hasta aquel entonces, desconocidos: "*El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero*

[40] Convenio del Consejo de Europa, abierto a la firma el 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal ("B.O.E." de 15 de noviembre de 1985).

que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

En su articulado, concretamente en su artículo 3, la Ley nos ofrecía algunas definiciones que nos permiten conocer el significado de los términos que se manejaban y que hoy en día seguimos manejando, con sustanciales diferencias eso sí. Estos términos son los siguientes:

a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. b) Fichero automatizado: Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) 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.

d) Responsable del fichero: Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

El objeto de la Ley era regular el tratamiento automatizado de los datos de carácter personal; así lo dice su propio título. Como expresa su artículo 1, lo que la ley pretendía era limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de la información en aras de la salvaguarda de los derechos de la personalidad, que el precepto, recogiendo la fórmula del artículo 18.4 de la Constitución, enumera a título indicativo: el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos.

Ahora bien, el término intimidad era utilizado siguiendo el concepto anglosajón *privacy,* no la intimidad de las personas, sino una facultad de disposición sobre la información personal, o datos expresivos de circunstancias o cualidades de la persona. El núcleo del problema que la Ley pretendía resolver era la recogida, la acumulación y el proceso informático de datos de una persona así como la adopción de decisiones que le afectan a partir de un perfil de su personalidad basado en una inferencia automática. La Exposición de Motivos menciona expresamente algunas de estas posibles decisiones como "la obtención de un empleo, la concesión de un

préstamo o la admisión en determinados colectivos". La Ley prevé a tal efecto un sistema preventivo o cautelar tendente a evitar que, por efecto del uso incontrolado de los datos, se produzcan perjuicios a las personas, en lugar de a reparar tales perjuicios a posteriori.

El objeto de la protección venía determinado por los conceptos de datos de carácter personal, fichero y tratamiento. Por datos se entendía "cualquier información concerniente a personas físicas identificadas o identificables". Por tanto, comprendía cualquier modalidad de información, entendida en el sentido de las tecnologías de la información, como conjunto de representaciones codificadas, numéricas, alfabéticas, gráficas, o imágenes, susceptibles de registro, proceso o transmisión. Así, la recogida de imágenes (equipos de control mediante pantallas, filmaciones, etc.) y sus modalidades de tratamiento debían ajustarse a los principios de la ley, siempre que fueran susceptibles de un tratamiento informatizado[41]. Finalmente, la referencia a una persona identificada o identificable convierte los datos personales (género) en "datos de carácter personal" (especie).

En cuanto a los principios de protección que enuncia esta Ley, sientan las bases de los que actualmente comprende nuestra legislación. Se trataba esencialmente de dos: el principio de proporcionalidad y el de transparencia. En cuanto al primero, hacía referencia tanto al aspecto cuantitativo como al cualitativo de los datos con relación a la finalidad del fichero y de los tratamientos -*Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean* ***adecuados, pertinentes y no excesivos*** *en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido* (artículo 4)-. Bien es cierto que no basta con que los datos sean pertinentes y proporcionados cualitativa y cuantitativamente, sino que han de ser recogidos, además, por medios que no sean fraudulentos, desleales o ilícitos. Por lo que se refiere a la transparencia, se trataba esencialmente el conocimiento de la existencia del fichero, de sus fines y del responsable. Estos

[41] HEREDERO HIGUERAS, M. "La LORTAD y su futuro. La Ley Orgánica 5/1992, de 29 de octubre, de regulación de tratamiento automatizado de los datos de carácter personal". Nº 19-22 (1998) (Ejemplar dedicado a: Jornadas Marco Legal y Deontológico de la Informática. Actas (volumen I)), págs. 463-498.

principios fueron formulados por primera vez en las Directrices de la O.C.D.E[42] y recogidos en el Convenio del Consejo de Europa de 1981.

Otro principio, que se mantiene también hoy, es el de la veracidad y exactitud de la información de carácter personal. Los datos han de ser exactos y puestos al día de manera que respondan con veracidad a la situación real del afectado.

El consentimiento del afectado, regulado en el artículo 7, ya era, y sigue siendo, un pilar clave de la protección de datos que la LORTAD optó por incluir entre sus principios. La norma del consentimiento, según se recogía en el artículo 6[43], estaba referida genéricamente al tratamiento de los datos, no sólo a la recogida. Ahora bien, existían excepciones a esta exigencia; así, el consentimiento de la persona no era necesario si el tratamiento lo exige una ley, si los datos se obtienen de fuentes accesibles al público, si la creación de un fichero automatizado es consecuencia de la libre aceptación de la relación jurídica cuyo desarrollo requiera el tratamiento, o si los datos fueran necesarios para el ejercicio de funciones de control y verificación de las Administraciones públicas. En todo caso, el consentimiento era necesario si se trataba de unos datos de determinada naturaleza, los ya entonces denominados *datos sensibles*. ¿Qué se entendía por tales? De acuerdo con el artículo 7, los relacionados con la ideología, la religión, las creencias, el sexo, el origen racial y la vida sexual.

En cuanto a la seguridad de los datos, regulada en el artículo 9 de la LORTAD, fue fruto del articulado del Convenio del Consejo de Europa (artículo 7), que elevó a principio de protección de datos la obligación del responsable del fichero de adoptar medidas de seguridad de los datos. Se trata de medidas de protección de los datos y del entorno (control del acceso a locales, sistemas, programas) y se basaban en varios criterios: naturaleza de los datos, riesgos potenciales y estado de la tecnología. Comprobamos de nuevo que muchas de estas medidas siguen en vigor en la actualidad.

Otro gran bloque de protección fueron los derechos que tenían los afectados, algunos siguen vigentes, pero en su mayoría han sido ampliados o modificados. De todos los derechos o garantías que comprende el Título III, el principal, que, a la vez, constituye la pieza esencial del sistema protector, es el derecho de acceso en

---

[42] Directrices sobre la protección de la vida privada y los flujos transfronterizos de datos de carácter personal, Recomendación aprobada por el Consejo de la O.C.D.E. el 23 de septiembre de 1980, versión española, Madrid, Presidencia del Gobierno, 1983.

[43] Art 6.1 LO 5/1992: *El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.*

sentido amplio o derecho a conocer la mera existencia de un fichero de datos personales (artículo 13), y en sentido estricto o derecho a conocer los datos (artículo 14). Este derecho, curiosamente, goza de una gran importancia en la actualidad. De este derecho emana otros muchos, por ejemplo, es un presupuesto necesario para ejercitar el de cancelación o el de rectificación, regulados ambos en el artículo 15.

Finalmente, con la aprobación de esta Ley, nace en España el primer organismo de protección de datos personales: La Agencia Española de Protección de Datos. El primer atisbo para su creación se encuentra en la Resolución del Parlamento Europeo de 1979[44] y, sobre todo, en la primera propuesta de Directiva comunitaria, cuyo artículo 26 imponía a los Estados miembros la obligación de crear una autoridad encargada de vigilar la aplicación en su territorio de las disposiciones de transposición de la Directiva. El objetivo era la creación de un órgano concreto y específico capaz de asumir el control de la aplicación del sistema protector determinado por la ley.

La labor de la Agencia parece haber estado centrada en el afán de controlar o vigilar a los responsables de los ficheros, en conseguir una notificación total de los ficheros existentes y en el ejercicio de la potestad sancionadora, y no tanto en orientar al afectado, en mediar entre el afectado y el responsable del fichero y en promover un "estilo" de tratamiento de los datos de carácter personal en consonancia con los fines de la LORTAD. El legislador estimó que la única posibilidad de ajustarse al modelo definido en la propuesta de Directiva era la de configurar a la Agencia como una de las llamadas "Administraciones independientes", concepto que comienza a perfilarse en la doctrina. Así, el artículo 34.1 la define como un Ente de Derecho público "que actúa con plena independencia de las Administraciones Públicas en el desempeño de sus funciones", y el artículo 35.2 dispone que su Director "no estará sujeto a instrucción alguna en el desempeño" de sus funciones. En esta línea, el artículo 16 del Real Decreto 428/1993, de 26 de marzo, desarrolla esta doble noción, disponiendo que el Director desempeña su cargo "con plena independencia y objetividad" y que "no estará sujeto a mandato imperativo, ni recibirá instrucciones de autoridad alguna". Esto implica, por tanto, la ausencia de toda relación jerárquica o de tutela.

---

[44] Resolución de 8 de mayo de 1979, del Parlamento Europeo, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática ("D.O.C.E.", no C 140, de S de junio de 1979).

Siete años después de su aprobación y entrada en vigor, la LO 5/1992 fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), que entra en vigor el 14 de enero del 2.000. La primera impresión que se desprende de la lectura de la nueva legislación, es la claridad de su contenido frente al articulado de la ya derogada LORTAD. Esta nueva ley fue, en parte, fruto de la normativa europea, en concreto, de la Directiva 95/46, que creó un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE), fijando límites estrictos para la recogida y utilización de los datos personales. La LOPD nació como proyecto de reforma de la LORTAD, pero acabó su cometido parlamentario como norma que la derogó. Nació, probablemente por ello, sin Exposición de Motivos donde quedasen determinados los objetivos del legislador al tiempo de redactarla, y con cierta polémica parlamentaria.

A nivel conceptual, la LOPD introduce nuevas definiciones referidas, entre otras, al responsable del fichero o tratamiento, al encargado del tratamiento, al consentimiento del interesado, a la cesión o comunicación de datos y a las fuentes accesibles al público. Precisamente, respecto a tales fuentes, el legislador lleva a cabo una enumeración, considerando, con carácter exclusivo, las siguientes: censo promocional, repertorios telefónicos, listas de personas pertenecientes a grupos profesionales, diarios, boletines oficiales y medios de comunicación.

En materia de principios de la protección de datos, hay importantes novedades respecto de la anterior normativa. En este sentido, y para los casos de recogida de datos por persona distinta al interesado, se obliga al responsable del fichero o su representante a informar al afectado, de forma expresa, precisa e inequívoca y dentro de los tres meses siguientes al momento del registro de sus datos, sobre el contenido del tratamiento y la procedencia de los datos.

Del mismo modo que la antigua LORTAD, el nuevo texto partió del principio del consentimiento del afectado para llevar a cabo el tratamiento de los datos de carácter personal, pero ahora dicho consentimiento debía ser inequívoco, claro, indudable. Sin embargo, a diferencia de la anterior normativa en protección de datos, la LOPD declara, en los casos de cesión, la nulidad del consentimiento del afectado siempre que éste no haya sido previamente informado acerca de la finalidad de dicha cesión y del tipo de actividad desarrollada por el cesionario de estos.

Para terminar con el apartado de los principios de la nueva Ley, destacó la obligación impuesta por dicha norma de regular, en contrato escrito, la realización de tratamientos por cuenta de terceros estipulando, expresamente, que el encargado del tratamiento únicamente tratará los datos siguiendo instrucciones del responsable y que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, siquiera para su conservación, a otras personas y, por otro lado, que cumplirá con las medidas de seguridad exigibles para el responsable del tratamiento según las Leyes vigentes.

Los derechos de los afectados, en la LOPD, contienen dos importantes innovaciones que benefician a las empresas responsables de datos de carácter personal por dos motivos: uno, porque se amplía el plazo a diez días (eran 5 días en la LORTAD) para hacer efectivos los derechos de rectificación o cancelación solicitados por los afectados y, dos, porque nace la obligación de conservar los datos de carácter personal durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la entidad responsable del tratamiento y el interesado[45].

Una novedad un tanto confusa, o quizá indeterminada, es que el artículo 7.3 abrió una puerta al tratamiento de datos sensibles referentes al origen racial, la salud y la vida sexual cuando lo establezca una ley, por razones de interés general. Es precisamente en las excepciones donde hay que mirar para ver cuál es el efectivo sistema de protección y de garantías otorgado a los ciudadanos. En esta línea, la posibilidad de tratamiento de datos sensibles se toleró en los supuestos en que existía una habilitación legal por razones de interés general[46]. Por tanto, aquí habría que concretar qué se entiende por interés general; de lo contrario, estaríamos ante un concepto jurídico indeterminado.

Por último, la LOPD siguió recogiendo, como ya sucedía antes, uno de los regímenes sancionadores más duros, si lo comparamos con la legislación aplicable en el resto de países, lo que sigue haciendo necesaria una normativa mucho más sensata en cuanto al importe de las multas, que regularice dicha situación adaptándose, en mayor medida, a la realidad empresarial actual ya que, en definitiva, son las empresas

---

45 MARZO I. "La Nueva protección de Datos". IEE Informáticos Expertos Europeos (2009).

46 SÁNCHEZ BRAVO, A. "La LO 5/1999: 10 consideraciones en torno a su contenido". *Revista de Estudios Políticos (Nueva Época)*, núm. 111, 2001.

españolas las que quedan obligadas, en muchos casos, a paralizar su actividad por no poder afrontar las elevadísimas cifras de las sanciones derivadas de los procedimientos iniciados por la Agencia de Protección de Datos.

El régimen jurídico de la protección de datos personales es muy complejo y requiere de herramientas reglamentarias que concreten las previsiones legislativas. Así, se aprobó, como Reglamento de desarrollo de la LO 15/1999, el Real Decreto 1720/2007, de 21 diciembre, vigente a día de hoy. Como bien dice su Exposición de Motivos, esta norma reglamentaria *nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la misma de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo*.

El 6 de diciembre de 2018, fecha en la que se produce la conmemoración de los 40 años de la Constitución de 1978, se publicó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD). No olvidemos, y así se reconoce en su propia Exposición de Motivos, que esta Ley nace directamente del ya citado Reglamento (UE) 2016/679, General de Protección de Datos (RGPD), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Hubo ciertas demoras en cuanto a su aprobación, ya que la Ley pudo estar lista para su entrada en vigor coincidiendo con la aplicación del RGPD, pero la tramitación parlamentaria se retrasó más de lo esperado a raíz de la imprevista incorporación en el Congreso, vía enmienda, del nuevo Título sobre garantía de los derechos digitales; título sin duda importante, pero que habría justificado la aprobación de una Ley *ad hoc* reguladora de los derechos en la sociedad digital, no de ciertos aspectos de su garantía.

En lo que se refiere al objeto de la Ley, en un principio pretendía adaptar nuestra legislación al RGPD y regular el derecho fundamental a la protección de datos, además de ser una norma más flexible y adaptada a la realidad actual. No debemos olvidar que el artículo 288 del Tratado de Funcionamiento de la Unión Europea señala que los Reglamentos europeos tienen alcance general, son obligatorios en

todos sus elementos y directamente aplicables en cada Estado miembro. Esto implica que la nueva Ley Orgánica no regula por completo el derecho fundamental a la protección de datos, sino que, más bien, desarrolla y adapta en lo necesario el Derecho español al RGPD.

En cuanto a la estructura, es similar a las normativas anteriores. Comienza, lógicamente, con el ámbito de aplicación de los Títulos I a IX (artículos 1 a 78) y de los artículos 89 a 94, que será cualquier tratamiento total o parcialmente automatizado de datos personales, así como el no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Una de las novedades que presenta esta Ley con respecto a las anteriores es que introduce el denominado "testamento digital" referido a las personas fallecidas (artículo 3). Si bien se excluye a éstas del ámbito de aplicación de la LOPDGDD, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a sus datos personales, así como su rectificación o supresión, salvo cuando la persona fallecida lo hubiese prohibido expresamente, prohibición que no opera con los datos de carácter patrimonial.

Por lo que se refiere a los principios relativos a la protección de datos (Título II), quiero hacer referencia al artículo 8 del RGPD, que regula las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información, que indica que el tratamiento de sus datos personales se considerará lícito cuando tenga como mínimo 16 años, si bien ya contemplaba expresamente que los Estados miembros pudieran establecer por ley una edad inferior, siempre que esta no fuera inferior a 13 años. De conformidad con la anterior previsión, en la LOPDPGDD se ha mantenido la edad de 14 años que ya se contenía en la normativa nacional para que el tratamiento de los datos personales de un menor de edad pueda fundarse en su consentimiento.

En cuanto a los derechos de las personas (Título III), se incluye una nueva modalidad en el derecho de información y es la información por capas[47]. Ahora bien, se reduce

[47] La información por capas consiste en dividir la información facilitada a los usuarios en una primera capa más genérica y, una segunda, más detallada. Un enfoque de **doble capa informativa** es útil, ya que permite proporcionar información clave de privacidad de inmediato y tener otra más detallada disponible en otros lugares para aquellos que lo deseen. Esto es particularmente valioso cuando hay espacio limitado para proporcionar más detalles, o si necesitas explicar un complicado sistema de información a las personas.

el contenido mínimo de la capa básica (a la identidad del responsable del tratamiento y de su representante, en su caso; finalidad del tratamiento; y posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD) frente a las recomendaciones de la guía publicada por la AEPD ("Responsable", "Finalidad", "Legitimación", "Destinatarios", "Derechos" y "Procedencia"). Además, se añade que siempre se deberá indicar una dirección electrónica o medio alternativo para acceder de forma sencilla a la restante información.

También se regulan ciertos aspectos del ejercicio de los derechos y, en particular, del derecho de acceso, pero no incorpora regulaciones adicionales relativas al resto de los derechos. Sí que lleva a cabo, en cambio, una explicación más detallada del tratamiento de cierta información (Título IV); así, la de los llamados datos de contacto, los sistemas de información crediticia, los tratamientos relacionados con ciertas operaciones mercantiles, los que tienen fines de video vigilancia, los sistemas de exclusión publicitaria –conocidos como «listas Robinson»[48]– o los de información de denuncias internas. Todos ellos supuestos que cabe integrar dentro de los tratamientos que se presumen lícitos en base al interés legítimo del responsable o de terceros (art. 6.1.f) RGPD). Se incluye también el tratamiento de información con fines públicos; es el caso de los tratamientos de datos en el ámbito de la función estadística pública, el tratamiento para fines de archivo en interés público por parte de las Administraciones Públicas o el tratamiento de datos relativos a infracciones y sanciones administrativas.

El Título V se dedica a la determinación del principio de responsabilidad proactiva, siguiendo el sistema establecido en el RGPD en su artículo 24: *Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento*. Gran parte de su contenido se recogía ya en el Reglamento de desarrollo de la LOPD. Totalmente nueva en relación con el régimen anterior es, sin embargo, la regulación, en los artículos 34 y siguientes, de la figura del delegado de protección de datos (DPD).

---

[48] Se trata de un directorio en el que se almacenan los datos de aquellas personas que quieren dejar de recibir publicidad intrusiva. El objetivo fundamental de la creación de este fichero es proteger al consumidor frente al acoso publicitario https://www.aepd.es/es/areas-de-actuacion/publicidad-no-deseada .

Esta figura fortalece su posición y tiene una labor activa en la resolución de conflictos en materia de protección de datos, ya que, con carácter previo a la presentación de una reclamación contra el responsable o el encargado del tratamiento por los afectados ante la AEPD o, en su caso, ante las autoridades autonómicas de protección de datos, aquéllos podrán dirigirse al delegado de protección de datos de la entidad contra la que se reclame, quien comunicará su decisión adoptada en el plazo máximo de dos meses a contar desde la recepción de la reclamación. Los códigos de conducta y los mecanismos de certificación son también instrumentos relevantes en el nuevo modelo de responsabilidad proactiva, lo que se pone de manifiesto en la regulación que de ambos contienen los artículos 38 y 39 LOPDGDD.

El Título VII es el más extenso y se dedica plenamente a la regulación de las autoridades de protección de datos, tanto la Agencia Española de Protección de Datos como las autoridades autonómicas. Igualmente detallada es la regulación de los procedimientos en caso de posible vulneración de la normativa de protección de datos que recoge el Título VIII. Y, en este punto, debe decirse que la normativa es sumamente confusa, pues emana de forma directa del contenido enunciado en el RGPD.

Finalmente y, sin duda, una de las principales novedades de la norma, el Título X reconoce y garantiza una serie de derechos digitales de los ciudadanos como son, por ejemplo, el derecho a la neutralidad de Internet (artículo 80), el de acceso universal a Internet (artículo 81), el derecho a la seguridad y educación digital (artículos 82 y 83), la protección de los menores en Internet (artículo 84), el derecho de rectificación en Internet (artículo 85), el derecho a la actualización de informaciones en medios de comunicación digitales (artículo 86) y el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (artículo 87), etc.

Como vemos, con esta Ley se adaptan y aclaran algunos conceptos del RGPD y, asimismo, se regulan de forma más específica determinadas cuestiones en el ámbito de la protección de datos en nuestro ordenamiento jurídico. Se trata de un normativa mucho más moderna y adaptada a la sociedad actual con la introducción del testamento digital, tratamiento específico en materia de salud…, pero también plantea algunas cuestiones polémicas como la inclusión de la utilización de medios tecnológicos y datos personales en las actividades electorales mediante la adicción de un nuevo artículo 58 bis en la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. O las dudas que suscita el hecho de contemplar que los responsables enumerados en el artículo 77.1 LOPDPGDD puedan comunicar los datos personales que les sean solicitados por sujetos de derecho privado no solamente cuando cuenten con el consentimiento de los afectados sino también cuando aprecien que concurre en los solicitantes un "interés legítimo" que prevalezca sobre los derechos e intereses de los afectados, puesto que esto puede chocar con el principio de seguridad jurídica.

2.3.2. Los Derechos ARCO.

La gran importancia de este conjunto de derechos ha sido puesta de manifiesto por el Tribunal Constitucional cuando, en dos de sus sentencias (290/2000 y 292/2000), definió el derecho fundamental a la protección de los datos de carácter personal[49]. En la STC 290/2000 se pone de manifiesto la importancia de la protección de datos y su consagración como un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de ellos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Como podemos observar, la doctrina del Tribunal Constitucional es totalmente coherente con los principios básicos de la protección de datos, que fueron sentados con anterioridad en los primeros textos de carácter internacional en la materia, y a través de los cuales se reconocía al titular de

[49] Tribunal Constitucional, Pleno, Sentencia 290/2000 de 30 de noviembre de 2000. Recurso 201/1993. Tribunal Constitucional, Pleno, Sentencia 292/2000 de 30 de noviembre de 2000. Recurso 1463/2000 2000 https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

los datos una serie de facultades o derechos de control sobre el tratamiento de las informaciones relativas a su persona.

No obstante, es ya con las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales del año 1985 y, sobre todo, con el Convenio 1085 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuando se establecen los derechos que suponen un control activo del tratamiento que realiza el responsable del fichero o tratamiento. Es de destacar que los derechos de cancelación y rectificación no se catalogan como garantías independientes. Las posibilidades de rectificar, suprimir y bloquear se mencionan en el artículo dedicado al derecho de acceso, y casi parecen derivarse del ejercicio del propio derecho de acceso.

Desde su entrada en vigor, en abril de 2008, el Real Decreto 1720/2007 (Reglamento de desarrollo de la LOPD) es la disposición de referencia en lo que se refiere al ejercicio de los derechos de acceso, rectificación, cancelación y oposición, y es en este Reglamento, vigente hasta nuestros días, donde se detallan las características comunes a estos derechos, que serían las siguientes:

-Son personalísimos, es decir, en principio, sólo pueden ser ejercidos por el titular del dato o por su representante legal. Ahora bien, curiosamente se admite también la posibilidad de su ejercicio por representante voluntario, *expresamente designado para el ejercicio del derecho*[50].

-Son independientes. El artículo 24.1 del Reglamento de desarrollo de la LOPD establece que «no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro».

-Su ejercicio deberá ser gratuito. El artículo 24.2 del Reglamento de desarrollo de la LOPD señala: «Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición». Continúa

---

[50] Artículo 23 Real Decreto 1720/2007, de 21 de diciembre: *1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado. 2. Tales derechos se ejercitan: 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.*

el tercer apartado del citado artículo prohibiendo, de forma expresa, mecanismos para el ejercicio de derechos impuestos por el responsable del fichero que puedan suponer un coste para el interesado. En concreto y a modo de ejemplo: 1) El envío de cartas certificadas o semejantes[51]. 2) La utilización de servicios de telecomunicaciones que impliquen una tarificación adicional al afectado.

-Su ejercicio debe reunir ciertos requisitos formales enumerados en el artículo 25 del Reglamento de desarrollo de la LOPD, dedicado al procedimiento para cuyo inicio se exige una comunicación dirigida al responsable del fichero. El Reglamento suprime el requisito de hacer llegar la petición al responsable del fichero por cualquier medio que permita acreditar su envío y recepción. Asimismo, elimina la obligación equivalente del responsable del fichero. Sin embargo, la carga de la prueba de la adecuada contestación a la solicitud del interesado recae en el responsable del fichero, tal y como establece el artículo 25.5, lo cual supone una obligación implícita de establecer mecanismos que dejen constancia de la respuesta remitida al titular de los datos. Como se desprende del propio articulado, el responsable deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros, de que se estime el derecho o se deniegue el mismo. Incluso, estará obligado a responder en el caso de recibir una petición de ejercicio de derechos que no cumpla los requisitos legales, en cuyo caso solicitará la subsanación de esta. Este punto que, a priori, no tiene por qué plantear problemas, ha suscitado numerosas reclamaciones ante la AEPD, precisamente por la falta de contestación por parte del responsable hacia el reclamante[52].

---

[51] Hasta la aprobación del Reglamento de desarrollo de la LOPD, la práctica habitual era exigir al interesado que remitiera su petición a través de correo certificado o, incluso, burofax, puesto que la Instrucción 1/1998 determinaba que el derecho debía ejercerse por cualquier medio que permitiera acreditar el envío y la recepción.

[52] Así podemos verlo, por ejemplo, en la Resolución E/07807/2015 de la AEPD ante la entidad TRAVELGENIO S.L. En resumen, un particular denuncia el reiterado envío de correos comerciales por parte de esta agencia de viajes, aun habiéndose dado de baja de la suscripción del boletín semanal con ofertas comerciales mediante el procedimiento que se indicaba en la propia página web. Estas comunicaciones comerciales se remiten a las direcciones de correo registradas en el fichero de clientes en las que no conste que se haya solicitado la baja. Pues bien, para darse de baja existe una casilla que genera un correo electrónico a la entidad y, a su recepción, un empleado de la compañía, manualmente, accede a los datos del fichero de clientes marcándolo como baja para el envío de comunicaciones comerciales. Ahora bien, no se envía ningún mensaje al usuario indicando que la baja ha sido tramitada. La AEPD argumenta, en base al artículo 25 del Reglamento

Es necesario tener en cuenta que, en muchos casos, el particular puede confundir a un mero prestador de servicios con la entidad responsable del fichero, y que no está obligado a conocer las relaciones contractuales que se han establecido entre distintas empresas o, incluso, entre empresas de un mismo grupo empresarial. El artículo 26 del Reglamento de desarrollo de la LOPD dispone que, en el supuesto de que los afectados ejerzan sus derechos ante el encargado del tratamiento, éste dará traslado de la petición al responsable del fichero, a menos que entre ambos exista un acuerdo que implique que aquél atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos.

-Finalmente, el interesado puede denunciar la vulneración de sus derechos a la Agencia Española de Protección de Datos o a la autoridad autonómica que corresponda, como bien dice la Exposición de Motivos de la LO 3/2018.

Una vez vistas las características generales del conjunto de estos derechos ARCO, pasamos a ver las propias de cada uno:

Acceso	Derecho del titular de datos personales a solicitar y obtener gratuitamente información sobre qué datos obran en poder del responsable del fichero, la finalidad de su tratamiento… En definitiva, qué datos tiene y qué hace con ellos.
Rectificación	Derecho del titular de datos personales a solicitar y obtener gratuitamente la rectificación de aquellos datos que obren en poder del responsable del tratamiento y sean incorrectos o no estén actualizados.
Cancelación	Derecho del titular de datos personales a solicitar y obtener gratuitamente el bloqueo de los datos que obren en poder del responsable del tratamiento, considerándose únicamente para la atención de posibles responsabilidades derivadas del tratamiento.
Oposición	Derecho del titular de datos personales a solicitar y obtener gratuitamente el cese en el tratamiento de datos o, en su caso, evitar que se produzca el mismo.

de desarrollo, que "el responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros".

Como ya hemos apuntado, el titular de los datos de carácter personal debe ejercer estos derechos ante el responsable del tratamiento, quien, dependiendo del derecho ejercido, deberá contestar dentro de un plazo concreto:

Acceso	Plazo máximo de un mes a contar desde la recepción de la solicitud.
Rectificación	Plazo máximo de 10 días a contar desde la recepción de la solicitud.
Cancelación	Plazo máximo de 10 días a contar desde la recepción de la solicitud.
Oposición	Plazo máximo de 10 días a contar desde la recepción de la solicitud.

El derecho de acceso actualmente se regula en el artículo 13 de la LO 3/2018 y se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679. Este derecho fue bautizado desde un primer momento, antes de que se promulgaran las primeras leyes de protección de datos, con la expresión *habeas data*, por estimar que constituía una modalidad de acción exhibitoria análoga a la de del *habeas corpus*. Aunque el propio Reglamento de desarrollo de la LOPD señala expresamente que los derechos del interesado son independientes unos de otros, el derecho de acceso puede ser, en muchos casos, el puente que conecta con esos otros derechos. De hecho, tiene un carácter intermedio con respecto a los demás, puesto que "la consecuencia de acceder a los datos y tener conocimiento de su estado puede condicionar el paso siguiente"[53]. Ahora bien, en la práctica, es común solicitar la cancelación de los datos, o bien oponerse al tratamiento, sin tener un conocimiento exacto de qué datos están siendo tratados. En otras ocasiones, se llega a conocer la inexactitud o incorrección de una información por medios distintos al derecho de acceso, por ejemplo, a través de una página web o de un periódico.

En concreto, el individuo debe poder acceder a la siguiente información de acuerdo con el artículo 15 RGPD:

a) los fines del tratamiento,

b) las categorías de datos personales de que se trate,

[53] SERRANO PÉREZ, M. "El derecho fundamental a la protección de datos. Su contenido esencial". *Los derechos fundamentales y las nuevas tecnologías. Anuario multidisciplinar para la modernización de las administraciones públicas*, nº 1, 2005.

c) destinatarios de la información: quién son los encargados del tratamiento y quién tiene acceso a los datos,

d) cesión de datos a terceros: si la información va a ser transferida a un destinatario diferente al que la obtuvo,

e) plazo de conservación de datos: el tiempo que permanecerá la información en los ficheros del responsable y/o destinatario, así como los criterios seguidos para determinar dicho plazo,

f) origen de la información: siempre que no se haya obtenido directamente del interesado,

g) existencia de decisiones automatizadas, lo cual incluye informar sobre la elaboración de perfiles y las consecuencias que dichos tratamientos podrían tener para el interesado.

En esta misma línea, el artículo 27.1 del Reglamento de desarrollo define 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 los datos y las comunicaciones realizadas o previstas de los mismos. Si nos fijamos, esta definición supone, en la práctica, una guía del contenido que deberá reflejar la contestación que el responsable del fichero enviará al afectado en respuesta a su solicitud de acceso. Por otra parte, el interesado, al dirigir su petición, también tiene la posibilidad de elegir el método de acceso: copia remitida por correo electrónico o postal, recogida en mano, tele copia, visualización de pantalla o cualquier otro propuesto por el responsable. Cuando este último no facilite el ejercicio del derecho por el medio elegido por el interesado, la AEPD entiende que no se ha atendido correctamente el derecho de acceso[54].

[54] Veamos un ejemplo, la Resolución AEPD TD/00038/2020: La persona afectada presentó una reclamación frente a la AEPD por considerar que la empresa VODAFONE ESPAÑA, S.A.U. no había atendido como es debido su derecho de acceso. En los hechos probados queda constatado que la parte reclamante ejercita su derecho de acceso siguiendo el procedimiento legalmente establecido para ello, sin obtener respuesta por parte de VODAFONE ESPAÑA S.A.U. En los fundamentos jurídicos, la AEPD se apoya en los

Ahora bien, el acceso puede denegarse en supuestos tasados por el artículo 30 del Reglamento de desarrollo de la LOPD[55]. Al respecto, Serrano Pérez afirma que «ante la ausencia de aclaración alguna, es de suponer que la valoración acerca de lo que constituye un interés legítimo corresponderá al responsable del fichero o del tratamiento"[56].

Por su parte, los derechos de cancelación (o supresión) y rectificación se regulan en los artículos 14 y 15 de la LO 5/2018 y tienen como rasgo común la capacidad de ser una injerencia activa en el tratamiento que realiza el responsable del fichero; característica que comparten con el derecho de oposición. Según Serrano Pérez[57], la diferencia fundamental entre ambos es que, mientras que el derecho de cancelación se ejercita cuando nos encontramos frente a un tratamiento ilegítimo bien porque se dirige a unos fines distintos de aquellos para los que se recabaron los datos, o bien porque estos ya no sean necesarios en relación con dichos fines, el de rectificación procede cuando existe constancia de una inexactitud o carencia. Los resultados de ambos derechos también son diferentes. El primero dará lugar a la supresión del dato. El segundo finalizará con la corrección de la información errónea y, además, como bien dice el artículo 14 LOPDGDD, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse[58].

---

artículos 12 y 15 del RGPD y 13 de la LO 3/2018 en los que básicamente se dice, como hemos comentado anteriormente, que el interesado tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando, o no, datos personales que le concierne y, cuando el responsable trate una gran cantidad de datos relativos al afectado y éste ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los mismos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique a qué datos o actividades de tratamiento se refiere dicha solicitud. En este supuesto, lógicamente, se estimó la reclamación y, un tiempo después, la parte reclamante ejercitó su derecho de acceso y, transcurrido el plazo establecido conforme a las normas antes señaladas, su solicitud obtuvo la respuesta legalmente exigible.

[55] Art 30 RDLOPD 1720/2007: *El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto. 2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.*

[56] SERRANO PÉREZ, M.: *El derecho fundamental a la protección de datos. Derecho español y comparado*. Madrid: Thomson Civitas. 2003, pp. 353.

[57] SERRANO PÉREZ, ob. cit., pp. 357 y 358.

[58] Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Con la LOPDGDD, el derecho de supresión se configura de tal manera que no da lugar al borrado o eliminación directa de los datos. En la mayor parte de los supuestos, los datos no se borrarán, sino que serán bloqueados. Si bien el RGPD no hace mención expresamente al bloqueo de los datos, en su artículo 17.3 sí se considera su "retención", configurándose ésta como excepciones al derecho de supresión cuando se haya solicitado por parte del interesado, en el caso de que el tratamiento sea necesario para:

- el ejercicio de la libertad de expresión e información,
- para el cumplimiento de una obligación legal,
- para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable,
- por razones de interés público en el ámbito de la salud pública,

-con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

-para la formulación, el ejercicio o la defensa de reclamaciones.

En cuanto al derecho de oposición, cabe señalar que no es nuevo, puesto que ya existía en la Directiva 95/46 y en la LO de 1999, y permite al interesado, en los casos previstos en el Reglamento (UE) 2016/679 (artículo 21), oponerse al tratamiento de sus datos personales aunque los datos se traten lícitamente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, o por motivos de intereses legítimos del responsable o de un tercero[59]. También podrá hacerlo en el supuesto de que los datos personales sean tratados con fines de mercadotecnia directa, incluyendo la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia, y ello en cualquier momento y sin coste alguno[60]. Por tanto, el

[59] Sobre el interés legítimo como base jurídica para el tratamiento de datos, puede verse el Considerando 47, que pone como ejemplo la existencia de *una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable.*

[60] Vid. Considerandos 69 y 70 RGPD.

afectado podrá en todo momento instar a que el responsable de los datos cese en el tratamiento de los suyos. Ahora bien, en el primer caso, tienen que darse dos requisitos, el relativo a la existencia de motivos relacionados con la situación particular del interesado y que el responsable no acredite la existencia de *motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, lo que obviamente requerirá llevar a cabo una ponderación específica, o para la formulación, el ejercicio o la defensa de reclamaciones.*

3. El derecho al olvido digital.

3.1. Concepto y fundamento.

El derecho al olvido, también conocido como el derecho a ser olvidado, es un derecho que poseen las personas físicas de hacer que se elimine una información concreta sobre ellas después de un periodo de tiempo. Ciertamente, se entiende que las personas tienen derecho a que se olvide la existencia de una serie de hechos acaecidos en el pasado y que no quieren que sean recordados de forma permanente[61]. En definitiva, se trata del derecho a solicitar que, en determinados casos, se supriman los datos personales que circulan por Internet ante el riesgo de que ello suponga la vulneración de los derechos al honor y a la intimidad personal[62]. En esencia, es el propio derecho a la autodeterminación informativa, también conocido como el derecho a la protección de datos de carácter personal[63]. Por tanto, el ciudadano esgrime, frente a terceros, este derecho a la protección de sus datos para pedir la

---

[61] CÓRDOBA CASTROVERDE D. "Los retos de la protección de datos en Internet. Caso Google Spain y derecho al olvido". *Afduam 21*, 2017, pp. 236-237.

[62] MURGA FERNÁNDEZ J.P "La protección de los datos personales y los motores de búsqueda en Internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido". *Revista Derecho Civil*, Vol., IV, nº4, octubre-diciembre 2017, pp. 181-209.

[63] TORRES MANRIQUE, J.I. "Analizando el derecho fundamental al olvido a propósito de su reciente reconocimiento y evolución". *Revista de Derecho y C. Sociales*, nº 13, 2017, pp. 209-231.

cancelación de una determinada información Son múltiples las razones por las que una persona puede considerar que una información, imagen o noticia, incluso aquella que puede parecer inofensiva, puede entrometerse en su intimidad personal y afectar a su dignidad.

El derecho al olvido se configura como subjetivo, novedoso y transversal[64]. Quizá no se debería considerar novedoso puesto que ya existía, si bien es cierto que la novedad es que, dados los tiempos actuales, su importancia es mucho mayor debido a la existencia del fenómeno Internet. Aunque es también un derecho personalísimo de cada individuo, no es absoluto, ya que su reconocimiento no puede llevarnos a posibilitar la construcción de un pasado a la medida de cada cual[65].

El fundamento del derecho al olvido es, como ya he apuntado, el derecho a la protección de datos reconocido constitucionalmente de forma generalista en el apartado 4 del artículo 18 de la Constitución. Nuestro Tribunal Constitucional entiende que el referido precepto «garantiza a la persona un poder de control y disposición sobre sus datos personales», el cual tiene como contenido esencial «una serie de facultades de su titular como consentir la recogida y el uso de sus datos personales, conocer los mismos, ser informado de quién los posee y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo que ponga fin a la posesión y empleo de tales datos»[66].

La sensibilidad sobre el público conocimiento y difusión de hechos pasados con datos personales, incluso transcurrido un lapso importante de tiempo, no funciona, o no es la misma en todos los países. Normalmente los ordenamientos europeos, optan por limitar estos datos personales del conocimiento público, permitiendo un acceso más limitado y su eventual cancelación. Pongamos un ejemplo: ¿Qué tiene en común un abogado que fue embargado por deudas a la Seguridad Social, un

---

[64] La transversalidad característica del derecho al olvido queda reflejada en el denominado "Código de derecho al olvido" disponible en el portal del BOE; a saber, una recopilación de las principales normas referentes al mismo teniendo en cuenta los diferentes ámbitos en los que se puede plantear.

[65] Como afirma la STS de 6 de julio de 2017(RJA 426/2017): "*El derecho al olvido no ampara la alteración del contenido de la información que ha sido lícitamente publicada, en concreto se refiere al borrado del nombre y apellidos o cualquier otro dato que consta en la misma*".

[66] Sentencia del Tribunal Constitucional de 30 de noviembre del 2000 [RTC\2000\290].

hombre cuya discapacidad aparece en un motor de búsqueda, un imputado en un proceso judicial que posteriormente ha sido absuelto, o un ciudadano perteneciente a una Red Social? La respuesta es simple: todos aparecen en el índice de resultados de los principales motores de búsqueda y, en la mayoría de estos casos, el titular de los datos publicados en la red no desea que los mismos aparezcan en este medio[67].

Las situaciones anteriormente descritas, surgen por la posibilidad que otorgan los motores de búsqueda de lo que conocemos por «googlearse» –buscar el nombre propio o el de otra persona en un motor de búsqueda, para comprobar qué resultados aparecen-; dicha práctica recibe también el nombre de «egosurfing»[68]. La mayoría de las veces son otros los que buscan nuestra información para muy diversos fines, por ejemplo, esta práctica se ha extendido en departamentos de recursos humanos que pretenden, a través de este medio, obtener más información del candidato, pero también lo realizan terceras personas, ajenas al usuario, por mera curiosidad.

Por tanto, la justificación de este derecho se basa en la fe en la capacidad del individuo de reinsertarse, de cambiar y mejorar, así como en la clara convicción de que el ser humano no puede reducirse meramente a su pasado[69]. El planteamiento expuesto nos lleva a valorar si este tipo de información personal debe ser publicada por los motores de búsqueda, convirtiéndose de este modo en accesible al público en general, debiendo tenerse en cuenta, para realizar una valoración adecuada, si ha transcurrido un importante periodo de tiempo entre el hecho y su publicación. Y lo más importante, si se cumple la exigencia constitucional de la protección de datos personales de los ciudadanos. Nace así el derecho al olvido, que tiene como finalidad «que el pasado no se convierta en presente continuo»[70].

---

[67] MATE SATUÉ, L.C. "¿Qué es realmente el Derecho al Olvido?". *Revista Derecho civil*, vol. III, nº 2 abril-junio 2016, Ensayos, pp. 187-222.

[68] Jerga habitual en Internet que hace referencia a la práctica de buscar nuestro propio nombre en bases de datos, medios escritos, Internet, etc. para comprobar la información que se acumula sobre nuestros datos personales.

[69] DE TERWAGNE, C. "Privacidad en Internet y el derecho a ser olvidado/derecho al olvido". *Revista de los Estudios de Derecho y Ciencia política de la UOC*, nº 13, febrero 2012, pp.55.

[70] MITJANS I PERELLÓ, Congreso Internacional sobre Internet, Derecho y Política: "Neutralidad de la Red y Derecho al olvido".

La difusión en Internet es global y, por tanto, los contenidos difundidos pueden ser capturados desde todo el mundo, siendo accesibles a un número indefinido de internautas, lo que puede generar un daño exponencialmente mayor que con otros medios de difusión[71]. En nuestro día a día, compartimos constantemente cantidades ingentes de información y podemos acceder a ella inmediatamente y prácticamente desde cualquier dispositivo electrónico conectado a Internet. Una vez los datos son incorporados a la Red, circulan libremente pasando de unas bases de datos a otras y de un servidor de Internet a otro[72]. Este fenómeno ha sido bautizado por el Profesor Troncoso como "efecto Hotel California": *you mayo enter, but you may never leave*[73].

La problemática del derecho al olvido suele surgir casi siempre en relación con un contenido personal publicado en Internet, que, al ser indexado por un buscador, alcanza una amplia difusión y afecta de forma negativa a la persona, vulnerando así su derecho a la protección de datos. Entre todos los datos que circulan por la Red, existe una cantidad significativa que son de contenido personal y, por tanto, con capacidad propia para identificarnos. Así, este tipo de datos, debido al volumen de información que manejan, se ha revelado como un negocio en auge, revolucionando la mercadotecnia y las estrategias de marketing con fines comerciales, pero, eso sí, provocando en numerosas ocasiones consecuencias negativas para algunos derechos fundamentales.

En el entorno del derecho al olvido digital en Internet figuran cuatro sujetos implicados, que son:

1º) *Editor*: es quien publica la información en Internet que se considera dañina o intempestiva por parte del afectado.

---

[71] A este respecto, la Sentencia del Tribunal de Justicia de la Unión Europea, de 25 de octubre de 2011, reconoce que «*el daño que producen los contenidos vertidos en Internet es mayor que el que producen los contenidos difundidos en prensa, porque, en el primer caso, el contenido está disponible en cualquier punto del planeta, mientras que no es así en el segundo caso*».http://curia.europa.eu/juris/liste.jsf?language=es&num=C-509/09

[72] SANCHO LÓPEZ M. "Garantías legales del concepto de privacidad. Entre el derecho al olvido y el nuevo Reglamento Europeo de Protección de datos". *Actualidad jurídica iberoamericana*, nº9, agosto 2018, pp. 176-201.

[73] TRONCOSO REIGADA, A. *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch, 2008.

2º) *Motor de búsqueda*: es la persona jurídica cuya actividad empresarial consiste en clasificar y mostrar ordenado el contenido de Internet a sus usuarios. Normalmente, lo hace mediante la presentación de aquél en una lista de resultados adaptada a la búsqueda de los usuarios. El buscador que mayor impacto tiene en España lógicamente es Google, aunque también existen otros con una aceptación más que amplia como son Bing o Yahoo.

3º) *Internauta*: es la persona que navega por Internet y que accede a la información publicada por un editor, bien directamente, o bien a través de la lista de resultados ofrecida por el buscador.

4º) *Afectado o protagonista del mensaje o información implicada*: es la persona que resulta mencionada en el contenido y que ve afectados sus derechos por aquél, y que, por ello, pretende su supresión o el enlace al mismo[74].

En definitiva, Internet es el caldo de cultivo perfecto para la proliferación de datos personales así como la memoria virtual y permanente que conforman los motores de búsqueda online y que suponen un almacenamiento, procesamiento y transferencia de información personal. Por tanto, esta nueva era tecnológica, la denominada era "post-privacy", obliga al Derecho a renovar sus mecanismos de protección de los derechos fundamentales y a reformular conceptos jurídicos como intimidad, o vida privada, cuyo significado se ha visto claramente alterado, configurándose así nuevas construcciones jurídicas que refuercen el control por parte de las autoridades de nuestros datos personales[75].

3.1.1. Construcción jurisprudencial del derecho al olvido.

El derecho al olvido es una mera creación jurisprudencial que surge como respuesta a las reiteradas vulneraciones de los derechos fundamentales, especialmente de la privacidad, que los usuarios padecen en Internet. Por tanto, el reconocimiento de

---

[74] MARTINEZ OTERO J.M. "La aplicación del derecho al olvido en España tras la STJUE Google contra AEPD y Mario Costeja". *Revista Bolivariana de Derecho*, nº 23, enero 2017, pp.112-133.

[75] SANCHO LÓPEZ. "Garantías legales del concepto de privacidad: entre el derecho al olvido y el nuevo Reglamento europeo de protección de datos". *Actualidad Jurídica Iberoamericana*, nº9, 2018 pp. 176-202.

este derecho se debe, en gran medida, a pronunciamientos jurisprudenciales valientes y modernos, adecuados y coherentes con los nuevos tiempos.

Las interpretaciones doctrinales y jurisprudenciales que hicieron emerger este nuevo derecho giraron en torno al derecho a la protección de datos, noción consolidada en nuestra tradición jurídica y cuyo reconocimiento se extiende por la inmensa mayoría de legislaciones nacionales de nuestro entorno, así como en el propio marco europeo, de igual modo que el derecho a la intimidad, al honor y a la dignidad. Fue el TJUE el que reconoció por primera vez el derecho al olvido, en la sentencia de 13 de mayo de 2014 (Google INC vs Agencia Española de protección de datos), más conocida como "caso Google" -sentencia que será abordada con detalle en el último epígrafe del presente trabajo-. Emerge así en el contexto europeo el derecho al olvido como un nuevo derecho ligado a la defensa de la privacidad de los ciudadanos en el ámbito de Internet, como una reacción a la atemporalidad de los datos personales en la Red, como una garantía frente a su tratamiento masivo y descontrolado[76]. El reconocimiento jurídico de la existencia de un derecho al olvido de la información no relevante contenida en la web por parte de los buscadores como Google, puede ser el primer paso a la hora de garantizar la privacidad de los datos de los internautas en este nuevo contexto tecnológico.

Ahora bien, este derecho tendrá unos límites distintos en función de la tradición jurídica del país que lo regule. En estados civilistas, su configuración y aplicación genera menos problemas, lo que favorece su reconocimiento por las agencias de protección de datos. De este modo, el derecho a la protección de datos persigue garantizar al individuo un poder de control sobre sus datos personales, no sólo desde el punto de vista de su uso sino también de su destino, con el fin de impedir una lesión de su dignidad y derechos

En nuestro país, el Tribunal Constitucional pone de manifiesto la configuración y protección del bien jurídico privacidad, de la que derivan facultades de control sobre los datos e informaciones del individuo —como recogen, entre otras, las sentencias

[76] SIMÓN CASTELLANO, P. "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", en VV. AA Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales, Cuadernos y Debates, nº 215, Centro de Estudios Político-Constitucionales, Madrid, 2013, p. 452.

254/1993[77], 11/1998, 94/1998, 104/1998 o 44/1999-. Es decir, en el caso de la privacidad electrónica, nos encontramos ante una situación de desprotección de los usuarios de Internet, lo que revierte directamente en el ámbito de la dignidad individual[78].

Ya la pionera STC 254/1993 configuró y reconoció el contenido constitucional de lo que se conoce en la doctrina y jurisprudencia comparadas como derecho a la autodeterminación informativa: "De *este modo, nuestra CE 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 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 CE llama "la informática"* (FJ 6º).

3.2. Los límites del derecho al olvido.

El derecho al olvido puede entrar en colisión con otros derechos y libertades que, en nuestro ordenamiento jurídico nacional y europeo, tienen distinto rango; entre ellos, podemos destacar, la libertad de información, la libertad de expresión, la libertad de empresa, la prohibición de discriminación y el derecho de propiedad. Por otra parte, el derecho al olvido tiene una estrecha interrelación con algunos derechos personalísimos cuya protección ha contribuido a la creación de aquél. El afectado puede ver vulnerados, como hemos comentado en repetidas ocasiones, su derecho a la protección de datos (artículo 18.4 CE), su honor, su intimidad personal y familiar, y su propia imagen (artículo 18 CE), también el derecho a la integridad física

---

[77] La STC 254/1993, de 20 de julio, ha concretado, no sin cierta confusión, el contenido constitucional de lo que se conoce en la doctrina y jurisprudencia comparadas como derecho a la autodeterminación informativa. http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383.

[78] LÓPEZ PORTAS, B. "La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE". *Revista de Derecho Político*, nº93, mayo-agosto 2015, pp.143-175.

o psíquica (artículo 15 CE) y al libre desarrollo de su personalidad[79]. Todos tenemos derecho a que se nos respete cualquiera que haya sido nuestra trayectoria de vida. Por tanto, el derecho al olvido podría activarse cuando se produce una vulneración de estos derechos, por ejemplo, el derecho al honor; así, cuando se nos difama a través de una página web, el afectado podrá ejercitar el derecho al olvido (sobre Google) para que deje de indexar[80] la información, y el derecho de cancelación sobre el editor web. Además, la aplicación del derecho al olvido no significa que se materialice el borrado de los datos personales, sino que lo que hace es dejar de indexarlos o de conectar al internauta con los mismos[81].

Ahora bien, ocurre que aquí el derecho al olvido puede chocar con la libertad de información (naturaleza objetiva del mensaje), o con la libertad de expresión (naturaleza subjetiva), del editor que publica un contenido. Por su parte, el usuario que busca y accede a un contenido en Internet está ejerciendo sus derechos de información regulados en el artículo 20.1 CE. Finalmente, el buscador de Internet está ejercitando, sin lugar a dudas, su derecho a la libertad de empresa establecido en el artículo 38 CE, puesto que es su actividad profesional, aunque podría tener cabida también como derecho comunicativo por su protagonismo en la efectiva difusión y acceso a un determinado mensaje.

Como vemos, el principal conflicto que se trata de solventar es el que enfrenta los derechos del editor, del buscador y del usuario. El editor y el internauta, al publicar y acceder a la información, ejercen derechos informativos. El buscador, por su parte, al ordenar los resultados. El buscador, por su parte, al ordenar los resultados, ejerce el derecho de libertad de empresa y también el derecho de información en su vertiente pasiva. Por último, el afectado esgrime su derecho a la protección de datos, normalmente en relación con el derecho al honor, a la intimidad y a la privacidad.

---

[79] SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital* Valencia: Tirant lo Blanch, 2012, pp. 116 y ss.

[80] Indexación: proviene del anglosajón índex que significa índice en español. Es realizar determinadas acciones enfocadas a que los buscadores identifiquen las páginas de tu sitio con una temática determinada. A partir de la asignación de temática Google, u otros buscadores, te asignan una categoría específica en sus listados de resultados.

[81] SEISDEDOS POTES, V. "Derecho al Olvido. Jaque a Google en Europa". *Cuadernos de Dereito Actual*, nº 2, 2014, pp.119-121.

El criterio jurisprudencial y doctrinal fijado es que no existen derechos absolutos, de modo que, cuando existe una colisión o conflicto entre ellos, se utiliza la herramienta de la ponderación para ver qué derecho prevalece[82]. En el caso del que hablábamos, habría que valorar si es preferible la accesibilidad de la información en la Red, o proteger los derechos de la persona afectada[83]. No toda la información es relevante ni tiene la misma naturaleza.

Un ejemplo de conflicto sería el derecho al olvido de los antecedentes penales: Un usuario anónimo introduce un nombre aleatorio en Google y, en el primer enlace que aparece en la lista de resultados, hay una noticia de hace diez años que cuenta que dicha persona se dedicaba al contrabando de armas y fue condenado, estando en la cárcel en reiteradas ocasiones. Imaginemos que, con el transcurso del tiempo, el condenado ha rehecho su vida, se ha reinsertado y la información que en su día se publicó ya no responde a la situación actual, pero sigue apareciendo en Internet. Aquí el derecho al olvido entra de nuevo en conflicto con el derecho a la información, y el tiempo es, en este caso, la herramienta de ponderación para resolver el conflicto.

El derecho al olvido debe dar prioridad a las exigencias del derecho a la información cuando los hechos que se revelen sean, o presenten, un interés específico, que está vinculado, en este caso, al interés periodístico de los hechos en concreto. Pues bien, cuando ya no se trate de una cuestión de actualidad, o potencialmente noticiable, y siempre y cuando ya no exista una razón legítima que justifique una nueva divulgación de la información, el derecho al olvido anula el derecho a la información. No obstante, se puede comentar la noticia, pero sin dar los nombres de las partes o identificarlos de alguna manera. En síntesis, el valor informativo de un caso inclina la balanza a favor del derecho a difundir a costa del derecho al olvido. Y, en cuanto esa noticia deje de tener relevancia, valor como noticia, etc., la balanza se inclinara en la otra dirección[84]. Se pueden admitir dos excepciones en las que el derecho al

---

[82] El carácter limitado de los derechos fundamentales fue reconocido muy tempranamente por la jurisprudencia constitucional. Así, la STC 11/198, de 8 de abril, señala, en su FJ7: *"(…) ningún derecho, ni aun los de naturaleza o carácter constitucional, pueden considerarse como ilimitados*". https://hj.tribunalconstitucional.es/esES/Resolucion/Show/11#complete_resolucion&fundamentos

[83] MARTINEZ OTERO J.M, "La aplicación del derecho al olvido en España tras la STJUE Google contra AEPD y Mario Costeja". *Revista Bolivariana de Derecho*, nº 23, pp.112-133.

[84] Vid. en este punto la STS de 5 de abril de 2016.

olvido será anulado por el derecho de información[85]: 1) Para los hechos relacionados con la historia, o cuando se trate de un tema de interés histórico. 2) Para los hechos vinculados al ejercicio de la actividad pública por parte de una figura pública.

4. El Caso Google y la responsabilidad del tratamiento de los datos personales.

4.1. STJUE 13 de mayo de 2014 contra AEPD y Mario Costeja: Los hechos.

Comenzamos a comentar la ya conocida sentencia que supuso un antes y un después en la forma de concebir el derecho al olvido digital.

El origen de los hechos se remonta al año 1998, cuando el periódico la Vanguardia publicó en dos anuncios, con distintas fechas, 19 de enero y 9 de marzo, información relativa a una subasta de inmuebles relacionada con el embargo al Señor Costeja como consecuencia de unas deudas que aquél tenía con la Seguridad Social. La publicación mencionaba al Señor Costeja, de nacionalidad española y domicilio en España, así como que era el titular de los bienes inmuebles subastados. Poco tiempo después, la editorial puso a disposición del público una versión electrónica del periódico. Lógicamente, esta publicación era un tanto incómoda para el interesado, pero, pese a ello, en un principio, entiende que la información es legal e idónea para la publicidad de la subasta. El problema surge cuando, con el paso del tiempo y desde el momento en el que dicha editorial saca una versión online de su periódico, los anuncios comienzan a ser indexados por Google y ofrecidos en sus listas de resultados, apareciendo así búsquedas asociadas al Señor Costeja y a las subastas. Por tanto, aquí es donde se encuentra el punto clave del asunto, el carácter sensible de informaciones que, en su día, fueron veraces y oportunas, pero que, con el paso del tiempo, han dejado de serlo[86]. Ocurre, sin embargo, que la memoria total de

[85] DE TERWAGNE C. "Privacidad en Internet y el derecho a ser olvidado /derecho al olvido". *Revista de los Estudios de Derecho y ciencia política de la UOC*, nº13, febrero 2012, pp. 53-55.

[86] En efecto, normalmente los contenidos que pretenden suprimirse son informaciones pretéritas cuya publicación estuvo justificada en un momento dado del pasado, pero que han perdido actualidad y cuya inmediata disponibilidad en Internet, el interesado considera excesivamente gravosa.

Internet y el poder de los buscadores impiden que dicha información se quede en el olvido.

Volviendo al Señor Costeja, más de una década después del embargo solicitó tanto a La Vanguardia, concretamente en el año 2009, como a Google la retirada de Internet del contenido y los enlaces, a fin de preservar su honor y la protección de sus datos en la Red. La editorial no accedió a la cancelación de dichos datos puesto que la citada publicación se había realizado por orden del Ministerio de Trabajo y Asuntos Sociales y su objetivo era dar la máxima publicidad posible a las subastas y lograr, así, un amplio número de licitadores. Aunque La Vanguardia no accediera, el Señor Costeja lo intentó por el otro lado y redactó un escrito a *Google Spain* solicitando que se tomasen las medidas idóneas para que no apareciese su nombre y apellidos en el motor de búsqueda y cualquier usuario pudiese, a través de esos enlaces, acceder a las subastas. *Google Spain* le remitió a *Google Inc.*, con domicilio social en California, Estados Unidos, por entender que ésta era la empresa que presta efectivamente el servicio de búsqueda en Internet, es decir, que ella era el prestador de servicio[87]. *Google Spain* alegó que su actividad se limitaba a la venta de espacios publicitarios en Internet y que, como tal, únicamente actuaba como representante comercial de *Google Inc.* para sus actividades publicitarias; concretamente, para la gestión de *AdWords*, un sistema de publicidad a partir de palabras clave[88]. Por todo

---

[87] **Prestador de Servicios:** Persona física o jurídica que proporciona un servicio de la sociedad de la información. Se consideran prestadores de servicios de la sociedad de la información, conforme a la Exposición de Motivos de la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico:

- Los operadores de telecomunicaciones.
- Los proveedores de acceso a Internet.
- Los portales.
- Los motores de búsqueda.
- Cualquier sujeto que disponga de un sitio en Internet.

Desde un punto de vista objetivo, los prestadores de servicios se caracterizan por las actividades que desarrollan o servicios que prestan.

[88] En relación con el funcionamiento de este tipo de sistemas publicitarios y la posible infracción de derechos de marca en Internet, véanse las Sentencias del Tribunal de Justicia de la Unión Europea de 23 de marzo de 2010, asunto Google Francia y Google, asuntos acumulados C-236/08 a 238/08, apartados 22-23; de 25 de marzo de 2010, asunto BergSpechte, C-278/08, apartados 5-7; de 8 de julio de 2010, asunto Portakabin, C-558/08, apartados 8-10; y de 22 de septiembre de 2011, asunto Interflora British Unit, C-323/09, apartados 9-13.

ello, *Google Spain* entendía que su responsabilidad debía quedar limitada al tratamiento de los datos personales relativos a sus clientes españoles de servicios publicitarios[89].

Con esta situación, el Señor Costeja presentó una reclamación ante la Agencia Española de Protección de Datos contra La Vanguardia Ediciones, S. L. y contra *Google Spain* y *Google Inc.* En ella solicitaba, por un lado, que se exigiera a La Vanguardia eliminar, o modificar, las dos publicaciones controvertidas para que no aparecieran sus datos personales o, subsidiariamente, que se exigiera al periódico la utilización de herramientas para proteger los mismos[90]. Mediante Resolución de 30 de julio de 2010, el Director de la Agencia Española de Protección de Datos estimó la reclamación formulada por el interesado contra *Google Spain* y *Google Inc.*, instando a ambas a adoptar las medidas necesarias para retirar los datos de sus listas de resultados e imposibilitar el acceso futuro a los mismos.

En este caso, la AEPD consideró, con muy buen criterio, que quienes gestionan motores de búsqueda son responsables del tratamiento de datos personales y, por ende, están sujetos a la normativa en materia de protección de datos. Con base en ello, la AEPD acepta que el requerimiento se pueda dirigir directamente a los explotadores de motores de búsqueda sin suprimir los datos o la información de la

---

89 Este mismo argumento territorial es empleado sistemáticamente por el resto de las empresas que gestionan motores de búsqueda contra las que llegan solicitudes a la Agencia Española de Protección de Datos, entre otros Yahoo y Bing. El segundo suele alegar que tiene su sede operativa en Luxemburgo y que, por lo tanto, no le afecta la legislación española. Por su parte, Yahoo se remite a un acuerdo que posee con Microsoft Corp. en virtud del cual toda reclamación presentada contra ella debe entenderse contra Microsoft Corp y, por ello, realizarse en su sede de Redmond, Washington, Estados Unidos.

90 Lo que el TJUE denomina en su sentencia como "herramientas facilitadas por los motores de búsqueda para proteger esos datos personales" no son otra cosa que protocolos de industria conocidos como robots.txt o códigos de exclusión, al alcance de cualquier programador, que impiden que el robot del buscador encargado de la indexación automática de contenidos –araña web–cree resultados de búsqueda partiendo del nombre y apellidos de una determinada persona. El uso de este tipo de códigos indica que el *Webmaster* de esa página web no desea que determinada información de la página fuente pueda ser recuperada para su difusión a través de motores de búsqueda. Sin embargo, los códigos de exclusión no son infalibles, pues no impiden técnicamente la indexación, sino que el proveedor del servicio que gestiona un motor de búsqueda puede decidir ignorar. Se trata de una suerte de "pacto de caballeros" entre los *Webmasters* que utilizan el robot.txt y el motor de búsqueda, que suele ser cumplido por los más importantes motores de búsqueda. Véase el Dictamen 1/2008 del Grupo de Trabajo del Artículo 29, p. 14.

página donde inicialmente esté alojada si el mantenimiento de esa información en dicha página está justificado por una norma legal. Por ello, la citada Resolución desestimó la reclamación contra la editorial, por entender que la publicación tenía una justificación legal, al haberse realizado por orden del Ministerio de Trabajo y Asuntos Sociales.

Por su parte, Google interpuso un recurso ante la Audiencia Nacional, que, antes de resolver sobre el fondo del asunto, trasladó una serie de cuestiones prejudiciales al TJUE en relación con la correcta interpretación de la normativa comunitaria en materia de protección de datos. El Tribunal remitente expone en el Auto de remisión que los recursos plantean la cuestión de cuáles son las obligaciones que tienen los gestores de motores de búsqueda en relación con la protección de los datos personales de aquellos interesados que no desean que determinada información, publicada en páginas web de terceros y que contienen sus datos personales, sea localizada, indexada y puesta a disposición de los internautas de forma indefinida.

El Tribunal nacional plantea un total de tres cuestiones prejudiciales:

1) Si es posible aplicar la normativa nacional debido al ámbito geográfico del litigio (recordemos que *Google Spain* es una empresa filial de la principal o matriz, que es *Google Inc.*, cuya sede central se encuentra en Mountain View, California).

2) Si la actividad de un motor de búsqueda como proveedor de contenidos, que consiste en hallar información publicada en Internet, indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse como "tratamiento de datos personales" y cuál es el grado de responsabilidad de los gestores de los motores de búsqueda.

3) Si la Directiva 95/46 permite al interesado exigir al gestor del motor de búsqueda que elimine, de la lista de resultados obtenida como consecuencia de una búsqueda efectuada a partir de su nombre, vínculos a páginas web que contengan información relativa a su persona, verídica y lícitamente publicada, pero que pueda perjudicarle.

4.2. Valoración del Abogado General y del TJUE.

Las preceptivas conclusiones del Abogado General, que fueron publicadas el 25 de junio de 2013, se mostraron completamente contrarias al derecho al olvido. El primer problema tiene que ver con la aplicabilidad del principio de territorialidad de la Directiva 95/46 (artículo 4), vigente por aquel entonces. El ámbito territorial de esta norma viene determinado, bien por la ubicación del establecimiento del responsable del tratamiento de datos personales en un Estado miembro, bien por la ubicación en territorio europeo de los medios, o del equipo, que se estén utilizando cuando el responsable del tratamiento esté establecido fuera del Espacio Económico Europeo. Por tanto, la nacionalidad o el lugar de residencia habitual de los interesados no son decisivos[91].

El Sr. Niilo Jaaskinen, a la hora de interpretar el concepto "establecimiento", aboga por tener en cuenta la perspectiva del modelo de negocio de los buscadores, basada en su principal fuente de ingresos, que no es otra que la publicidad a partir de palabras clave, para lo cual un motor de búsqueda necesita tener presencia en los mercados nacionales del sector de la publicidad, a través de sus filiales[92]. Sostiene que se lleva a cabo tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable del tratamiento cuando la empresa que provee el motor de búsqueda establece en un Estado miembro, con el fin de promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes u operadores de ese país[93].

En cuanto al tratamiento de los datos personales, teniendo en cuenta que los datos sobre los que se origina el litigio fueron publicados en páginas web fuente de terceros, y no así por Google, las operaciones llevadas a cabo por el motor de búsqueda consistentes en la recopilación, grabación, organización y almacenamiento de los contenidos de la página web fuente y, por ello, de los datos personales en

---

[91] Dictamen 8/2010, sobre el Derecho aplicable, del Grupo de Trabajo del Artículo 29, p.8; y Conclusiones del Abogado General Niilo Jääskinen, presentadas el 25 de junio de 2013, apartado 58.

[92] Conclusiones del Abogado General, apartado 64. Por este motivo, entiende que el análisis ha de llevarse a cabo considerando al operador económico que lleva a cabo la función de búsqueda y la labor publicitaria como una única unidad (apartado 66). En este sentido, el Abogado General sigue el razonamiento del Grupo de Trabajo del Artículo 29, contenido en su Dictamen 8/2010, p. 10.

[93] Conclusiones del Abogado General, apartados 67-68.

cuestión, sean automáticas o no, pueden entrañar efectivamente el uso, revelación, mediante transmisión, difusión o puesta a disposición, de esos datos personales y, por ello, implican un tratamiento en el sentido del artículo 2, letra b) de la citada Directiva[94].

Ahora bien, aquí es cuando el Abogado General hace una distinción entre *Google Inc.* y *Google Spain*, puesto que considera que el proveedor de los servicios de Internet no sea responsable del tratamiento de los datos. Este Abogado entiende que el proveedor de servicios de motor de búsqueda en Internet que simplemente proporciona una herramienta de localización de información, no ejerce ningún control sobre los datos personales incluidos en las páginas web de terceros, pues aquéllos no se muestran como tales de modo específico, y dicho proveedor no es consciente de su existencia en un sentido distinto del hecho estadístico de que las páginas web probablemente incluyen datos de terceros; en otras palabras, el proveedor desconoce que las páginas web contienen datos personales[95]. Por ello, en este caso, la AEPD no tiene por qué requerir a un proveedor de servicios que elimine una información de su índice, salvo en los supuestos en los que, de la actividad de dicho proveedor, sí pueda emanar una responsabilidad por el tratamiento de datos personales, lo que sucedería únicamente cuando éste indexe, o archive datos personales, en contra de las instrucciones o las peticiones del editor de la página web. Por último, el Abogado General se muestra contrario a la existencia de un derecho al olvido y, por ende, al ejercicio del derecho de cancelación y oposición y bloqueo de datos por parte del afectado en el sentido que le permita contactar con los proveedores del servicio de motor de búsqueda para evitar la indexación de la

---

[94] Con arreglo al artículo 2, letra a) de la Directiva 95/46, se entiende por dato personal "*toda información sobre una persona física identificada o identificable*". El hecho de que el carácter de dato personal de los publicados por la página web fuente pueda ser desconocido para el gestor del motor de búsqueda en Internet, dada la automaticidad de las labores de recopilación, indexación y disposición u ordenación de los datos llevada a cabo por el buscador, sin intervención humana, no modifica esta afirmación.

[95] Con ello, el Abogado General sigue las consideraciones señaladas por el Grupo de Trabajo del artículo 29, en su Dictamen 1/2008, en el que se afirmaba que "*el principio de proporcionalidad requiere que, en la medida en que un proveedor de un motor de búsqueda actúe exclusivamente como intermediario, no debe considerarse como responsable principal del tratamiento de datos personales efectuado. En este caso, los responsables principales del tratamiento de datos personales son los proveedores de información*". Vid. MUÑOZ, J. "El llamado derecho al olvido y la responsabilidad de los buscadores". *Diario La Ley*, nº 8317, 23 de mayo de 2014, p.3.

información que le afecta personalmente y que ha sido publicada en páginas web de terceros[96]. Afirma de manera categórica que, a su entender, la Directiva no establece un derecho general al olvido que faculte a un interesado para restringir, o poner fin, a la difusión de datos personales que considera lesivos o contrarios a sus intereses. Lo contrario convertiría una preferencia subjetiva del interesado, por sí sola, en una razón legítima para permitir dicha solicitud de borrado, cosa que no se deduce, según JÄÄSKINEN, de la norma europea. La finalidad del tratamiento y los intereses a los que sirve, al compararse con los del interesado, son los criterios que han de aplicarse cuando se procesan datos sin su consentimiento y no las preferencias subjetivas del interesado. De lo contrario, se afectaría el contenido fundamental del artículo 11 de la Carta de Derechos Fundamentales de la Unión Europea, tanto al derecho a libertad de expresión del editor de la página web como a la libertad de información de los usuarios de Internet.

Por lo que se refiere a la valoración del TJUE, en el caso Google, el Tribunal de Luxemburgo fue, ante todo, un juez garante de los derechos fundamentales, haciendo honor a la alta condición jurídica que ya venía atribuyéndose el derecho a la protección de datos personales tanto en su jurisprudencia como en el marco legal y constitucional europeo. El TJUE alude al alto nivel de protección otorgado a este derecho por la Directiva 95/46, el artículo 8 CEDH y los principios generales del Derecho comunitario. Sin embargo, no limita su alcance al de un derecho meramente legalizado por la Directiva 95/46 —como afirmaba el Abogado General en sus Conclusiones— sino que le reconoce el alcance «constitucional» derivado de su consagración en los artículos 7 y 8 CDFUE[97] relativos al respeto a la vida privada y

---

[96] Antes de adentrarse en el estudio de la interpretación de la norma europea, advierte que las conclusiones ofrecidas en estos apartados únicamente serán relevantes si el TJUE rechaza la postura defendida por JÄÄSKINEN en relación con el segundo bloque de cuestiones, que excluye a Google con carácter general de la categoría de responsable del tratamiento con arreglo al artículo 2, letra d).

[97] Carta de los Derechos Fundamentales de la Unión Europea, Estrasburgo 12 de diciembre de 2007, arts. 7 y 8: *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.*

Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le concierne. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le concierne y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

al derecho a la protección de los datos personales —donde se impone que los datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley; que toda persona tiene derecho a acceder a los datos recogidos que le concierne y a obtener su rectificación y que el respeto de estas normas estará sujeto al control de una autoridad independiente—. Esto es, el TJUE no limita su interpretación a un mero juicio de legalidad comunitaria valorando la vigencia de la Directiva, sino que recurre al marco constitucional europeo preservando el valor jurídico de la CDFUE y garantizando la vigencia del derecho a la protección de datos en ella consagrado[98].

En cuanto a las cuestiones prejudiciales, comparte la opinión del Abogado General y sostiene que la actividad del motor de búsqueda que consiste en hallar información publicada en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de "tratamiento de datos personales". Sin embargo, no comparte la postura de exonerar de responsabilidad al gestor del motor de búsqueda; según el TJUE, dicho gestor es quien determina los fines y los medios de su actividad y, así, del tratamiento de datos personales que efectúa él mismo en el marco de aquélla, aunque no ejerza un control efectivo de los datos personales tratados, pues éstos son publicados en las páginas web de terceros.

En efecto, el TJUE señala el carácter decisivo del papel de los motores de búsqueda en la difusión global de esos datos personales, en la medida en que facilitan su acceso por todo internauta a partir de una búsqueda del nombre del interesado y permiten la organización y agregación de la información publicada por terceros en Internet, facilitando el acceso a ella por los internautas y permitiéndoles obtener, mediante la lista de resultados, una visión estructurada de la información relativa a esa persona que puede encontrarse en Internet.

En cuanto a la primera cuestión prejudicial, el TJUE sostiene, al igual que la Directiva, que, recordemos, permite incluir geográficamente, en el concepto de establecimiento, el tratamiento de datos personales en el marco de sus actividades todo supuesto en el que el gestor del motor de búsqueda cree en un Estado miembro

---

98 RALLO LOMBARTE, A. "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet". *Revista Teoría y Realidad Constitucional*, nº 39, 2017, pp. 583-610.

una sucursal o filial destinada a garantizar la comercialización de espacios publicitarios en ese buscador y cuya actividad se dirija a los habitantes de este país, como sucede, en el litigio principal, con la filial *Google Spain*, domiciliada en España y destinada a la venta de espacios publicitarios, fundamentalmente a empresas radicadas en España[99].

Por tanto, el Tribunal efectúa una interpretación restrictiva de la Directiva; ésta no exige que el tratamiento de datos personales controvertido sea efectuado "por" el propio establecimiento en cuestión, sino que basta con que se realice "en el marco de las actividades" de ese establecimiento, es decir, que no es la empresa matriz la que tiene que realizar el tratamiento de datos personales, sino que puede ser una empresa filial como es el caso de *Google Spain*. Recordemos que Google cuenta con numerosas sucursales y filiales por todo el mundo[100]. Pues bien, el TJUE entiende que la actividad llevada a cabo por *Google Spain* constituye una parte esencial de la actividad comercial del grupo Google y que está estrechamente vinculada con *Google Search* (uno de los numerosos productos que forman el conglomerado de Google) y, por ello, el tratamiento de datos personales realizado por este buscador se lleva a cabo en el marco de las actividades del establecimiento de *Google Spain*, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda sea económicamente rentable y, con ello, permitir a Google realizar sus actividades de tratamiento de datos personales.

Por otra parte, considera el Tribunal que, para el correcto ejercicio de los derecho ARCO, debe llevarse a cabo una ponderación, en atención a las circunstancias del caso, entre, por un lado, el derecho a la vida privada y a la protección de datos personales del interesado, quien habrá de acreditar las razones legítimas propias de su situación particular que justifiquen el ejercicio de este derecho, y, por otro, el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión.

---

[99] Para ello, el TJUE toma en consideración el contenido del Considerando 19 de la Directiva, en el que se aclara que "*la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante*".

[100] En la actualidad, Google ha cambiado su estructura empresarial y ha establecido una nueva matriz, llamada *Alphabet*, que cobijará al negocio de búsquedas en Internet y otras filiales.

Si bien, con carácter general, los derechos relativos a la privacidad, contemplados en los artículos 7 y 8 CDFUE, han tener prevalencia sobre el mencionado interés de los internautas, este equilibrio puede depender de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que la persona a la que se refiere la información desempeñe en la vida pública. Por tanto, cualquier tribunal nacional podrá ordenar al buscador eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona, determinados vínculos a páginas web, publicadas por terceros, que contengan información sobre esa persona, aunque no se haya ordenado, previa o simultáneamente, la eliminación de esa información de la página web fuente y, en su caso, aunque la publicación de la información sea en sí mismo lícita.

A continuación, el TJUE establece una responsabilidad "nueva"; el tratamiento de datos personales llevado a cabo en la actividad de un motor de búsqueda se añade al efectuado por los editores de sitios de Internet y afecta de modo adicional a los derechos de los interesados. Es decir, habrá una responsabilidad de los editores de una página web, si bien es cierto que da más importancia a la del motor de búsqueda, puesto que el TJUE defiende que la afectación de los derechos a la vida privada y a la protección de datos personales es diferente en cada uno de estos dos casos, siendo mayor la injerencia que la actividad del motor de búsqueda pueda suponer en los derechos fundamentales del interesado frente a la menor afectación asociada a la publicación originaria de la información por una página web, y ello dado el decisivo papel que el buscador desempeña para la difusión de esa información.

El TJUE va un paso más allá a la hora de interpretar la Directiva y entiende que debe hacerse en el sentido de que permita al interesado, por sí solo y directamente, exigir al gestor de un motor de búsqueda eliminar de la lista de resultados obtenida como consecuencia de una búsqueda a partir de su nombre, vínculos a páginas web, publicadas legalmente por terceros y que contienen información o datos verídicos relativos a su persona, cuando esos datos pueden perjudicar o, simplemente, porque el interesado desee que tales datos "se olviden" tras un determinado lapso de tiempo. Entiende que, incluso un tratamiento inicialmente lícito de datos exactos, puede devenir, con el tiempo, incompatible con la Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron, cosa que

sucede cuando los datos en cuestión sean inadecuados, no pertinentes o ya no pertinentes o excesivos en relación con estos fines y el tiempo transcurrido.
Lógicamente, hay que valorar cada caso y cada circunstancia y, en ningún momento, el hecho de que pueda existir un derecho al olvido, tiene que presuponer necesariamente que la inclusión de la información en la lista de resultados del motor de búsqueda cause al interesado un perjuicio efectivo. Este argumento pone en valor la prevalencia general de los derechos del interesado a la protección de datos personales y de su vida privada sobre el interés económico del gestor del motor de búsqueda y sobre el interés del público en encontrar la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, esta prevalencia podría no darse atendiendo a razones concretas como el papel desempeñado por el interesado en la vida pública, que conlleva un interés preponderante del público en tener acceso a la información de que se trate mediante la inclusión de ésta en las listas de resultados de búsqueda del motor.
Atendiendo al caso que nos ocupa, el TJUE consideró que, teniendo en cuenta el carácter sensible de la información para la vida privada del interesado –recuérdese que se trataba de anuncios de una subasta inmobiliaria vinculada a un embargo por deudas a la Seguridad Social– y atendiendo al hecho de que su publicación inicial se remontaba a 16 años atrás, no parecían existir razones concretas que justifican un interés preponderante del público en tener acceso a esta información en el marco de una búsqueda, lo que permitiría al interesado exigir al gestor del motor de búsqueda que se eliminaran estos vínculos de la lista de resultados.

4.3. Las principales cuestiones del caso Google.

Una vez vistos los hechos y los pronunciamientos tanto del Abogado general como del TJUE, pasamos a analizar las principales cuestiones suscitadas y resueltas en este caso.
1. ¿Resulta aplicable la normativa de protección de datos española a la actividad de Google, buscador domiciliado en Estados Unidos?
En cuanto a la aplicación territorial de la normativa española en protección de datos, el artículo 2.a) LOPD establecía que la legislación española se aplicará "cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un

establecimiento del responsable del tratamiento"[101]. Esta previsión situaba bajo la normativa española a aquellos editores con sede en España –medios de comunicación online, boletines oficiales, etc.-, así como a los perfiles de redes sociales.

En el caso particular de Google como buscador, tanto la STJUE como el Abogado General entendieron que quedan sujetos a la legislación de un Estado miembro cuando tienen en su territorio oficinas que colaboran de forma sustancial a la prestación del servicio, como pueden ser aquellas destinadas a vender espacios publicitarios. En el caso Costeja, Google argumentó que su servicio de buscador no está situado en España, y que, por ello, la legislación española no le resultaba de aplicación[102]. No obstante, ni el Tribunal ni el Abogado General Jääskinen aceptaron esa distinción entre gestor de búsqueda (*Google Inc.*) y gestor de publicidad (*Google Spain*), valorando la indiscutible conexión entre las actividades de ambas empresas[103]. Por lo tanto, cuando un buscador tenga su sede en España, o bien mantenga en nuestro país una oficina o sucursal con una actividad vinculada indisociablemente al buscador –como es el caso de *Google Spain*, que gestiona los espacios publicitarios en el motor de búsqueda-, quedará vinculado a la normativa nacional de protección de datos.

2. En caso de que la normativa española resulte de aplicación, ¿quién es el responsable del tratamiento: el editor o el buscador?

El artículo 3.d) LOPD y el artículo 2.d) de la Directiva 95/46 definía al responsable del fichero o tratamiento como la "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". A tenor de este artículo, cabía concluir sin mayores discusiones que el editor de la página web era responsable del tratamiento, toda vez que es quien

---

[101] El artículo es una transposición casi literal del artículo 4 de la Directiva 95/46/CE.

[102] Sobre la argumentación de Google para rechazar la aplicabilidad de la legislación española, véase: RALLO LOMBARTE, A. *El derecho al olvido en Internet*. Madrid: Centro de Estudios Políticos y Constitucionales, 2014, pp. 137 y ss.

[103] En este sentido, afirma el párrafo 57 STJUE: "*Pues bien, toda vez que dicha presentación de resultados está acompañada, en la misma página, de la presentación de publicidad vinculada a los términos de búsqueda, es obligado declarar que el tratamiento de datos personales controvertido se lleva a cabo en el marco de la actividad publicitaria y comercial del establecimiento del responsable del tratamiento en territorio de un Estado miembro (…)*".

publica el contenido. Lo que no resultaba tan evidente era si el buscador de Internet realizaba un tratamiento sujeto a la normativa.

A esta cuestión, se han ofrecido respuestas contradictorias. Por un lado, se ha sostenido que los buscadores son responsables del tratamiento de datos en la medida en que su actividad se ajusta a la definición legal contenida en el mencionado artículo 3.d) LOPD. Desde esta posición, se afirma que es evidente que el buscador localiza, indexa, almacena, organiza y presenta los datos, por lo que está decidiendo sobre la finalidad y uso del tratamiento, y debe ser considerado responsable. Además, la actividad del buscador tiene efectos muy sustanciales en la difusión de la información; efectos de los que es plenamente responsable. Mientras que, sin la participación de un buscador, un contenido en la Red tiene una difusión ciertamente restringida, la actividad del buscador multiplica la visibilidad del contenido, asociándolo, además, al nombre del afectado en las búsquedas que se hagan en Internet. Con base en estos dos argumentos, se ha defendido la responsabilidad de los buscadores en el tratamiento de los datos, siendo ésta la postura del TJUE y de la AEPD.

Otras voces, sin embargo, han cuestionado la responsabilidad del buscador en el tratamiento de datos. Los argumentos que se esgrimen desde estas posiciones son los siguientes:

-El buscador no trata los datos personales como tales, sino como información contenida en Internet.

-El buscador no tiene poder editorial sobre los contenidos, simplemente facilita su búsqueda. -Imponer al buscador responsabilidad sobre los datos que "canaliza" resultaría desproporcionado, toda vez que su sistema de tratamiento de datos es ciego. Entender que el buscador es responsable del tratamiento llevaría a conclusiones desproporcionadas y absurdas como, por ejemplo, la de que todos los buscadores actúan en la ilegalidad en la medida en que no han solicitado permiso para indexar datos personales.

La idea latente en todos estos argumentos es la misma: el buscador es un mero intermediario en la Red, una herramienta para localizar información, pero sin capacidad decisoria sobre la misma[104]. En la medida en que el buscador actúe como

[104] Estos argumentos fueron esgrimidos por el propio TJUE en su sentencia de 23 de marzo de 2010 (asuntos acumulados C-236/08 y C-238/08 Google France c. Louis Vuitton), nº2010 I-02417, donde se señala que, para gozar de la exclusión de responsabilidad

un intermediario, carezca de medios para modificar la información y no decida sobre los datos, no debe imponerse la responsabilidad sobre los mismos. Recordemos que esta fue la postura adoptada por el Abogado General en el presente caso.

3. En caso de que exista un tratamiento de datos sujeto a la normativa española, ¿concurren intereses legítimos que justifiquen un tratamiento sin consentimiento del afectado?

En este sentido, el artículo 6.2º de la LOPD incluía diversos supuestos en los que se podía prescindir del consentimiento del afectado. Entre ellos, no será preciso el consentimiento cuando "los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos".

Pero, ¿a qué intereses legítimos se hace referencia exactamente para justificar el tratamiento de datos personales sin consentimiento? Si la información es veraz, el editor estará protegido por el derecho a la información, en su dimensión activa. Además, dependiendo del interés público de la información, esta protección será mayor o menor. Por su parte, el internauta podrá esgrimir el mismo derecho, si bien en su dimensión pasiva. Finalmente, el buscador podrá alegar tanto su derecho a la libertad de empresa (artículo 38) como, a nuestro entender, el propio derecho a la información, el derecho a informar. Entendemos que, aunque está realizando una actividad comercial, sirve de forma trascendental al derecho a la información, ordenando el contenido de Internet y permitiendo a los internautas acceder a todo tipo de fuentes. En efecto, el interés económico no excluye la aplicabilidad de las libertades informativas, como ya tiene dicho tanto la jurisprudencia europea como la nacional sobre la comunicación publicitaria sin ir más lejos.

Sea como fuere, frente a este catálogo de intereses legítimos, emerge el derecho a la protección de datos del afectado. Este conflicto de derechos debe solventar por la vía de la ponderación, valorando cuál de ellos debe prevalecer. Los criterios seguidos por el TJUE, para llegar a cabo esta ponderación, son, como no podía ser de otro modo, la veracidad y el interés público. En efecto, ante la solicitud de retirada de un contenido o un enlace, el editor o el buscador deberán valorar si dicha información

---

reconocida en la Directiva 2000/31/CE, la actividad del prestador de servicios de la información debe tener una naturaleza meramente técnica, automática y pasiva, lo que implica que el prestador "no tenga conocimiento ni control de la información transmitida o almacenada" (párrafo 113).

es veraz y tiene interés público. Si la respuesta es positiva, no tienen obligación de retirar el contenido, aunque el mismo pueda resultar perjudicial o molesto para el afectado. Por el contrario, si el paso del tiempo ha convertido dicho contenido en no veraz, o ha hecho menguar su interés público, deberán aceptar la solicitud de borrado.

Esta obligación de retirada, como bien dice el TJUE, corresponde sobre todo al buscador. Mientras que, en muchas ocasiones, el editor no tiene por qué retirar un contenido –por ejemplo, una hemeroteca de un diario perdería su razón de ser si borrase noticias-, el buscador sí debe hacerlo, por dos motivos. Primero, su tarea no está amparada por un derecho fundamental (derecho a la información), sino solo por un derecho constitucional (libertad de empresa). Segundo, porque su función de difusión es la que fundamentalmente genera el perjuicio al afectado, al multiplicar la visibilidad del contenido.

Teniendo en cuenta que la sentencia que comentamos se dictó cuando estaba vigente la LOPD y la Directiva 95/46, debemos responder a estas cuestiones con el vigente RGPD y la LOPDGDD:

1) En cuanto a la cuestión de la aplicabilidad de la normativa, el RGPD se aplica, según el artículo 3, en los casos siguientes:

- su empresa o entidad trata datos personales como parte de las actividades de una de sus sucursales establecidas en la Unión Europea (UE), independientemente del lugar donde sean tratados los datos, o
- su empresa está establecida fuera de la UE y ofrece productos o servicios (de pago o gratuitos) u observa el comportamiento de las personas en la UE.

Por tanto, como vemos, se sigue la premisa que apuntaban tanto el TJUE como el Abogado General cuando entendieron que los buscadores (en este caso Google) quedaban sujetos a la legislación de un Estado miembro si tenían en su territorio oficinas que colaborasen de forma sustancial a la prestación del servicio, puesto que se entiende que, aunque su sede no esté en la UE, opera con filiales o sucursales en suelo europeo y, por tanto, está sujeta a la normativa europea, independientemente de que los datos no sean tratados en esa sucursal en cuestión.

2) En cuanto a la existencia de un interés legítimo para el tratamiento de los personales sin el consentimiento del afectado, el RGPD sigue las pautas marcadas

por la anterior normativa. Se regula actualmente en el artículo 6.1 y también en los artículos 13 y 14 cuando hablan del derecho de información. No obstante, el RGPD introduce una serie de novedades al respecto en sus considerandos: criterios para la ponderación[105]; su no aplicación, como regla general, a las Administraciones Públicas; y algunos supuestos (ejemplos) de posible aplicación del interés legítimo en favor del responsable. La AEPD sigue la línea de la ponderación y establece que habrá que valorar si hay un interés legítimo perseguido por el responsable del tratamiento, o por el tercero o terceros a los que se comuniquen los datos, que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado que requieran protección conforme a lo dispuesto en el artículo 1 RGPD, o si, por el contrario, los derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable o el tercero pretende fundamentar el tratamiento o la cesión de los datos de carácter personal.

3) En cuanto a la responsabilidad del responsable del tratamiento, se regula en el artículo 24 RGPD y en el 28 LOPDGDD, que es el encargado de establecer las obligaciones generales del responsable, indicando que se deberán determinar las medidas técnicas y organizativas apropiadas a fin de garantizar y acreditar que el tratamiento es conforme a la normativa en la materia. Ahora bien, en cuanto al caso que nos atañe, la responsabilidad del editor o bien del buscador, como apuntaba el TJUE en sus conclusiones, la indexación de la información personal es clave y esta tarea corresponde al buscador puesto que es el que ofrece los resultados indexados cuando se realiza una búsqueda por nombre.

4.3.1. Responsabilidad de los editores.

Tras la STJUE Google contra AEPD y Mario Costeja, la Audiencia Nacional pronunció, durante los años 2014 y 2015, numerosas sentencias sobre el derecho al

---

[105] Considerando 47 RGPD 679/2016:
-Que el interesado sea cliente o esté al servicio del responsable.
– La evaluación (ponderación) debe realizarse de forma meticulosa.
– La perspectiva del interesado, de manera que podrían prevalecer sus intereses sobre los del responsable cuando se proceda al tratamiento de datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento posterior.

olvido. Casi todas coincidían en que eran casos pendientes de la resolución de las cuestiones prejudiciales presentadas ante el TJUE. Los procesos, en su mayoría, eran recursos planteados por *Google Spain* frente a resoluciones de la AEPD que le obligaban a borrar enlaces de las páginas de resultados para proteger el derecho a la protección de datos de los afectados. En todas estas sentencias se reconoce el derecho al olvido del particular, desestimando así los recursos presentados por Google y responsabilizando al motor de búsqueda.

También hubo algunas sentencias que estimaron parcialmente los recursos planteados por *Google Spain*. Este es el caso de las SSAN de 29 de diciembre 2014 (RAJ 2014, 5211), 3 de febrero de 2015 (RAJ 2015, 342/2015), 19 de febrero de 2015 (RAJ 2015, 649) y de 30 diciembre de 2015 (RAJ 2014, 5241), que deniegan el derecho al olvido puesto que el particular no presentó suficientes pruebas sobre las páginas web que le eran perjudiciales. En estos casos, la argumentación de la Audiencia Nacional es la siguiente: Quien ejercita el derecho de oposición al tratamiento debe aportar la información necesaria para que "tanto el responsable del tratamiento como la propia AEPD cuente con los elementos necesarios para llevar a cabo el juicio de ponderación (…)". De ello se desprende, por tanto, que quien pretende la desindexación de un determinado contenido deberá justificar por qué este contenido de las páginas enlazadas resulta extemporáneo, perjudicial y carente de interés público a fin de que el buscador y la AEPD puedan valorar la pertinencia del borrado. *A sensu contrario*, meras exigencias de retirada de enlaces carentes de una argumentación que las respalde y justifique, no deben ser atendidas[106].

Exponemos, a continuación, la STS de 15 octubre de 2015 (RAJ 2015, 4132), que resulta interesante ya que, en lugar de abordar la responsabilidad de un buscador de Internet, se ocupa principalmente del papel del editor; en este caso, la editorial informativa de El País. La citada resolución judicial, además, puntualiza que el llamado "derecho al olvido digital" no ampara que cada uno construya un pasado a su medida, impidiendo la difusión de informaciones sobre hechos que no considere positivos, ni tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya ese pasado a su medida.

---

[106] MARTINEZ OTERO J. M. "La aplicación del Derecho al Olvido en España tras la STJUE Google contra AEPD y Mario Costeja". *Revista Bolivariana de Derecho*, nº 23, enero 2017, pp. 112-133.

Los hechos se remontan a los años ochenta cuando dos personas estuvieron implicadas en tráfico de drogas; tras cumplir condena, rehicieron su vida personal, familiar y profesional. La noticia sobre su detención, ingreso en prisión y padecimiento del síndrome de abstinencia, aparecía en aquellas fechas en los primeros lugares de las consultas que se hacían utilizando como palabras clave sus nombres y apellidos en los motores de búsqueda de Internet. La empresa editora del diario y responsable de la hemeroteca, ya digitalizada, no atendió la petición de adoptar las medidas necesarias para evitar la difusión actual y permanente de la información publicada cuando sucedieron los hechos, razón por la que los afectados interpusieron una demanda para la protección de su honor, su intimidad y su derecho a la protección de los datos personales.

El diario alegaba que la noticia indexada era veraz, mientras los interesados entendían que la visibilidad de la noticia era excesiva y desproporcionadamente perjudicial, por lo que requerían al diario la adopción de una serie de medidas orientadas a minimizar la accesibilidad de sus datos en relación con la citada noticia. En concreto, los interesados solicitaban: 1) la adopción de medidas para impedir la indexación de la noticia por los buscadores de Internet (protocolos de exclusión como *robot.txt*, o códigos como *noindex* o *noarchive*); 2) la modificación de las noticias de la hemeroteca de modo que no aparecieran sus nombres ni sus iniciales; 3) la adopción de medidas técnicas para evitar que la información pudiera ser indexada por el propio buscador interno de www.elpais.com.

El TS, tras estimar que la acción ejercitada no había caducado y considerar que el editor de una página web en la que se incluyen datos personales es responsable de que el tratamiento de estos respete las exigencias derivadas del principio de calidad de los datos, realiza la ponderación entre el ejercicio de la libertad de información que suponen las hemerotecas digitales, y los derechos al honor, la intimidad y la protección de datos personales de las personas afectadas por las informaciones contenidas en aquéllas. Además el TS utiliza una de las premisas que habían sido usadas, en otros casos similares, por el TJUE y es que, efectivamente, cuando hay responsabilidad sobre el tratamiento de datos personales, los principales responsables son los gestores de los motores de búsqueda, pero ello no significa que los editores de las páginas web no tengan la condición de responsables del tratamiento con los consiguientes deberes de respetar el principio de calidad de datos y atender el ejercicio de los derechos que la normativa de protección de datos otorga

a los afectados, así como la responsabilidad derivada de no respetar estas exigencias legales.

Pese a lo dicho, la Sala rechaza taxativamente las medidas solicitadas por los interesados sobre la procedencia de eliminar los nombres y apellidos de la información recogida en la hemeroteca, o de impedir que sea indexada por el motor de búsqueda interno de aquélla, pues considera que estas medidas suponen una restricción excesiva de la libertad de información vinculada a la existencia de las hemerotecas digitales[107].

Como vemos, el derecho a la información prevalece aquí sobre el derecho a la privacidad; los editores, en su mayoría diarios de prensa, se amparan en la libertad de información y expresión para contar noticias, aun a riesgo de vulnerar los principios de la protección de datos personales.

5. Conclusiones.

1) El derecho a la protección de datos no es ni más ni menos que el derecho a la privacidad, a nuestra intimidad, a mantener nuestra esfera privada fuera de la injerencia del resto. El derecho a la protección de datos es un derecho a la autodeterminación informativa, es decir, la persona decide qué contar y cómo contarlo, o, por el contrario, decide no divulgar sus datos personales, u oponerse a su tratamiento en el supuesto en el que aquéllos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados.

2) Este derecho entra en conflicto con otros derechos fundamentales, como pueden ser el derecho a la información y la libertad de expresión. Para solucionar esos conflictos se acude a la regla de la ponderación y se valora en cada caso qué derecho debe prevalecer.

3) Hemos visto la progresiva unificación en el ámbito de la UE de toda la normativa en materia de protección de datos, particularmente gracias a la aprobación del RGPD, que pretende dejar atrás la disparidad de criterios seguidos por los Estados

[107]http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/El-Supremo-reconoce-el--derecho-al-olvido--digital-de-dos-procesados-implicados-en-un-caso-de-drogas-en-los-ochenta

miembros. Se aplica con carácter general y de forma obligatoria a todo el territorio europeo y, por tanto, hay una mayor uniformidad en la aplicación de ley.

4) Gracias a los derechos ARCO se pone al alcance de los afectados una serie de herramientas que pueden utilizar cuando consideren que se está vulnerando su derecho a la protección de datos. A los derechos tradicionales (Acceso, Rectificación, Cancelación y Oposición), el RGPD ha añadido el derecho a la portabilidad de los datos personales, el derecho a la limitación de los datos y el ya conocido derecho al olvido; todo ellos también reconocidos y recogidos en vigente LO 3/2018.

5) La importante STJUE de 13 de mayo de 2014 dejó claras varias cosas; en primer lugar, con esta sentencia se abre una puerta para que los ciudadanos puedan reclamar ante los buscadores de Internet, para que eliminen aquellos enlaces en donde aparece su nombre. El motor de búsqueda, tras muchas dudas y opiniones, es considerado también responsable del tratamiento de datos personales y el afectado podrá dirigirse al él, puesto que es quien indexa, almacena y, en definitiva, difunde esa información.

6) La citada sentencia fue también trascendental sobre la cuestión de la aplicabilidad territorial de la normativa. El TJUE entiende que *Google Spain* es una filial de *Google Inc.*, que, además de estar ubicada en España (es decir tiene su establecimiento en nuestro país), realiza actividades comerciales aquí; está, por tanto, sujeta a la normativa española y europea en materia de protección de datos. El TJUE desacreditó por completo, y con mucho acierto, el argumento de Google de que el motor de búsqueda no realiza un tratamiento de los datos personales en el marco de las actividades desarrolladas en España. De esta forma, se sientan las bases de cómo deben actuar las grandes corporaciones de Internet en el marco de sus actividades: Deberán someterse a la legislación europea todas las empresas que tengas oficinas, sucursales, filiales, etc. que operen en el territorio europeo, lo que ya se recoge en el RGPD.

6) Esta sentencia marcó un antes y un después en la historia de Internet, ya que su impacto no alcanza solo a la garantía de los derechos fundamentales (privacidad y protección de datos personales) sino incluso al obligado rediseño de los servicios de Internet (buscadores, redes sociales, etc.). Como hemos comentado a lo largo del

trabajo, el derecho a la protección de datos no es absoluto, nadie puede construir un pasado a su medida, o decidir que se suprima una determinada información de Internet, sino que debe verse en cada caso qué derechos (derecho a la privacidad vs derecho a libertad de información) entran en conflicto, qué intereses se suscitan y ponderarlos.

7) Se ha analizado como, por primera vez, se pone de relieve la importancia que debemos darle a la protección de datos, es decir, nuestra privacidad, por encima del mero interés económico del gestor de un motor de búsqueda de Internet. El TJUE, con gran acierto, no discute la actividad desarrollada por los motores de búsqueda sino su afectación a los derechos fundamentales de los afectados, en esencia al respeto de su vida privada. Como vemos, no todo vale en Internet, ni Google ni ningún buscador, por muy poderosos que sean, pueden tratar información personal en su provecho, escudándose en el derecho a la libertad de expresión para no eliminar los datos personales de los usuarios. Gracias a esta sentencia, se sentó un precedente y, lo más importante, se reconoció por primera vez el derecho al olvido digital.

6. Bibliografía.

AZURMENDI, A. "Derecho de autodeterminación informativa y el derecho al olvido en Internet: La generación de Google del derecho a la vida privada", Revista Derecho y Política, Una década de transformaciones, AA. VV, 2014, pp. 203-218.

ARS IURIS SALMANTICENSIS. "Protección de datos y derechos digitales" Revista Crónica de legislación, 2019 vol. 7, pp. 233-237.

DE TERWAGNE, C. "Privacidad en Internet y derecho a ser olvidado / derecho al olvido" Revista de Internet, Derecho y Política 2012, nº 13.

CHELIZ INGLÉS, M.C. "El derecho al olvido digital" Una exigencia de las nuevas tecnologías recogida en el futuro reglamento de protección de datos. Revista Actualidad Jurídica Iberoamericana, agosto 2016, nº5.

CHÉLIZ INGLÉS, M. C. "El derecho al olvido digital. Una exigencia de las tecnologías recogido en el Reglamento general de protección de datos". nº5 agosto, 2016, pp. 260-261.

CÓRDOBA CASTROVERDE, D. "Los retos de la protección de datos en Internet. Caso Google Spain y derecho al olvido" Conferencia pronunciada en la Facultad de Derecho de la Universidad autónoma de Madrid, 2017.
DE TERWAGNE, C., "Privacidad en Internet y derecho a ser olvidado / derecho al olvido" Revista de Internet, Derecho y Política 2012, nº 13.

DÍEZ-PICAZO, L. *Derecho y masificación social. Tecnología y Derecho Privado, Civitas,* Madrid, 1979.

FERNÁNDEZ VILLAZÓN, L.A. "El nuevo reglamento europeo de protección de datos" Revista Nueva Época, 2016, volumen 19, nº1.

HEREDERO HIGUERAS, M. "La LORTAD y su futuro. La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal" Revista de Informática y Derecho.

HERRÁN ORTIZ, A.I. "El derecho a la protección de datos en la sociedad de la información" Cuadernos de Deusto de Derechos humanos, nº26, 2003, pp.9-11.

LOPEZ PORTAS, B. "La configuración jurídica del derecho al olvido en el derecho español a tenor de la doctrina del TJUE" Revista Derecho Político nº 93, 2015, pp. 143-175.

MARTÍNEZ, J. "La aplicación del derecho al olvido en España tras la STJUE Google Spain contra AEPD y Mario Costeja" Revista Bolivariana de Derecho, nº23, enero 2017, pp. 112-133.

MATÉ SATUÉ, L.C "¿Qué es el derecho al olvido?" Revista Derecho Civil, 2016 volumen 3, nº2, pp. 187-222.

MINERO ALEJANDRE, G. "A vueltas con el derecho al olvido" Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital. Revista Jurídica UAM, 2014, nº 30, pp. 129-155.

MITJANS PERELLÓ, I. Congreso Internacional sobre Internet, Derecho y Política: "Neutralidad de la Red y Derecho al olvido".
MURGA FERNANDEZ, P. "La protección de datos y los motores de búsqueda en Internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido" Revista Derecho Civil, nº4, 2017.

PÉREZ GÓMEZ, A.M. "El Derecho al olvido digital en Europa, una lucha de titanes" Revista la Propiedad Inmaterial nª22, 2016, pp. 173-186.

PÉREZ LUÑO, A.E. *Derechos Humanos, Estado de Derecho y Constitución,* Tecnos*,* 4ª ed., Madrid, 1991.

PÉREZ LUÑO, A.E. *Los derechos humanos en la sociedad tecnológica.* Universitas, Madrid, 2012.

PALACIOS GONZALEZ, M.D. "El poder de autodeterminación de los datos personales en Internet" Revista de Internet, Derecho y Política, 2012, nº 14.

RALLO LOMBARTE, A. "El tribunal de Justicia de la Unión Europea como juez garante de la privacidad de Internet" Revista UNED Teoría y Realidad constitucional, 2017, nº 39, pp. 538-610.

SÁNCHEZ BRAVO, AA. "La ley orgánica 15 /199 de protección de datos de carácter personal: diez consideraciones en torno a su contenido" Revista de Estudios Políticos (Nueva Época) nº11, 2001.

SANCHO LÓPEZ, M. "Garantías legales del concepto de privacidad: entre el derecho al olvido y el nuevo reglamento europeo de protección de datos" Revista Jurídica Iberoamericana, 2018, nº 9, pp. 176-201.

SERRANO PÉREZ, M. "El derecho fundamental a la protección de datos. Su contenido esencial" Los derechos fundamentales y las nuevas tecnologías, nº1, 2005.

SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital,* Valencia, Tirant lo Blanch, 2012.

SEISDEDOS POTES, V. "Derecho al olvido. Jaque a Google en Europa" Revista Cuadernos de Dereito Actual, 2014, nº2.

TORRES MANRIQUE, J.I. "Analizando el derecho fundamental al olvido a propósito de su reciente reconocimiento y evolución" Revista Misión Jurídica, 2017, nº13, pp. 2019-231.

TOURIÑO, A: *El derecho al olvido y a la intimidad en Internet.* Catarata, Madrid.

TRONCOSO REIGADA, A. *La protección de datos personales. En busca del equilibrio.* Tirant Lo Blanch*,* 2008.

TRONCOSO REIGADA, A. "Los límites del acceso a la información" Revista Iberoamericana de Derecho Informático, 2016, nº 1, pp. 45-53.

JURISPRUDENCIA UTILIZADA:

JURISPRUDENCIA TRIBUNAL CONSTITUCIONAL:
-STC 292/2000, de 30 de noviembre. (BOE núm. 4, de 04 de enero de 2001).
http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276

-Tribunal Constitucional, Pleno, Sentencia 290/2000 de 30 de noviembre de 2000. Recurso 201/1993. Tribunal Constitucional, Pleno, Sentencia 292/2000 de 30 de noviembre de 2000. Recurso 1463/2000 2000.
https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

-Tribunal Constitucional, Pleno, Sentencia 290/2000 de 30 de noviembre de 2000. Recurso 201/1993. Tribunal Constitucional, Pleno, Sentencia 292/2000 de 30 de noviembre de 2000. Recurso 1463/2000 2000.
https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

-STC 254/1993, de 20 de julio.
http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383

-STC 11/198, de 8 de abril.
https://hj.tribunalconstitucional.es/esES/Resolucion/Show/11#complete_resolucion&fundamentos

JURISPRUDENCIA TRIBUNAL SUPREMO.

-STS de 6 de julio de 2017(RJA 426/2017).
https://supremo.vlex.es/vid/686461129

-STS de 15 octubre de 2015 (RAJ 2015, 4132).
https://www.boe.es/biblioteca_juridica/comentarios_sentencias_unificacion_doctrina_civil_y_mercantil/abrir_pdf.php?id=COM-D-2015-35_Comentarios_a_las_Sentencias_de_Unificacion_de_Doctrina__Civil_y_Mercantil__Derecho_al_olvido_en_internet
http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/El-Supremo-reconoce-el--derecho-al-olvido--digital-de-dos-procesados-implicados-en-un-caso-de-drogas-en-los-ochenta

JURISPRUDENCIA TRIBUNAL DE JUSTICIA DE UNIÓN EUROPEA.

-STJUE, de 18 diciembre de 2008, caso C-73/07, Tietosuojavaltuutettu y Satakunnan Markkinapörssi Oy, Sata media Oy.
http://revista-estudios.revistas.deusto.es/article/viewFile/248/393

-STJUE 25 de octubre de 2011, Número de asunto = C-509/09.
http://curia.europa.eu/juris/liste.jsf?language=es&num=C-509/09

-STJUE de 23 de marzo de 2010 (asuntos acumulados C-236/08 y C-238/08 Google France c. Louis Vuitton), nº2010 I-02417.
http://curia.europa.eu/juris/liste.jsf?num=C-236/08&language=es

-STJUE de 13 de mayo de 2014, ECLI:EU:C:2014:317.
http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

RESOLUCIONES AEPD.

-Resolución AEPD TD/00038/2020.
https://www.aepd.es/es/taxonomy/term/2512?page=1

- Resolución E/07807/2015
https://www.aepd.es/es/taxonomy/term/2421?page=3