

# **El derecho a la protección de datos y delimitación del “derecho al olvido” en la Unión Europea**

*EU Data Protection rights, “right to be forgotten” delimitation*

**M<sup>a</sup> Pilar DOPAZO FRAGUÍO**

Universidad Complutense de Madrid (España)  
mdopazo@ucm.es

Recepción: Junio 2018

Aceptación: Septiembre 2018

## **RESUMEN**

El vigente Reglamento General de Protección de Datos (RGPD), normativa europea directamente aplicable y con plenos efectos desde el 25 de mayo de 2018, ha supuesto un importante reconocimiento y avance en aras de reforzar la protección de datos personales en el ámbito de la Unión Europea. En este sentido, se dicta un marco regulatorio común y uniforme, que a su vez podrá ser completado por cada Estado miembro. No obstante, cumple admitir que se trata de una temática compleja, y sobre todo en atención a los importantes retos jurídicos que aún plantean los entornos tecnológicos y medios digitales de comunicación a través de la Red. En este contexto temático e instrumental, una de las cuestiones que adquieren mayor interés, es la relativa a la delimitación funcional y operativa del “derecho a olvido”. Al respecto, en este texto, se analiza su actual configuración doctrinal, con base en observar destacados pronunciamientos del Tribunal de Justicia de la Unión Europea, y asimismo su incorporación positiva en el precitado RGPD, entre otras innovaciones jurídicas que son examinadas en este trabajo, todo ello con el propósito de significar cuáles son las principales aportaciones de este marco regulatorio general.

**Palabras clave:** Protección de Datos Personales (PDP); “derecho al olvido”; derecho de acceso a la información.

**Clasificación JEL:** K3, K23, O34.

## ABSTRACT

The current General Data Protection Regulations (RGPD), European regulation directly applicable and with full effect from May 25, 2018, has been an important recognition and progress to strengthen the protection of personal data within the European Union. In this sense, a common and uniform regulatory framework has been passed, which in turn can be completed by each Member State. However, it admits that it is a complex issue, especially in view of the important legal challenges that still arise in technological environments and digital means of communication through the Internet. In this thematic and instrumental context, one of the issues that we estimate maintain greater interest, is the one relative to the functional and operational delimitation of the "right to be forgotten". In this regard, in this text, its current doctrinal configuration is analysed, based on observing outstanding pronouncements of the Court of Justice of the European Union, and also its positive incorporation in the aforementioned RGPD, among other legal innovations that are examined in this work, all with the purpose of signifying what are the main contributions of this general regulatory framework.

58

**Key words:** Protection of Personal Data (PDP); "right to be forgotten"; right of access the information.

**JEL Classification:** K3, K23, O34.



## 1. INTRODUCCIÓN: CONSIDERACIONES PREVIAS ACERCA DEL DERECHO A LA PROTECCIÓN DE DATOS

En la actualidad, es patente el amplio reconocimiento jurídico de que dispone el derecho a la protección de datos (DPD, en adelante) como derecho fundamental en el Ordenamiento de la Unión Europea (UE). Con certeza, cabe afirmar que ello ha sido fruto del avance cultural, socioeconómico y jurídico promovido en nuestro entorno, lo que demuestra que concurre una mayor sensibilidad hacia esta cuestión y su tratamiento jurídico, estimando así que la información relativa a datos personales, *per se*, constituye un valor digno de especial protección. En este sentido, la UE ha procedido a consolidar de forma positiva la regulación común en esta materia, con el propósito de armonizar la disciplina aplicable en los Estados miembros, y asimismo reforzar el deber de tutela pública que requiere la protección de datos. Sin duda, esto ha supuesto un importante proceso de innovación jurídica, en el que ha destacado la aportación de la Jurisprudencia europea e interna, sobre todo en virtud de recientes pronunciamientos a los que en este estudio se hace expresa referencia (siendo objeto de análisis específico aquellos que –a nuestro juicio– son más significativos en esta materia).

59

Conforme a este proceso de evolución normativa, los datos personales adquieren una consideración específica por parte del Ordenamiento vigente, identificados por su valor como potenciales activos intangibles, en términos económicos, y a su vez, hoy constituyen bien jurídico protegido, objeto del reconocido derecho precitado (directamente relacionado con la identidad y privacidad de cada persona). Y, de este modo, este derecho queda vinculado a otro fundamental, -el derecho a la intimidad-, y asimismo mantiene una singularidad propia, que lo identifica por su objeto: la información personal, y, por ende, relativa a la esfera privada del individuo. Como tal, se trata de un bien jurídico sumamente sensible, siendo factible su posible vulneración mediante, por ejemplo, la difusión de datos no veraces, erróneos o inexactos, el uso no autorizado por terceros, etc.

Ilustra sobre el resultado de este progreso en aras del efectivo y sólido reconocimiento actual del DPD, la arquitectura regulatoria europea dictada con base al vigente Reglamento General de Protección de Datos (RGPD, 2016)<sup>1</sup>, aplicable con plenos efectos desde el pasado mayo 2018. El dictar este acto normativo vinculante, no ha sido casual, sino que responde a la necesidad detectada por el legislador europeo de ofrecer un eficaz marco común para la tutela pública del DPD en el ámbito de la UE. La cuestión no es baladí, pues con ello también se trata de atender a los nuevos desafíos que plantea la dinámica informativa y de comunicación que se desarrolla en la actualidad, de forma global y generalizada por medios electrónicos y diversas redes. Por ende, era necesario actualizar la legislación europea en materia de protección de datos, determinando al efecto, un régimen jurídico básico común y preceptivo que conforme a

unos criterios uniformes sea aplicable en todos los Estados miembros. Ello, pretende disciplinar el tráfico o circulación de información en la UE, y a su vez, mediante el RGPD ha sido positivizada la reciente doctrina jurisprudencial del TJUE dictada en materia de protección de datos (doctrina del “derecho al olvido”), entre otras novedades incorporadas en el mismo (que se detallan en este trabajo).

En consecuencia, esta nueva regulación europea en materia de protección de datos, (Reglamento General de Protección de Datos, RGPD 2016), supone un importante hito en el Derecho de la UE, en orden a su principal pretensión: fijar una disciplina uniforme de obligado cumplimiento que garantice la protección del DPD, y que compele a implementar medidas preventivas, sistemas de evaluación y de supervisión necesarios por parte de los operadores responsables. De igual modo, a dicha finalidad se establecen un cuadro de principios rectores básicos, así como un conjunto de deberes específicos que han de ser observados. En su defecto, se dicta un régimen sancionador, así como la posibilidad por parte de los Estados miembros de habilitar otras medidas de vigilancia de cumplimiento y aquellos protocolos complementarios que se estimen oportunos.

60

El interés principal de esta regulación ha motivado la realización de este estudio, en el que se ofrece una síntesis de los contenidos esenciales de esta normativa, analizando sus principales aportaciones. Al respecto, cumple significar que, con el RGPD, el Derecho de la Unión Europea ha identificado de forma satisfactoria el valor y la funcionalidad del DPD, observando además la operativa hoy empleada en el tráfico jurídico y comercial; y, por ende, la necesidad de prevenir y afrontar con éxito los nuevos riesgos y desafíos que conlleva la circulación generalizada y accesible de información. En suma, se trata de hacer compatibles el principio de transparencia informativa y el DPD, como binomio viable y consustancial que ha de ser garantizado en los Estados democráticos y de Derecho, en aras de mayor seguridad jurídica.

Con todo, se reconoce que la protección de los datos personales es una materia compleja, pues supone ponderar cada caso planteado y resolver posibles conflictos, por ejemplo, ante supuestos en que se produzca una colisión entre derechos o intereses, se ha de proceder a tratar de conciliar intereses privativos, o, incluso, dictaminar cuál es el preferente cuando existiera un interés público o colectivo frente a otro privado. A ello, suma mayor dificultad el fenómeno de la globalización internacional que caracteriza la actividad comercial prestada a través de la Red (internet) o redes y plataformas tecnológicas a través de las que hoy se prestan diversos servicios y se divulga información (no siempre veraz o actualizada). Pues, como se sabe, hoy los nuevos medios y herramientas empleadas en comunicación permiten un acceso abierto y generalizado, que no siempre cuenta con un control suficiente. En la era de la sociedad de la información digitalizada y de ágil consulta, la protección de datos adquiere un especial valor, y, por tanto, la normativa ha de ser óptima para asegurar la protección de los mismos. Pues, sin duda, hay que reconocer las muchas ventajas que ofrece Internet y



el empleo de TIC (tecnologías de información y comunicación), pero también prevenir y actuar con rigor desde el Derecho frente a nuevas amenazas, tales como los denominados “ciberriesgos”.

### **2. TUTELA PÚBLICA DEL DPD EN LA UNIÓN EUROPEA: VALOR Y FUNCIONALIDAD ACTUAL**

Conforme a lo expuesto, y en atención al visible escenario global, la protección pública del DPD recobra un destacado interés en los actuales Estados democráticos; así, la Unión Europea ha focalizado de una forma eficaz la necesidad de armonizar las distintas legislaciones de los Estados miembros en esta materia, en orden a reforzar la tutela otorgada a este derecho, que asimismo se configura como un “bien jurídico” digno de una especial protección (tal y como hemos avanzado en el epígrafe precedente). De este modo, actuando en consecuencia y conforme al debido rigor normativo que exige esta cuestión, se dicta el precitado y hoy vigente, Reglamento General de Protección de Datos (RGPD, 2016).

Al respecto, hay que poner en valor que esta acción normativa pretende actualizar y perfeccionar la Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos<sup>2</sup>, porque no resultó suficiente a los fines precitados. Además, en virtud del nuevo RGPD se han tenido en cuenta otros aspectos e implicaciones que la protección de datos conlleva en la práctica, pues junto a la defensa de los derechos privativos que corresponden al ciudadano, también se considera la tutela de información por su impacto en el orden económico, la defensa de la competencia y, con todo, en aras de asegurar el buen desarrollo del mercado interior. Este aspecto también se subraya en el texto del propio RGPD vigente, por cuanto, -cabe inferir-, el procurar la seguridad jurídica en el tráfico de información o datos es asimismo una cuestión que no puede ser ignorada a la hora de diseñar políticas estratégicas claves a los fines mencionados.

61

#### **2.1. Evolución de la normativa europea y configuración actual del DPD**

Cabe estimar como positiva la evolución de la normativa comunitaria europea, hasta llegar al actual contexto regulatorio que se brinda al derecho a la protección de datos (DPD), y esto ha sido así, -en gran medida-, gracias a la labor realizada por los juristas e instituciones europeas. Asimismo, en España, digno es subrayar la labor de la Agencia Española de Protección de Datos. Y, en este sentido, de forma especial, hay que destacar la valiosa aportación procurada por reciente jurisprudencia europea e interna dictada en esta materia. Por otra parte, también cabe admitir que la protección de datos personales es una temática aún compleja de abordar, por múltiples factores y variables que han de ser ponderadas en cada caso; a ello se suma, los eventuales riesgos de la comunicación digital o información divulgada vía redes electrónicas, como ya ha sido señalado en este texto (supra).

Con todo, puede afirmarse con certeza que el reconocimiento del DPD dispone hoy de base jurídica declarativa suficiente, quedando consagrado como derecho fundamental, lo que ha sido fruto de un proceso evolutivo y mediante su declaración en distintos instrumentos internacionales y europeos principales, como son: Resolución 45/95 de la Asamblea General de las Naciones Unidas, versión revisada de los Principios Rectores para la Reglamentación de Ficheros Computadorizados de Datos Personales (ONU), Resolución de Naciones Unidas A/C.3/68/L.45/Rev.1 “El Derecho a la Privacidad en la Era Digital (2013); Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal (Estrasburgo, 28 de enero de 1981), y a tenor de las recomendaciones de la Asamblea del Consejo de Europa, Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos; Carta de Derechos Fundamentales de la Unión Europea (artículo 8); Tratado de Funcionamiento de la Unión Europea (artículo 16 TFUE). Y, determinando el actual marco regulatorio específico aplicable en la UE, el vigente Reglamento UE 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de datos personales).

62

Centrado este estudio, de forma principal, en el estudio del derecho a la protección de datos y su configuración en el marco del Derecho europeo, en primer lugar, cabe mencionar que este derecho se reconoce como un valor digno de especial protección por el Artículo 8 de la Carta de los Derechos Fundamentales (2010/C 83/02), donde de forma expresa se proclama que “*Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*”; de igual modo, dicta el Artículo 16 del Tratado de Funcionamiento de la Unión Europea (Art.16.1 TFUE), precepto que a su vez otorga competencias normativas a la Unión Europea sobre esta materia.

Ahora bien, conviene puntualizar que los datos personales protegidos no son únicamente aquellos relativos a la vida personal o a la intimidad de una persona, pues también abarcan a cualquier tipo de información relativa a un individuo, y cuyo conocimiento, comunicación o uso por terceros (no autorizados de forma expresa por el titular de los datos) puede afectar o perjudicar al mismo (persona titular del DPD); esto es, incidiendo de forma negativa o vulnerando su(s) derecho(s), inclusive aquellos otros que no fueran fundamentales.

Al respecto, también conviene advertir que el ámbito objetivo del derecho a la protección de datos es amplio, quedando identificado como tal la información personal (objeto de tutela específica), que de igual modo integra aquellos datos sujetos a información pública; esto es, que fueran, -en principio-, de libre acceso para cualquier interesado. Ya que no por el hecho de ser “pública” dicha información (por ejemplo, vía su constancia en registro público, base de datos o análogas fuentes, o bien por otro



cualquier otro medio de comunicación) dejaría de estar bajo la facultad de disposición que es reconocida al titular de dichos datos (afectado).

Este planteamiento inicial, en buena lógica parece fuera de duda, pero lo cierto es que la cuestión no ha sido pacífica. De este modo, sentar esta interpretación ha precisado del buen hacer procurado por la doctrina. En este sentido, hay que destacar, en nuestro país, la jurisprudencia consolidada en materia de protección de datos y asimismo en relación con otros derechos fundamentales vinculados, que ha sido dictada, en España, por el Tribunal Constitucional (TC) y por el Tribunal Supremo. Gracias a varios pronunciamientos (entre otros, se refieren los más relevantes infra), junto los aportados por el propio TJUE (objeto específico de estudio en este texto), cabe afirmar que hoy felizmente han sido positivizados en el Ordenamiento vigente nuevos derechos fundamentales (o lo que se conoce bajo el término genérico de “derechos de última generación”), siendo, por tanto, así configurados con identidad y régimen jurídico propio en el Derecho de la UE.

Tal es el caso del denominado “derecho de autodeterminación informativa”, reconocido por el Tribunal Constitucional (STC 292/2000, de 30 de noviembre)<sup>3</sup>, y asimismo en relación con el mismo, el derecho fundamental que ha sido acuñado como "libertad informática" (cfr., STC 254/1993, de 20 de julio, 94/1998, de 4 de mayo, y STC 202/1999, de 8 de noviembre)<sup>4</sup>; de igual modo, más recientemente, en virtud de otros pronunciamientos relevantes ha sido configurado el “derecho al olvido”.

63

En particular, la citada doctrina sobre el derecho al olvido ha sido sentada por el Tribunal de Justicia de la Unión Europea (TJUE) en la Sentencia de 13 de mayo de 2014 “asunto Google”, y posteriormente, también queda completada por otras, como la STJUE de 9 de marzo de 2017. En el mismo sentido, en España, STS 545/2015, de 15 de octubre de 2015, reconoce el “derecho al olvido digital”, y, por otra parte, también con motivo de otros asuntos, han sido dictadas decisiones judiciales que han rechazado su aplicación en otros casos planteados (cfr., Auto TS Civil 4 abril 2018). Todo ello, pone de relieve que el derecho al olvido es una doctrina consolidada, pero no implica reconocer un derecho absoluto, ni universal, pues implica la valoración de cada supuesto en concreto.

Esta doctrina del “derecho al olvido” por su interés y actualidad jurídica, es analizada de forma específica en este texto (vid., ulteriores epígrafes 5 y 6), procediendo así a ofrecer un examen acerca de dos de las sentencias europeas que estimamos destacan en esta cuestión, al perfilar la interpretación de este derecho y su delimitación, a saber, STJUE 2014 y STJUE 2017 (precitadas). En efecto, podemos hoy manifestar que estas resoluciones, sin duda alguna, han impulsado la configuración jurídica del DPD en el vigente Derecho positivo europeo. Siendo prueba de lo mencionado, el propio texto normativo del nuevo Reglamento general de protección de datos (RGPD), que ha

incorporado esta doctrina, entre otras novedades, que de igual modo son expuestas –en síntesis– en este trabajo (vid., epígrafe 4).

Completando lo señalado, y antes de analizar –de forma específica– la jurisprudencia europea precitada, es necesario hacer referencia a la doctrina del Tribunal Constitucional español dictada y en relación con esta materia; por estimar que facilita conocer el ámbito del DPD, cómo se interpreta y cuál ha sido su proyección jurídica. De este modo, en nuestro Ordenamiento cabe significar la STC 292/2000, en la que se expone con suma claridad el contenido y la delimitación del “derecho a la protección de datos”, y, además, detalla su diferenciación con respecto al “derecho a la intimidad” del Artículo 18.1 Constitución Española (vid., F.J. 5º y 6º)<sup>5</sup>. Asimismo, en esta sentencia, el TC señala que, si bien ambos derechos son fundamentales, hay que admitir la propia singularidad del derecho a la protección de datos frente a aquel; y ello, porque el objeto del DPD es más amplio que el del derecho a la intimidad. De este modo, se razona lo expuesto, *“(…) ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 C.E., sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, F.J. 4), como el derecho al honor, citado expresamente en el art. 18.4 C.E., e igualmente, en expresión bien amplia del propio art. 18.4 C.E., al pleno ejercicio de los derechos de la persona”*.

64

Sentada esta doctrina, sin embargo, lo cierto es que abordar esta temática del DPD, en la práctica, no siempre es sencillo, ya que exige un análisis ponderado en cada caso, y, además, es preciso hacer hincapié en la evaluación de algunos aspectos relativos a su ámbito de ejercicio y limitaciones, entre otros. De forma específica, por ejemplo, convendrá examinar la delimitación del “derecho al olvido” en determinados supuestos, en los que el ejercicio de esta facultad puede colisionar con otros derechos fundamentales, o principios reconocidos por el Ordenamiento, sobre todo en atención a observar si concurre o ha de primar el interés público (v.gr., principio de transparencia, principio de publicidad registral, etc.), frente al interés privado que pudiera alegarse por el titular de datos afectado. En este sentido, la STJUE 2017 que es analizada en este trabajo resulta muy ilustrativa (vid., epígrafe 6). En cualquier caso, lo que se pone de relieve en esta cuestión es que son varios los elementos objeto de examen en atención a cada asunto; lo que a su vez demuestra que el derecho a la protección de datos personales y la aplicación, en particular, de la doctrina del “derecho al olvido” requieren mayor desarrollo. Quedando así patente que es de plena actualidad, sobre todo a la luz de reciente jurisprudencia europea (STJUE 2017), y en orden a observar la aplicación que sigue el RGPD en vigor.





Conforme a esta motivación, en este texto también se reflexiona (vid., epígrafes ulteriores) sobre la dimensión actual del DPD y cuáles son sus elementos esenciales, cómo ha evolucionado de forma positiva y cuál es su actual configuración jurídica en el Derecho comunitario europeo, y con el propósito de reforzar la tutela de este derecho fundamental. Derecho fundamental declarado (textos normativos citados, supra), que a su vez hoy, dando un paso más, también se reconoce como un valioso activo (desde un enfoque económico) y, por ende, “bien jurídico protegido” (desde la perspectiva jurídica actual).

### 2.2. **Ámbito de protección: datos personales, intimidad y privacidad**

En España, conforme ha sido expuesto (STC precitada), el objeto del derecho fundamental a la protección de datos no sólo se refiere a los datos íntimos de la persona, sino “*a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales*”, por lo que el ámbito digno de protección aquí no es sólo la intimidad individual, -ya dotada de tutela por el art. 18.1 CE-, sino que de forma específica son los datos de carácter personal. Y como tales, también lo son aquellos datos personales públicos, “accesibles al conocimiento de cualquiera”, y que no por ello han de quedar fuera del poder de disposición del afectado (STC 292/2000, F.J.6º, párrafos 2º y ss.). Por tanto, estos datos públicos también deben ser protegidos, garantizando así a su titular una plena y eficaz tutela.

65

No obstante, con respecto a este último punto, hay que tener en cuenta la posibilidad prevista en el nuevo RGPD en orden a la aplicación de determinadas excepciones al régimen general, cuando se trate de datos o información de interés público, conforme dicta la legislación vigente, véase por ejemplo lo previsto en Considerandos 55, 36, 73 y 154 RGPD (actividades electorales, acceso del público a documentos oficiales, información en registros públicos, entre otros supuestos posibles). Esto es, en atención a objetivos importantes de interés público general de la Unión o de un Estado miembro.

En consecuencia, se infiere que, en principio –esto es, con carácter general-, el DPD otorga plenas facultades de disposición a su titular en lo relativo a información privativa o datos personales; esto supone, v.gr., que el titular podrá conocer y decidir sobre el tratamiento conferido a sus datos, y, por ende, en un sentido extensivo, sobre toda información relativa a su persona. Además, en este sentido conviene precisar otro aspecto relevante, como es el hecho de que el DPD queda vinculado -de forma necesaria- con la noción de “privacidad”.

La privacidad es, sin duda, un apreciado valor intangible, consustancial a la personalidad humana y factor determinante de una adecuada calidad de vida. Por ello, hoy adquiere una identidad jurídica propia, y así se configura como un bien jurídico digno de especial protección, por ser sumamente sensible a impactos externos adversos (que la perturben o vulneren). Por tanto, este concepto jurídico “de nueva generación” ligado al reconocimiento de los derechos de la personalidad y a la dignidad humana, se

añade como un aspecto más, que cabe estimar y observar por su directa relación con el DPD; en este sentido se ha pronunciado la doctrina<sup>6</sup>. Con todo, en la actualidad, existe consenso acerca de que, en efecto, se trata de un bien sensible que precisa del máximo grado de tutela jurídica pública, al ser consustancial a la dignidad, y como tal constituye un presupuesto esencial ligado al derecho fundamental a la intimidad.

A su vez, cabe recordar que el derecho a la intimidad, expresamente consagrado junto con el derecho al honor y a la propia imagen por la Constitución Española (Artículo 18 CE, 1978), se asienta en la necesidad de disponer por toda persona de una esfera interior protegida frente a posibles injerencias externas; esto es, no se trata tanto de un derecho a ocultar aspectos personales, sino más bien un deber de respeto hacia un ámbito de libertad individual que es esencial para el pleno desarrollo de la personalidad y para garantizar la dignidad humana<sup>7</sup>. Pero, además, implica que los poderes públicos adopten las medidas oportunas para proteger al ciudadano afectado, pues solo así cabe asegurar la efectividad de este derecho<sup>8</sup>.

66

Ahora bien, mencionado lo anterior, conviene puntualizar que la noción de privacidad es más amplia, tiene mayor alcance, y, por ende, va más allá que el propio concepto de intimidad, tal y como ha declara el Tribunal Europeo de Derechos Humanos<sup>9</sup>. En consecuencia, hay que diferenciar privacidad y derecho a la intimidad, admitiéndose en todo caso la concurrencia lógica de los vínculos existentes entre ambas nociones.

Por tanto, el fundamento de la privacidad, en concreto, se ubica en el respeto a la intimidad y dignidad humana, y asimismo comprende la libertad para decidir sobre el control de la información personal del individuo y sobre la disposición o el posible uso en lo relativo a los (sus) datos personales. De este modo, cabe inferir que esta noción aporta un valor añadido esencial en aras de propiciar la funcionalidad del derecho a la protección de datos, objeto principal de este estudio. Esto es, la privacidad opera como presupuesto esencial que posibilita materializar la propia singularidad de este derecho; y con ello, facilita el eficaz ejercicio del mismo, a fin de garantizar que este pueda ser alegado frente al posible empleo o difusión de datos -no autorizado- que generador de graves perjuicios o efectos adversos para el titular de los mismos<sup>10</sup>.

### **3. EL TRATAMIENTO DE DATOS PERSONALES EN EL DERECHO EUROPEO: EVOLUCIÓN Y RÉGIMEN VIGENTE (RGPD)**

Con respecto al tratamiento de datos, hay que destacar que, en ámbito comunitario, durante este tiempo, ha sido un aspecto al que se ha prestado especial atención para diseñar una normativa que permitiera conciliar la protección de datos con la dinámica que, por otra parte, supone el derecho a la libertad de información (veraz)<sup>11</sup>. En este sentido, en el Derecho comunitario europeo el tratamiento y circulación de información



relativa a datos personales, fue previsto por la Directiva 95/46/CE (cf., artículo 1.2.), señalando que la libre circulación de datos entre los Estados no debía ser prohibida o afectada por restricciones –en principio–, por lo que ha de resultar compatible con la pretendida protección de datos<sup>12</sup>. De forma expresa el vigente RGPD, en su artículo 1.3., dice, “*La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*”.

No obstante, en este tiempo, era preciso instaurar un régimen jurídico europeo más completo y eficiente en aras de asegurar el valor y la debida tutela del DPD. En este camino evolutivo y para procurar avanzar en dicho propósito, ha sido fundamental el papel desempeñado por la doctrina jurisprudencial, y, en la actualidad, queda previsto el texto actual del RGPD. Cuyo artículo 4 define «tratamiento»: “*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*”; y, además, precisa la noción de «limitación del tratamiento»: “*el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*”; y, a continuación, establece los Principios aplicables para proceder a la ejecución adecuada, artículo 5, “Principios relativos al tratamiento”, y en los artículos 6 a 11, desarrolla cada uno de los mismos).

67

Al respecto, consideramos oportuno examinar estas nociones jurídicas que son básicas en esta materia, pues constituyen los pilares determinantes del DPD conforme al actual régimen aplicable. Y realizar algunas precisiones en cuanto a la terminología empleada.

### 3.1. Noción jurídica de tratamiento de datos

Hay que recordar que la Directiva 95/46 CE<sup>13</sup> sobre tratamiento de datos de carácter personal se adoptó con la finalidad principal de *armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros*. Si bien, la práctica ha demostrado –en estos años– que sus directrices no fueron suficientes para lograr la pretendida armonización entre las legislaciones nacionales; y, además, la dinámica comunicativa y comercial de la era digital advirtió sobre nuevos riesgos, por lo que ha sido preciso diseñar un régimen jurídico, más actualizado, y que con rigor (efectos directos y vinculantes) reforzara la tutela pública del DPD en la Unión Europea.

De este modo, ha sido adoptado el Reglamento general de protección de datos (RGPD 2016)<sup>14</sup>, cuyo marco jurídico vinculante significa el DPD, configurado con entidad propia, y a su vez estimando el deber de respetar todos los derechos fundamentales,

libertades y principios reconocidos en la precitada Carta de Derechos Fundamentales, conforme asimismo declaran los Tratados. Así, el RGPD subraya, “*en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información (...)*”. Y, a su vez, se señala la posible delimitación del derecho a la protección de datos, por cuanto este DPD no es un derecho absoluto; ergo, en su consideración y aplicación ha de proceder en equilibrio con otros derechos fundamentales, esto es, en atención al *principio de proporcionalidad* (Considerando 4).

Al respecto, también el RGPD señala que las posibles limitaciones a su ejercicio han de estar previstas legalmente, conforme a observar los criterios comunes fijados por esta normativa, y además han de ser implementadas con base a instrumentos y medidas que se dictaran por cada Estado respetando unos criterios uniformes, conforme a lo dictado por dicho régimen jurídico, y en todo caso, garantizando el principio de legalidad y seguridad jurídica, así como el principio de transparencia informativa.

68

En este aspecto insiste el RGPD, también en relación con el régimen de control y supervisión que opere en cada Estado, vías para reclamaciones y recursos, y régimen sancionador, entre otras posibles herramientas que habilitara cada Estado para la tutela del DPD<sup>15</sup>; asegurando que todas ellas puedan ser accesibles para el interesado/s, así como sus efectos o consecuencias previstas. De igual modo, señala que dichas restricciones han de ser motivadas, ponderando su aplicación en cada caso y su justificación; ya que en una sociedad democrática se ha de asegurar que cualquier eventual limitación relativa a derechos/libertades fundamentales ha de ser razonada, congruente e indispensable, cumpliendo con el principio de proporcionalidad<sup>16</sup>.

### **3.2 Motivación del impacto de esta cuestión en la normativa europea**

Expuesto lo previo, cumple afirmar que la configuración actual del DPD como derecho fundamental<sup>17</sup>, -asimismo reconocido como bien jurídico digno de una especial protección por parte del Ordenamiento europeo e interno (o nacional)-, ha sido fruto de una positiva evolución de la arquitectura legal europea, en gran medida impulsada por la reciente doctrina jurisprudencial y científica, como ya se ha expresado en el epígrafe precedente. A su vez, se admite la complejidad de esta materia, como viene demostrando la práctica jurídica en este campo, sobre todo ante los desafíos que plantean los actuales (y futuros) entornos tecnológicos globales, donde de forma generalizada o mayoritaria opera la comunicación y dinámica informativa (mediante el empleo de TIC, servicios y plataformas digitales, difusión vía internet, etc.). En este contexto es evidente que el Derecho de la UE ha de afrontar con éxito los “nuevos fenómenos que surgen en los nuevos entornos donde se opera y prestan servicios”, como ya se ha señalado con carácter previo en este texto (por ejemplo, beneficios vs.



amenazas o riesgos generados por el uso de herramientas telemáticas o electrónicas) en estos escenarios. En este sentido, se pronuncia el Considerando 6 del RGPD.

Por tanto, ha sido preciso abordar con mayor rigor la protección de datos por el Ordenamiento europeo, ya que el tratamiento de datos también implica considerar el DPD en relación con otros derechos fundamentales (conciliación). En este sentido, por ejemplo, el Considerando 153 RGPD, señala que el Ordenamiento de los Estados miembros ha de conciliar el DPD con “*las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, (...)*”. Y, en todo caso, dice, como premisa general, Considerando 2 RGPD, que el tratamiento de datos de carácter personal debe respetar las libertades y derechos fundamentales, añadiendo que este Reglamento “*pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas*”. Lo expresado, por ende, es coherente con lo declarado en el Considerando 4 RGPD, “*(...) El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad*”.

69

Por otra parte, también el propio RGPD advierte sobre la necesidad de observar en determinados casos la concurrencia de razones de interés público que han de primar (por lo sí cabe posibles excepciones al régimen general previsto por el vigente RGPD). En este sentido, se señala que cuando exista un interés público “deben” autorizarse excepciones a la prohibición de tratar ciertas categorías especiales de datos personales cuando así lo determinara el Derecho de la Unión o de los Estados miembros, “siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales”, por ejemplo, por razones de seguridad, supervisión, investigación de infracciones o delitos, salud pública, y también en el ámbito de la legislación laboral, protección social, pensiones, entre otros. (vid., Considerandos 52, 54, 55 y 56,...).

En consecuencia, si concurre un interés general o colectivo, que ha de ser atendido de una forma satisfactoria ha de ser atendido por autoridades europeas e internas, de forma coordinada, colaborativa y eficaz. Lo que también pone de manifiesto que la aplicación del nuevo régimen general en materia de protección y tratamiento resulta de interés tanto desde su perspectiva técnica y jurídica, como cultural, social y económica. Lo que no impide reconocer que precisará de los oportunos desarrollos mediante normativa interna o nacional con de fin de concretar su adecuada aplicación en determinados supuestos.

En este sentido, también el propio texto del RGPD reconoce la importancia de lo mencionado, al admitir e identificar con certeza que “La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales”

(Considerando 6). Y, en consecuencia, se advierte que *“Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas”* (Considerando 7).

En todo caso, los Considerandos del texto normativo RGPD motivan, con detalle, la necesidad de disponer de una regulación común (general) que ha de servir para armonizar y dar mayor uniformidad a las legislaciones de los Estados miembros de la UE en esta materia, y superando a la previa Directiva. Y conforme a esta finalidad principal se dicta este nuevo acto normativo, Reglamento europeo, de aplicación directa y vinculante en todos los Estados miembros de la UE.

70

A su vez, el RGPD supone revisar y actualizar otras normativas europeas dictadas en tanto establecían directrices acerca del régimen aplicable a determinadas tipologías de tratamiento, este es el caso en particular de la 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<sup>18</sup>.

Así, el RGPD 2016 (precitado) incorpora relevantes novedades, dictando un marco regulatorio europeo común más sólido, para garantizar una eficaz tutela del DPD, y cuya preceptiva ejecución genere confianza y seguridad; lo que, por otra parte, es clave para el desarrollo del mercado interior asimismo en aras de encaminar buenas prácticas (lícitas y respetuosas) ante el paradigma de la economía digital. Pues, con todo, no se puede ignorar que los datos personales suponen un valioso activo, detectado por los principales operadores y sectores en un mercado competitivo. Por ello, ahora más que nunca, -cabe inferir- el DPD ha de contar con una tutela pública reforzada. No siendo esta una cuestión casual o de menor importancia frente a otros temas.

En este escenario jurídico y estratégico, el vigente Reglamento (RGPD) fija las normas uniformes y específicas que podrán garantizar un alto nivel de protección de los datos de las personas físicas y, a su vez, evitar las posibles barreras que obstaculizasen la circulación de información y datos personales dentro de la UE. Al efecto, resulta claro que el grado de protección brindado a los derechos y libertades de las personas en lo relativo al tratamiento de sus datos ha de ser el mismo en todos los Ordenamientos nacionales; esto es, conforme a unas reglas básicas comunes y sin que existan discrepancias entre las legislaciones de los Estados miembros. Y, en todo caso, el RGPD hace especial hincapié en una premisa que ha de resultar clave en esta disciplina: las personas físicas deben tener el control de sus propios datos personales, para lo cual



debe ser reforzada la seguridad jurídica y la práctica operada por las personas físicas, los operadores económicos y las autoridades públicas.

Lo mencionado, por tanto, conlleva promover modelos de tratamiento y gestión responsable de los datos personales, lo que se propugna como un deber para los operadores que actúen en el ámbito de la UE, asimismo podrá ser para entidades internacionales interesadas o con establecimiento en la misma (físico o virtual), que presten servicios o emprendan actividades que impliquen el tratamiento de datos. De igual modo, se insiste en el deber de las autoridades competentes de los Estados miembros en orden a garantizar la debida tutela pública del derecho a la protección de datos (DPD); por lo que será preciso establecer los oportunos desarrollos normativos, habilitar las medidas necesarias de control y supervisión, así como eficaces vías que permitan atender con celeridad posibles reclamaciones o recursos, entre otros protocolos de acción.

Sin duda, con ello se trata de promover sistemas de gestión y tratamiento de datos “corresponsables”, en donde de forma proactiva colaboren todos los actores y sectores (privados y público); lo que, en efecto, implicará vigilar buenas prácticas, implementar procedimientos de autoevaluación, de prevención de riesgos y de seguridad, además de los correspondientes de evaluación (por tercera parte independiente), acreditación y verificación. Pues, no se puede ignorar la especial naturaleza que caracteriza y es precisa el tratamiento de datos, en el que concurren elementos técnicos y jurídicos, (entre otros posibles, como los reputacionales), como ya ha sido puesto de relieve por la doctrina científica y por la propia jurisprudencia, asimismo estas consideraciones han sido estimadas, de forma progresiva, por la legislación dictada en esta materia<sup>19</sup>. No obstante, y aunque el avance ha sido favorable, aún cabe admitir que resta por hacer en este sentido a fin de enfrentar con éxito nuevos retos jurídicos.

71

### 3.3. Los “Principios de la protección de datos”

Sumado a las nociones y consideraciones expuestas, cabe señalar que el régimen jurídico (general) aplicable a la PDP establece un cuadro preceptivo de “Principios de la protección de datos”<sup>20</sup>, que permiten concretar el DPD en la práctica de su ejercicio, así como cuáles son los aspectos, facultades y obligaciones que deben ser observadas en lo relativo al tratamiento de datos. El cuadro básico de estos principios ya quedaba previsto en la Directiva, pero, ha sido completado con otros en el actual RGPD. Aquí de nuevo digno es significar la aportación de la Jurisprudencia.

De este modo, al vigente texto del RGPD dicta una serie de principios rectores (en concreto, se declaran seis) que en esta materia han de servir para disciplinar toda acción y proceso de gestión de la información y comunicación sobre datos personales; con ello, en el tratamiento de datos personales son de necesaria observancia dichos presupuestos. Esto es, más allá de ofrecer una mera guía facilitadora u orientativa, son principios preceptivos, cuyo cumplimiento es obligado. Hacer hincapié en este aspecto es

importante, tanto desde una perspectiva estratégica y operativa, como sobre todo a efector de poder acreditar seguir un óptimo cumplimiento legal (*compliance*), por parte de entidades, empresas y profesionales. Y ello, porque estos principios no solo han de constituir un modelo autorregulatorio o código de conducta y buena praxis en materia de DPD, que cada operador pudiera adoptar; sino que su implementación es obligada, en el presente, ya que forman parte de la propia base regulatoria dictada (Sistema jurídico europeo aplicable en esta materia, desde el pasado 25 de mayo de 2018, cf., Artículo 99 RGPD). De este modo, el Artículo 5 del Reglamento General de Protección de Datos dicta estos seis principios, y que son desarrollados con precisión a lo largo de este texto normativo, siendo por tanto premisas claves del régimen vigente, y como tales han de ser consideradas en el empleo, tratamiento y almacenamiento de datos de carácter personal a. En síntesis, el contenido enunciado de estos seis principios es:

- Los datos personales han de ser tratados de forma lícita, leal y transparente.
- Los datos personales deben ser recogidos con fines concretos, explícitos y legítimos.
- Los datos personales deben ser adecuados, pertinentes y limitados a la finalidad que motiva su tratamiento.
- Los datos personales deben ser veraces, exactos y actualizados.
- Los datos personales han de mantenerse de forma adecuada (custodia) y de forma que se pueda permitir su identificación y conocimiento por los interesados; además, dicho empleo, depósito o registro únicamente lo será por el tiempo máximo que fuera necesario para los fines del tratamiento.
- Los datos personales han de ser tratados de forma que se garantice su seguridad (gestión y prevención de riesgos).

72

Estos principios son desarrollados en los siguientes preceptos de este Reglamento (Artículos 6 a 11). Y, entre ellos, hay que destacar el “principio de finalidad”<sup>21</sup>, en virtud del cual, los datos han de ser recogidos para fines determinados (Art.5.1.b. RGPD), ya que supone un presupuesto preliminar que resultará idóneo para evaluar cada práctica operada en este terreno; y, en particular, en orden a poder valorar (o acreditar) el grado de (su) adecuación que un operador obligado (entidad, empresa o profesional) cumple el vigente RGPD<sup>22</sup>.

#### **4. REFERENCIA A LAS PRINCIPALES APORTACIONES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)**

Además de lo señalado en materia de tratamiento de datos personales, es necesario, - considerando el objeto de este estudio y para concluir el mismo-, dedicar un epígrafe a significar cuáles han sido las principales novedades incorporadas por el nuevo RGPD<sup>23</sup>. Con ello, se pretende ofrecer una síntesis del régimen jurídico europeo general hoy





vigente, exponer su funcionalidad, así como propiciar una reflexión sobre las implicaciones que conllevara en el Derecho de la Unión Europea.

### 4.1. Principales aportaciones

El Reglamento General de Protección de Datos nace con la intención del Parlamento europeo y del Consejo europeo de unificar el criterio y legislación en materia de protección de datos en los Estados Miembros de la UE, ya que la previa Directiva (derogada por este Reglamento) no logró armonizar las diferentes leyes estatales, que incluso en ciertos casos resultaban poco rigurosas o ineficaces, v.gr., en lo relativo a dictar unas medidas mínimas exigibles en seguridad, régimen sancionador, entre otros aspectos que hoy se evidencian fundamentales para la protección eficaz del DPD. Por ello, el RGPD insiste en fijar un régimen básico, común y vinculante, en lo relativo al tratamiento de la información personal. Y, además, se acentúa lo relativo a las facultades y defensa de los ciudadanos ante la posible vulneración de sus derechos (v.gr., usuarios de servicios y comunicación a través de la Red, redes sociales y páginas web, u otras plataformas accesibles).

El RGPD entró con plenos efectos en vigor el 25 de mayo del 2018 (art. 99 RGPD). Y deroga de forma expresa la Directiva previa (art. 94), así como cualquier legislación anterior, europea y nacional, que pudiera ser contraria a la misma. En el caso de España, la normativa dictada: Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de carácter personal (LOPD), y en su desarrollo el Real Decreto 1720/2007, del 21 de diciembre. Como Reglamento europeo que es, tiene carácter vinculante y de aplicación directa en todos los Estados de la UE, regulando la protección de las personas físicas en lo que respecta: (i) al tratamiento de datos personales y (ii) a la libre circulación de estos datos. En concreto, este régimen es aplicable “al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero” (Artículo 2.1); quedando excluido, de forma expresa, el tratamiento de datos que operase en los siguientes supuestos (Art.2.2.): “a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención”.

Este sistema jurídico resulta innovador en algunas cuestiones, entre otras, por ejemplo, incorpora nuevos principios y deberes respecto a la precedente Directiva. Con ello, el marco regulatorio europeo queda completado y actualizado. Dicho régimen focaliza una serie de principios que han de regir en materia de protección de datos, y a su vez, dicta una serie de deberes que los sujetos obligados (entidades, empresas y profesionales) han

de cumplir, en relación con el tratamiento y privacidad de información y datos. También refiere códigos de conducta y guía modelos autorregulatorios; establece un régimen de evaluación y verificación; autoridades y organismos competentes, a efectos de dictar desarrollos normativos y habilitación de medidas de control; y, por último, disciplina un régimen de responsabilidad y sancionador. Conforme a lo señalado, todas las entidades y profesionales que traten datos de carácter personal han de tener adaptados sus sistemas y medidas de tratamiento de datos, herramientas y registros informativos, medios informáticos e instrumentos contractuales. En este sentido, con respecto a las obligaciones que corresponden a los sujetos responsables (y encargados), deberán identificar y evaluar las áreas o escenarios de riesgo, marcar protocolos de comunicación y para solicitar los oportunos consentimientos (que precisan de constancia expresa), así como documentar los tratamientos que cada entidad implementa y conforme a la tipología de datos personales que se emplean o usan. Para lo cual, se ha de realizar un inventario de todas las acciones o prácticas de tratamiento que efectúa cada empresa. También designar a la figura del Delegado de datos, tal y como ordena el RGPD.

#### **4.2. Deberes para los operadores (entidades, empresas y profesionales)**

74

Entre las obligaciones que afectan a los sujetos responsables del tratamiento de datos (operadores), cabe destacar:

- La incorporación necesaria de la figura del Delegado de Protección de Datos (DPD). El Reglamento obliga a quienes realicen ciertos tratamientos, a designar un delegado, que ha de ser un profesional experto, que disponga de una formación específica y acreditada, tanto en PDP como en análisis de riesgos y medidas de seguridad de la información, que podrá ser personal interno o externo a la entidad.
- La obligación de registrar documentalmente las acciones y procesos de tratamiento. Dicho deber, corresponde tanto a los Responsables de ficheros como a los Encargados del tratamiento de datos (figuras definidas en el Artículo 4, apartados 7 y 8).
- Para el tratamiento de datos personales, se exige disponer del previo consentimiento expreso por parte del titular de los datos. En consecuencia, ya no es suficiente con un consentimiento tácito, por lo que los operadores o empresas quedan obligadas a solicitar dicho consentimiento y asegurar su constancia, también respecto a los datos previos de que dispongan (antes de la entrada en vigor del RGPD).
- Es necesario implementar métodos de evaluación de impacto y análisis de riesgos, haciendo especial referencia al tratamiento de cierta tipología de datos, medidas preventivas y de seguridad adoptadas.
- Quedan reforzados los deberes de transparencia informativa.
- Se establece la obligación de notificar cualquier tipo de vulneración de los sistemas de seguridad implementados relativos los datos personales. Así, en



plazo máximo de 72 horas deberá ser comunicado cualquier eventualidad a la Agencia Española de Protección de Datos (AEPD), y de igual modo, en casos graves será necesario notificarlo a los afectados o interesados, con el fin de evitar mayores daños o perjuicios.

- Conforme al RGPD, será preciso revisar los instrumentos contractuales vigentes, así como diseñar nuevos modelos contractuales asegurando que cumplen con el RGPD. De igual modo, será necesario proceder a realizar nuevos contratos con los encargados de tratamiento, en cuyo clausulado se ha de prestar especial atención en lo relativo a las facultades de acceso a datos por terceros (respetando lo previsto como “contenido mínimo necesario”).
- Por otra parte, cabe señalar que -en principio- el RGPD no diferencia entre datos personales y datos profesionales. Por lo que las empresas han de adoptar las oportunas acciones en atención a cada perfil y categoría de datos.

### 4.3. Derechos de los ciudadanos

A su vez, el RGPD incluye nuevos derechos del ciudadano, que completan a los ya reconocidos por la normativa precedente (Directiva y LOPD, en España). De este modo, el cuadro de derechos previsto comprende los siguientes: derecho de acceso, derecho a la portabilidad de datos, derecho de cancelación, derecho de rectificación, derecho de oposición, y el “derecho al olvido”. Este derecho al olvido, -expuesto con detalle en epígrafe previo-, en la práctica, supone una manifestación de los derechos de cancelación u oposición en el entorno digital u online. No obstante, este derecho tiene algunas limitaciones como son: la libertad de expresión, el derecho a la información, el interés público en el ámbito de la salud, la investigación, y la defensa de reclamaciones o recursos.

75

Y, además, de forma específica se reconoce el “derecho a la limitación del tratamiento”, y el “derecho a no ser objeto de decisiones individualizadas”, de forma que no se podrán adoptar decisiones que incluyan medidas -no consentidas de forma expresa por el interesado- cuando estas evalúen o valoren aspectos personales, o con referencia a la persona, o medidas basadas en el tratamiento automatizado y que pudieran generar perjuicios o efectos jurídicos en el titular de datos, o que le afectaran de forma grave.

## 5. DOCTRINA EUROPEA SOBRE “EL DERECHO AL OLVIDO” (STJUE DE 13 DE MAYO DE 2014)

El 13 de mayo de 2014 la Gran Sala del Tribunal de Justicia de la Unión Europea dictó Sentencia en el asunto *Google Spain S.L c. Agencia Española de Protección de Datos (AEPD)*<sup>24</sup>, con este pronunciamiento se responde a la cuestión prejudicial planteada en 2014, por la Sala de lo Contencioso-Administrativo de la Audiencia Nacional (España) en el caso relativo a lo que se ha denominado “derecho al olvido”. Siendo este asunto de gran repercusión en los medios de comunicación europeos e internacionales<sup>25</sup>, hoy

mantiene su interés y actualidad jurídica. Con este pronunciamiento del Alto Tribunal, concerniente a la interpretación del Derecho europeo e interno (en España, LOPD conforme a la Directiva 95/46/CE)<sup>26</sup>, concreta de forma definitiva las responsabilidades de los buscadores de internet en relación con la protección de los datos personales, y asimismo otorga tutela ante la situación de indefensión generada, en este asunto, al no haber admitido la compañía Google que le era aplicable la normativa española y europea reguladora de la materia.

En esta sentencia, se declaran entre otros aspectos fundamentales, los siguientes<sup>27</sup>,

(i) La actividad de los motores de búsqueda supone el tratamiento de datos de carácter personal, siendo responsable de la misma la entidad que desarrolla dicha acción: el propio motor, dado que éste determina los fines y los medios de esta actividad.

(ii) Ese tratamiento está sometido a las normas de protección de datos de la Unión Europea, cuando la entidad o compañía dispone en un Estado miembro de establecimiento destinado a la actividad mercantil o de promoción de espacios publicitarios, y asimismo realiza una actividad que se dirige a los ciudadanos de dicho Estado.

(iii) Se reconoce el ejercicio del derecho a las personas a solicitar del motor de búsqueda que se supriman referencias a información o datos que les afecten, incluso cuando si dicha información no hubiera sido eliminada por el editor de la misma, o no se hubiera promovido su desindexación. En su defecto, las personas afectadas podrán reclamar ante la AEPD y los Tribunales.

Lo descrito supuso una importante aportación, así pues, se configura la denominada doctrina del “derecho al olvido” (en la actualidad, ya integrado en el texto del vigente RGPD). Si bien, al respecto es oportuno recordar que ya, previamente, la AEPD había defendido dicha argumentación, interpretando que sí era aplicable en este caso, conforme a la legislación española y europea vigente en aquel momento. En este sentido, la doctrina española ya hace hincapié en el fundamento del derecho al olvido, que se infiere de los propios principios y valores enunciados en el Artículo 10.1 Constitución<sup>28</sup>. Más lo cierto es que de forma explícita la doctrina del derecho al olvido no se formularía -como tal- hasta dictar esta Sentencia 2014, que fue así favorable a la pretensión y argumentación defendida por España. En este sentido, digno es apreciar que fue relevante la labor de la AEPD y de la Abogacía del Estado en este procedimiento europeo, tal y como ha sido reconocida<sup>29</sup>. No obstante, se debe insistir en que el derecho al olvido, que confirma el TJUE con este pronunciamiento, no supone un derecho absoluto, y, por ende, mantiene un alcance limitado. En la práctica, su ámbito de aplicación comprende el que ya era



reconocido a los derechos de cancelación y oposición, y es a través de ellos como asimismo puede ser ejercitado, por el afectado/s (titular de los datos).

En definitiva, en virtud de esta STJUE 2014, y conforme a la Directiva 95/46/CE, se dictó que los responsables de los motores de búsqueda en internet quedaban obligados a reconocer a los afectados lo que se denominó el “derecho al olvido”, que suponía ejercer los derechos de oposición y de cancelación (en este caso aplicados a información disponible en la red), contenidos en dicha normativa europea y que integran el derecho fundamental a la protección de los datos personales. A dicho efecto, los interesados han de dirigirse al buscador y solicitar que cese la difusión de datos cuando estos pudieran afectar o producir lesión en sus derechos, sin justificación suficiente.

(iv) Se declara la preferencia del DPD. Lo que supone que, con carácter general (o, en principio), ha de prevalecer el derecho a la protección de datos de las personas frente al interés privativo de un operador o mercantil. Por ejemplo, en este caso, se dicta que prevalece dicho derecho fundamental sobre el “mero interés económico del gestor del motor de búsqueda”. Si bien, también cabe admitir como posible excepción en aquellos supuestos en que el interesado fuera persona de relevancia pública y/o el acceso a la información quedara justificado con base al interés público.

77

En suma, dicho litigio permitió sentar la doctrina del derecho al olvido, y con ello se puso de manifiesto la necesidad de fijar una normativa europea común más sólida que resultara eficaz en aras de asegurar la protección de datos. A su vez, también ya se precisa que el derecho al olvido admite ciertos límites, justificados, en aras de hacer compatible su ejercicio con el respeto a otros derechos fundamentales reconocidos, y, de igual modo, en atención a la preferente tutela del interés público en determinados supuestos (por ejemplo, porque se tratara de una información relevante para la ciudadanía u opinión pública, entre otras razones, como ya hoy constan previstas en el texto vigente del RGPD, tal y como hemos referido supra). Recordando, en este sentido, la importancia del principio de transparencia y el derecho de acceso a la información pública, previstos en el Ordenamiento<sup>30</sup>.

Además, con esta resolución STJUE 2014 donde se reconoce, -por vez primera de forma expresa-, el «derecho al olvido» frente a los motores de búsqueda, también resulta ilustrativa para otros planteamientos, y permite reflexionar sobre la necesidad de prevenir eventuales riesgos o amenazas vía entornos digitales (v.gr., uso y difusión de información o datos sin disponer del previo consentimiento del titular de los mismos, entre otros)<sup>31</sup>, sin duda, motivados por una fácil y generalizada accesibilidad a la red, o el empleo masivo de otras redes o vías electrónicas de comunicación para ofrecer o prestar de servicios global, etc.<sup>32</sup> Y, con todo, esta doctrina del “derecho al olvido” ha supuesto una importante aportación, que orienta la innovación jurídica en materia de

protección de datos; al considerar de forma específica la no adecuación a Derecho de determinadas prácticas que se desarrollan en los entornos digitales<sup>33</sup>. Agregado a ello, cabe advertir que no siempre la información divulgada es con base a fuentes de calidad, o pudiera contener sesgos o no ser veraz<sup>34</sup>. Por ende, esta STJUE fue determinante para estimar que era necesario fijar una regulación eficaz con el fin de tutelar el DPD en la Unión Europea. Y en este sentido, esta STJUE ha sido valiosa, propiciando una doctrina jurisprudencial que ha sido clave en este ámbito, de utilidad para orientar o impulsar el nuevo RGDE, que de forma expresa integra esta doctrina; y a su vez para encaminar el diseño de protocolos de actuación<sup>35</sup>. Con posterioridad, ha sido completada esta doctrina del “derecho al olvido” (STJUE 2014), mediante otros pronunciamientos; así, cabe citar la STJUE 2017 que ha permitido abundar en la configuración del “derecho al olvido”, en concreto, en lo relativo a los posibles límites que pudieran resultar aplicables a este derecho. Si bien, es necesario precisar que el “derecho al olvido” no es absoluto, por lo que admite limitaciones, como avanzó nuestro Tribunal Supremo (STS de 15 de octubre de 2015)<sup>36</sup>.

78

## **6. POSIBLES LÍMITES AL DERECHO DE ACCESO A LA INFORMACIÓN: ANÁLISIS DE LA STJUE DE 9 DE MARZO DE 2017**

La Sentencia del Tribunal de Justicia Europeo (TJUE), Sala Segunda, de 9 de marzo de 2017<sup>37</sup>, asunto C-398/15, *S. Manni c. Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce*, resulta ilustrativa en orden a ofrecer una delimitación del derecho al olvido en el ámbito de la información registral. De este modo, su análisis permite observar las implicaciones que el ejercicio del derecho al olvido puede conllevar observando su posible colisión con otros derechos (fundamentales); en este caso, el derecho de acceso a la información registral. El pronunciamiento dictado en este asunto muestra una posición europea neutral y sumamente orientativa para los Estados, con carácter general, a fin de evitar dudas interpretativas o prevenir ante eventuales conflictos, que se suscitaran y pudieran afectar al deber de transparencia informativa.

### **6.1. Exposición del asunto planteado (C-398/15)**

En síntesis, lo que en este asunto se plantea es si procede la aplicación del derecho al olvido con respecto a datos publicados en el registro societario (en Italia), -lo que en España es el Registro mercantil-. Y, esta sentencia, dictada en el asunto C-398/15 y con objeto de resolver el planteamiento de una petición de decisión prejudicial, que fue presentada -conforme al artículo 267 TFUE- por la Corte Suprema di Cassazione (Tribunal Supremo de Casación de Italia), a través de Resolución de 21 de mayo de 2015, recibida en el Tribunal de Justicia el 23 de julio de 2015, en el procedimiento entre *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce*, y *Salvatore Manni*.



Y, en este asunto, el pronunciamiento estimó los argumentos del Abogado General, y sostiene que los Estados miembros no pueden garantizar a las personas físicas el derecho a obtener la supresión de datos (personales) que figuren por su relación con sociedades mercantiles; asimismo, se señala que esta cuestión podrá ser prevista por la normativa estatal, evaluando cada supuesto, y, en su caso, después de la liquidación de la entidad mercantil (o societaria) de que se tratara, a efectos de la posible supresión de datos personales que conciernen a personas, inscritos en el registro. Pero, en todo caso, la Sentencia insiste en dar preferencia al interés general público; esto es, al derecho de acceso de información en relación con lo inscrito en el Registro, garantizando así la eficacia del principio de publicidad registral, así como el cumplimiento de la legislación vigente. Por tanto, la postura adoptada por el TJUE es neutral y conciliadora. Y, de igual modo, en este pronunciamiento se hace especial hincapié en la necesidad de proteger los intereses de terceros en relación con las sociedades mercantiles, la seguridad jurídica, la lealtad de las transacciones comerciales y el buen funcionamiento del mercado interior.

### **6.2. La postura neutral del Tribunal de Justicia de la Unión Europea**

Conforme a dicha resolución, el TJUE adopta una postura flexible que pretende ser conciliadora; al declarar, de forma expresa, que no cabe excluir el adoptar otras posibles medidas ante supuestos especiales. De esta forma, se abre la posibilidad de ponderar situaciones particulares que puedan surgir, en las que fuera procedente estimar o considerar determinados motivos que justificaran adoptar resoluciones extraordinarias (v.gr., que pudieran limitar de hecho el acceso a determinada información, o que establezcan restricciones temporales, u otras decisiones o protocolos que habilitara cada Estado miembro al respecto). Así, esta sentencia precisa que esta decisión corresponde, en cualquier caso, a los Estados miembros, conforme a la aplicación del Artículo 14, párrafo primero, letra a), de la Directiva 95/46<sup>38</sup>. Luego, por vía del Derecho interno nacional, cabe establecer disposición en contrario, y, de esta forma, adoptar una decisión final sobre si las personas físicas pueden (o no) solicitar a la autoridad competente y/o responsable del registro la posible aplicación de dicho tipo de limitación de acceso a los datos personales.

En definitiva, corresponderá al legislador interno/nacional regular esta cuestión y establecer la previsión de posibles excepciones o limitaciones. De igual modo, se señala que el Artículo 14 impone a los Estados miembros el deber de garantizar al interesado el ejercicio del “derecho de oposición”, en los casos previstos en las letras e) y f) del Artículo 7. Recordando a su vez que dicha facultad se podrá ejercer en cualquier momento, y con base a motivos legítimos, estimando cada caso concreto y cuando los datos que le conciernan sean objeto de adecuado tratamiento, *salvo cuando la legislación nacional disponga otra cosa*<sup>39</sup>.

## **CONCLUSIONES**

Expuesto lo anterior, cabe concluir afirmando que, en el contexto actual de la Unión Europea, sin duda, la tutela del derecho a la protección de datos adquiere especial relevancia; ello se pone de manifiesto considerando el especial valor que los datos personales –hoy y a futuro– implican en la práctica, por lo que el reconocimiento de la identidad propia de este derecho y la sensibilidad de su objeto constituye una cuestión jurídica esencial. En consecuencia, desde el Derecho de la Unión Europea se hace hincapié en garantizar su debida tutela, tal y como ilustra el vigente Reglamento General de Protección de Datos (RGPD 2016). Y, de este modo, gracias al impulso de la doctrina científica y sobre todo de la reciente jurisprudencia europea, se consolida el derecho a la protección de datos, vinculado directamente con el derecho fundamental a la intimidad, siendo así estimada la privacidad como un aspecto esencial que ha de ser preservado ante posibles amenazas o eventuales riesgos. El derecho a la protección de los datos relativos a la persona (DPD) se caracteriza, por tanto, por las propiedades de su objeto; los datos personales se configuran, así como un apreciado bien jurídico, muy sensible, y, por ende, digno de especial tutela jurídica. En este sentido, cabe afirmar que el Reglamento General europeo en materia de protección de datos (RGPD) supone un destacado hito jurídico, en tanto el Derecho de la UE se dota de un régimen común y vinculante; con la pretensión de reforzar la tutela de este derecho, y, a dicho fin, asegurar un adecuado tratamiento de los datos personales con base a la configuración de una normativa uniforme y de obligado cumplimiento. De este modo, se disciplina esta materia y su práctica, determinando un cuadro de principios y medidas concretas, que han de ser adoptadas e implementadas por todo operador o responsable de datos.

80

Por otro lado, y pese al avance regulatorio que supone el RGPD, aún quedan por resolver nuevos desafíos en esta materia. Pues, se admite que el abordar desde una perspectiva jurídica –y con eficacia– esta cuestión no es una labor sencilla, ya que en torno a la misma confluyen diversos factores, entre otros, el impacto de la comunicación digital global y asimismo los entornos tecnológicos donde se desarrollan distintas prácticas comerciales y relaciones jurídicas. Estas nuevas herramientas y ecosistemas cuya dinámica es a través de la Red o redes, es donde de forma generalizada operan distintos medios de información y de prestación de servicios. Por lo que el adoptar una normativa común en materia de protección de datos personales es clave, en nuestro tiempo, en aras de dictar una disciplina aplicable al tratamiento de datos. Conforme a dicho marco normativo, asimismo convendrá acordar medidas de actuación conjuntas con el fin de prevenir, y, en su defecto, enfrentar con éxito eventuales riesgos, que también afectarían a la seguridad del tráfico jurídico y económico, como aquellos relativos a ciberseguridad.





En suma, ante un escenario global que se advierte complejo, cabe significar la necesaria aportación que supone el RGPD, ya que determina un marco regulatorio general y común, asimismo por la innovación jurídica que implica, y por el rigor con que se establecen un conjunto de deberes específicos, exigibles a los operadores responsables en materia de tratamiento de datos; si bien, estimamos que aún resta por resolver algunos retos técnicos y jurídicos que concurren en esta materia, sobre todo en orden a observar la rápida evolución de las prácticas que se desarrollan –y de forma generalizada– vía entornos digitales globales. Por ello, se infiere que, con el fin de asegurar la eficacia de esta norma general y vinculante, resultará de igual modo clave el desarrollo normativo del mismo por parte de cada Estado miembro. Al respecto, será fundamental –a nuestro juicio– proceder a evaluar la implementación de medidas de actuación específicas, así como de disciplina y supervisión habilitadas, colaborativas y coordinadas por autoridades europeas y nacionales, amén de otras destinadas a establecer o reforzar posibles protocolos internacionales de actuación. Por cuanto, en esta temática no se puede ignorar la amplia proyección y celeridad que caracteriza a los entornos digitales globales, donde navega la información y comunicación, así como donde de forma progresiva se abren paso nuevas prácticas jurídicas (o también las denominadas fórmulas contractuales “inteligentes”). Lo cierto es que, en este contexto evolutivo, los datos personales son observados por su interés creciente, como bienes intangibles cada vez más estimados por su potencial valor, también desde un enfoque mercantil y económico.

Por ello, cabe pensar que más allá del Reglamento General de Protección de Datos (RGPD), desde la perspectiva jurídica y económica se ha de avanzar en aras de garantizar una tutela jurídica más eficiente del derecho a la protección de datos. En este sentido, en España, ha sido aprobado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos (BOE núm. 183, de 30/07/2018), y recientemente, vid., Proyecto de Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (BOCG, Senado, núm. 289, de 23 de octubre de 2018) que incorpora al Ordenamiento español al modelo establecido por el RGPD, y desarrolla materias contenidas en el mismo.

### BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AEPD (2018). “Guía del Reglamento *General* de Protección de Datos para responsables de tratamiento”. Madrid 2018. Disponible en: <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf> (Fecha última consulta: 10/06/2018).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AEPD (2018), “Aprobada la nueva Ley Orgánica de Protección de Datos”, información disponible en: <https://www.aepd.es/prensa/2018-11-23.html> (Fecha última consulta: 28/11/2018).

APARICIO SALOM, J. (2013). *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal*. Aranzadi, Navarra.

ARENAS RAMIRO, M. (2006). *El derecho fundamental a la protección de datos personales en Europa*, Tirant Lo Blanch, Valencia.

BARNÉS VÁZQUEZ, J. (1998). “El principio de proporcionalidad”, *Cuadernos de Derecho Público*, 5, Instituto Nacional de Administración Pública, Madrid.

BOE (2018). Código del Derecho al Olvido - BOE.es.

CAPODIFERRO CUBERO, D. (2017). “La libertad de información frente a Internet”, *Revista de Derecho Político*, N°.100, Monográfico con motivo del XL aniversario de la Constitución Española (I), 701-737.

82

CARRILLO LÓPEZ, M. (2003). El derecho a no ser molestado: información y vida privada. Thomson-Aranzadi, Navarra.

DI PIZZO CHIACCHIO, A. (2016). “Efectos en la jurisprudencia del Tribunal Supremo de la doctrina sentada en el caso "Google Spain": la interpretación de la responsabilidad de los gestores de motores de búsqueda en la implementación del derecho al olvido digital”, en *Revista jurídica de Catalunya*, 115,(4)939-976.

GUICHOT, E. (2005). *Datos personales y Administración Pública*. APDCM / Thomson-Civitas, Madrid, 230-233.

HERNÁNDEZ LÓPEZ, J.M. (2013). *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*. Aranzadi, Navarra.

HERRRÁN ORTIZ, A.I. (2003). “El derecho a la protección de datos en la sociedad de la información”, *Cuadernos Deusto de Derechos Humanos*, 26, Universidad de Deusto (Bilbao). Disponible en: <http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf> (Fecha consulta: 30/05/2018).

LÓPEZ PORTAS, M.B. (2015). “La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE”, *Revista UnED Facultad de Derecho*, 93. Disponible en:



<http://revistas.uned.es/index.php/derechopolitico/article/view/15140>. (Fecha consulta: 30/05/2018).

LUCAS MURILLO DE LA CUEVA, P. (2008). “El derecho a la autodeterminación informativa y la protección de datos personales”, *Azpilcueta: cuadernos de derecho*, 20. 43-58.

LUCAS MURILLO DE LA CUEVA, P. (2000). “Las vicisitudes del derecho de la protección de datos personales”, en *Revista Vasca de Administración Pública*. Vol. 2, 58, 211-242.

MARTÍNEZ MARTÍNEZ, R. (2007). “El derecho fundamental a la protección de datos: perspectivas”, Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas», *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, IDP, 5, 47-61. Disponible en: <https://dialnet.unirioja.es/download/articulo/2372613.pdf>; y <https://idp.uoc.edu/articles/10.7238/idp.v0i5.436/galley/3341/download/> (Fecha consulta: 30/05/2018).

83

NÚÑEZ LÓPEZ, M. y DEL MAR FERREIRO, M. (2013). “Una aproximación para empresas a la Ley Orgánica de Protección de Datos”, en *Derecom*, 15. Nueva Época. Septiembre-Noviembre, págs. 93-109. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=4399157> (Fecha consulta: 30/05/2018).

OLLERO TASSARA, A. (2008). *De la protección de la intimidad al poder de control sobre los datos personales. Exigencias jurídico-naturales e historicidad en la jurisprudencia constitucional*. Real Academia de Ciencias Morales y Políticas, Madrid.

ORTI VALLEJO, A. (1994). “El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)”, *Derecho Privado y Constitución*, 2. 305-332.

PIÑAR MAÑAS, J.L. (Dir.) (2016). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*. Reus, Madrid.

PIÑAR MAÑAS, J.L. (2014). “Aplicación extraterritorial de la Directiva 95/46/CE sobre protección de datos y derecho al olvido frente a los motores de búsqueda. Comentario rápido a la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, Caso GOOGLE”, en *Iuris: Actualidad y práctica del derecho*, 215, 20-23.

PIÑAR MAÑAS, J.L. (2014). “Transparencia y derecho de acceso a la información pública: algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno”, *Revista catalana de dret públic*, 49, 1-19.

PIÑAR MAÑAS, J.L. (2008). “¿Existe la privacidad?”, Universidad CEU San Pablo, Madrid 2008 (10-11 y 12). Disponible en:  
<http://dspace.ceu.es/bitstream/10637/3372/1/Lecci%C3%B3n%20Magistral%20Inaug%20curso%2008-09%20USP.pdf> (Fecha consulta: 02/06/2018).

RALLO LOMBARTE, A. (2017). “De la ‘libertad informática’ a la constitucionalización de nuevos derechos digitales (1978-2018)”, *Revista de Derecho Político*. Monográfico con motivo del XL aniversario de la Constitución Española (I). Nº.100, 639-669.

REBOLLO DELGADO, L. (2000). *El derecho fundamental a la intimidad*. Dykinson, Madrid, pp.78 y 79.

84

REBOLLO DELGADO, L. y SERRANO PÉREZ, M<sup>a</sup>. (2014). *Manual de protección de Datos*. Dikynson, Madrid 2014.

RUIZ MIGUEL, C. (1994). *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Civitas Madrid.

RUIZ MIGUEL, C. (2003). “El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea : análisis crítico”, *Revista de Derecho Comunitario Europeo*, nº 14, 7-43. Texto disponible en:  
<https://dialnet.unirioja.es/servlet/autor?codigo=176117>. (Fecha consulta: 30/05/2018).

SIMÓN CASTELLANO, P. (2012). *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch, Valencia, pp. 115 y ss.

SIMÓN CASTELLANO, P. (2012). “El encaje constitucional del derecho al olvido digital en perspectiva comparada”, en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*,. 54.

## REFERENCIAS

<sup>1</sup> Reglamento (UE) 2016/679, del Parlamento europeo y de Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre



circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE L 119/1, de 4.5.2016.

<sup>2</sup> DOCE núm. 281, de 23 de noviembre de 1995.

<sup>3</sup>Tribunal Constitucional (España). Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica. (BOE núm. 4, de 4 de enero de 2001. Sección: Suplemento del Tribunal Constitucional. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332>

<sup>4</sup> Sobre la configuración doctrinal de este derecho fundamental, véase ORTI VALLEJO, A., ORTI VALLEJO, A. (1994). “El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)”, *Derecho Privado y Constitución*, núm. 2. Enero-Abril, págs. 305-332.

<sup>5</sup> Cfr., F.J.5º, último párrafo, “Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 C.E., con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 C.E. debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 C.E.), bien regulando su ejercicio (art. 53.1 C.E.). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran”. Y, a continuación, se detalla dicha diferenciación, al señalar, “6. La función del derecho fundamental a la intimidad del art. 18.1 C.E. es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, F.J. 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, F.J. 5; 144/1999, F.J. 8; 98/2000, de 10 de abril, F.J. 5; 115/2000, de 10 de mayo, F.J. 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.” (F.J.6º, párr.1º). El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado”.

85

<sup>6</sup> PIÑAR MAÑAS, J.L. (2008). “¿Existe la privacidad?”, Universidad CEU San Pablo, Madrid 2008 (págs.10-11 y p. 12). Disponible en: <http://dspace.ceu.es/bitstream/10637/3372/1/Lecci%C3%B3n%20Magistral%20Inaug%20curso%2008-09%20USP.pdf> (Fecha consulta: 02/06/2018)

<sup>7</sup> Así concluye HERRRÁN ORTIZ, “En definitiva, el derecho a la intimidad no se asienta sobre la ocultación de determinados aspectos de la personalidad del individuo al conocimiento ajeno, sino sobre la necesidad de un ámbito de libertad interior, como instrumento imprescindible para el pleno desarrollo de la personalidad individual y como garantía de respeto a la dignidad personal”. HERRRÁN ORTIZ, A.I., “El derecho a la protección de datos en la sociedad de la información”, *Cuadernos Deusto de Derechos*

*Humanos*, nº.26, Universidad de Deusto (Bilbao), 2003 (pág.12). Disponible en: <http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf>

<sup>8</sup> Tal y como señala, REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*. Dykinson, Madrid 2000. (págs.78 y 79).

<sup>9</sup> La doctrina sobre esta cuestión y la noción de privacidad, cita STEDH de 28 de enero de 2003, asunto Peck c. Reino Unido, epígrafe/apartado 57), asimismo, en España, el Tribunal Constitucional, STC 233/2005 de 26 de septiembre (F.J.4º), ha señalado que el derecho a la intimidad de las personas garantizado por el art. 18.1 CE en cuanto derivación de la dignidad humana reconocida por el art 10.1. CE implica considerar que debe reconocerse un núcleo propio o área privativa de todo individuo que sea reservada frente a la acción o el conocimiento de los demás, lo que es necesario en nuestra cultura para asegurar una calidad mínima de la vida humana (STC70/2002, de 3 de abril, F.J. 10º, y STC 231/1988, de 2 de diciembre). PIÑAR MAÑAS, J.L., “¿Existe la privacidad?”, Universidad CEU San Pablo, Madrid 2008 (en concreto, vid., págs.6, pp.10-11 y p.12). Disponible en: <http://dspace.ceu.es/bitstream/10637/3372/1/Lecci%C3%B3n%20Magistral%20Inaug%20%20curso%2008-09%20USP.pdf>

<sup>10</sup> Sobre la noción de privacidad y DPD, vid., HERRRÁN ORTIZ, A.I., “El derecho a la protección de datos en la sociedad de la información”, *Cuadernos Deusto de Derechos Humanos*, nº.26, Universidad de Deusto (Bilbao), 2003. (vid., en concreto, págs.9 a 22). Disponible en: <http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf> (Fecha última consulta: 06/06/2018).

86

<sup>11</sup> Sobre el requisito exigido de la veracidad, es contundente nuestro Ordenamiento español al consagrar en la Constitución española el derecho fundamental a la información, cf., Artículo. 20.1.d.) del Texto Constitucional, 1978.

<sup>12</sup> Vid., referencia expresa realizada por HERRRÁN ORTIZ en este sentido, -en concreto pág. 22-, exponiendo lo relativo al propósito de la Directiva 95/46/CE, dentro del estudio que dedica a la protección de datos de carácter personal y su evolución en el Derecho comunitario europeo. HERRRÁN ORTIZ, A.I., “El derecho a la protección de datos en la sociedad de la información”, *Cuadernos Deusto de Derechos Humanos*, op. cit., págs. 22-51.

<sup>13</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (DOCE L núm. 281, de 23 de noviembre de 1995). Nota: disposición derogada por el vigente el Reglamento General de Protección de Datos (RGPD, 2016).

<sup>14</sup> REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE L 119/1, de 4.5.2016 (cfr., Artículos 94 y 99): *aplicable a partir del 25 de mayo de 2018*.

<sup>15</sup> Véase al respecto, v.gr., lo expresado en Considerando 129, “*Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento,*



*incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto (.../...)”.* (Nota: lo subrayado corresponde al autor).

<sup>16</sup> En este sentido, se ha pronunciado la jurisprudencia y de forma expresa el TEDH. Al respecto, vid., BARNÉS VÁZQUEZ, J., “El principio de proporcionalidad”, *Cuadernos de Derecho Público*, 5, Instituto Nacional de Administración Pública, Madrid, 1998.

<sup>17</sup> Al respecto, vid., in extenso, ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Tirant Lo Blanch, Valencia 2006. Y, MARTÍNEZ MARTÍNEZ, R., “El derecho fundamental a la protección de datos: perspectivas”, Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas», *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, nº IDP 5 (2007), págs.47-61. <https://dialnet.unirioja.es/descarga/articulo/2372613.pdf>

<sup>18</sup> Directiva sobre la privacidad y las comunicaciones electrónicas. (DO L 201 de 31.7.2002, p. 37). Al respecto, cfr., lo señalado por el Considerando 173 del RGPD, “*El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo (2), incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento*”.

87

<sup>19</sup> APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal*. Aranzadi, Navarra 2013. HERNÁNDEZ LÓPEZ, J.M., *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*. Aranzadi, Navarra, 2013. PIÑAR MAÑAS, J.L. (Dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*. Reus, Madrid 2016.

<sup>20</sup> Cf., Artículo 4 LOPD Calidad de los datos; y, en la actualidad, enunciados los “principios relativos al tratamiento” en el Artículo 5 del nuevo Reglamento General de Protección de Datos (RGPD). A saber, “1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida,

*destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). Y al respecto, se añade que "2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)"*

<sup>21</sup> Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014. Procedimiento/Asunto - C-131/12 - EU:C:2014:317, Google Spain y Google. Disponible en: <http://curia.europa.eu/juris/liste.jsf?num=C-131/12>

<sup>22</sup> A efectos prácticos, resulta ilustrativo consultar, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". Madrid 2018. Disponible en: <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>

<sup>23</sup> Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE L núm. 119, de 4 de mayo de 2016. Este Reglamento europeo, -como se sabe- es acto normativo vinculante y directamente aplicable, si bien, entró en vigor el 25 de mayo de 2016, y, conforme a lo previsto, su plena eficacia operará, -dos años después-, desde el 25 de mayo de 2018. Texto normativo disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES>

88

<sup>24</sup> Al respecto, vid., RALLO LOMBARTE, A., *El derecho al olvido en Internet. Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid 2014; y, SILVA DE LA PUERTA, M., "El «derecho al olvido» como aportación española y el papel de la Abogacía del Estado", *Actualidad Jurídica Uría Menéndez*, nº. 38, octubre - diciembre 2014, págs. 7-12. Disponible en: <http://www.uria.com/es/publicaciones/listado-revistas/44/numero38.html>

<sup>25</sup> GUICHOT, E., *Datos personales y Administración Pública*. APDCM / Thomson-Civitas, Madrid 2005. (pág. 230-233).

<sup>26</sup> Para mayor detalle sobre LOPD, vid., APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal*. Aranzadi, Navarra 2013. NÚÑEZ LÓPEZ, M. y DEL MAR FERREIRO, M., "Una aproximación para empresas a la Ley Orgánica de Protección de Datos", en *Derecom*, nº. 15. Nueva Época. Septiembre-Noviembre, 2013. págs.93-109. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=4399157> (Fecha consulta: 30/05/2018). REBOLLO DELGADO, L. y SERRANO PÉREZ, M<sup>a</sup>. *Manual de protección de Datos*. Dikynson, Madrid 2014.

<sup>27</sup> Cfr., AEPD: "El Tribunal de Justicia de la Unión Europea respalda las tesis de la AEPD en relación con los buscadores y el derecho al olvido en internet", Nota informativa publicada, Madrid, 13 de mayo de 2014.

<sup>28</sup> Al respecto, SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch, Valencia 2012, págs. 115 y ss. Y, del mismo autor, "El encaje constitucional del derecho al olvido digital en perspectiva comparada", en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº. 54, 2012.

<sup>29</sup> SILVA DE LA PUERTA, M., "El «derecho al olvido» como aportación española y el papel de la Abogacía del Estado", *Actualidad Jurídica Uría Menéndez*, nº. 38, octubre - diciembre 2014, págs.7-12.





<sup>30</sup> Sobre lo que existe abundante doctrina, y por ello este estudio no estima preciso extenderse en este punto, y al no ser el objeto principal del mismo, pero en todo caso si se realiza breve referencia a la doctrina sentada sobre el derecho a la información, a modo de recordatorio y en relación con esta materia. Así, cabe citar, entre otras aportaciones, Véase al respecto, LUCAS MURILLO DE LA CUEVA, P., “Las vicisitudes del derecho de la protección de datos personales”, en *Revista Vasca de Administración Pública*. Vol. 2, nº 58, 2000, pág. 211-242. Y, haciendo referencia expresa al derecho a la información frente al derecho fundamental a la protección de datos, vid., MARTÍNEZ MARTÍNEZ, R., “El derecho fundamental a la protección de datos: perspectivas”, págs.54-56, en *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, IDP, nº. 5, 2007. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/2372613.pdf>; y <https://idp.uoc.edu/articles/10.7238/idp.v0i5.436/galley/3341/download/> (Fecha consulta: 10/05/2018). Citando in extenso el trabajo de CARRILLO LÓPEZ, Marc, *El derecho a no ser molestado: información y vida privada*. Thomson-Aranzadi, Navarra 2003.

<sup>31</sup> Vid., Conclusiones presentadas por el Abogado General JÄÄSKINEN en el asunto Google Spain y Google, C-131/12, EU:C:2013:424, apartado 2.El propio Abogado General Jääskinen reconoció en sus conclusiones que el cambio tecnológico «*ha hecho surgir una serie de circunstancias sin precedentes, en las que tiene que establecerse un equilibrio entre diversos derechos fundamentales, como la libertad de expresión, el derecho a la información y la libertad de empresa, por un lado, y la protección de los datos personales y la privacidad de los par titulares, por otro.*”.

<sup>32</sup> Vid., Auto de la Audiencia Nacional de 27 de febrero de 2012, que acordó plantear esta cuestión prejudicial, y en que de forma muy expresiva dice: “*Internet traspasa fronteras y límites temporales y los buscadores potencian ese efecto, permitiendo una difusión global de esa información y facilitando su localización*”.

89

<sup>33</sup> Así se reconoce que estos nuevos escenarios plantean ´destacados retos jurídicos. Al respecto, RALLO LOMBARTE, A., “De la ‘libertad informática’ a la constitucionalización de nuevos derechos digitales (1978-2018)”, págs. 639-669; CAPODIFERRO CUBERO, Daniel, “La libertad de información frente a Internet”, págs. 701-737, ambos trabajos en *Revista de Derecho Político*, Año 2017, Nº. 100, Monográfico con motivo del XL aniversario de la Constitución Española (I).

<sup>34</sup> Vid., STC 104/1986, de 17 de julio, y en sentencias posteriores, STC 160/2003, hacen hincapié en el deber de diferenciar el derecho a la información de la libertad de expresión; la primera, hace referencia a comunicar o difundir hechos relevantes para la opinión pública o “noticiales” y exige veracidad; mientras que la segunda, supone manifestar opiniones, ideas o pensamientos.

<sup>35</sup> Al respecto, resulta de interés la lectura del Considerando 66 del mismo, dice, “*A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales*”. Y, además, se precisa en el Considerando 67, que “*Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema*”.

<sup>36</sup> La Sala de lo Civil del Tribunal Supremo, constituida en Pleno, valora el denominado “derecho al olvido” en su sentencia de 15 de octubre de 2015 (SP/SENT/827960). <https://blog.sepin.es/2015/10/derecho-olvido-tribunal-supremo-civil/> (Fecha última consulta: 8 mayo 2018). Esta resolución confirma en España los criterios que ya establecieron el TJUE y la Audiencia Nacional (vid., SAN, Sala de lo Contencioso-Administrativo, Sec. 1ª, de 29 de diciembre de 2014, Recurso 725/2010). De este modo, en esta sentencia se ofrece una valiosa ponderación entre los derechos fundamentales reconocidos y que protegen el honor y la libertad de información, por ello, se ha interpretado que con esta sentencia el TS se pronuncia sobre los límites del Derecho al olvido.

<sup>37</sup> Texto íntegro St., cfr., <http://curia.europa.eu/juris/document/document.jsf?text=&docid=194059&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=1255487>

<sup>38</sup> Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DOCE núm. 281, de 23 de noviembre de 1995.

<sup>39</sup> Por su interés, se incluye el fallo de esta Sentencia: *En virtud de todo lo expuesto, el Tribunal de Justicia (Sala Segunda) declara, “Los artículos 6, apartado 1, letra e), 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en relación con el artículo 3 de la Directiva 68/151/CEE del Consejo, de 9 de marzo de 1968, Primera Directiva tendente a coordinar, para hacerlas equivalentes, las garantías exigidas en los Estados miembros a las sociedades definidas en el segundo párrafo del artículo 58 del Tratado, para proteger los intereses de socios y terceros, en su versión modificada por la Directiva 2003/58/CE del Parlamento Europeo y del Consejo, de 15 de julio de 2003, deben interpretarse en el sentido de que, en el estado actual del Derecho de la Unión, incumbe a los Estados miembros determinar si las personas físicas a las que se refiere el artículo 2, apartado 1, letras d) y j), de esta Directiva pueden solicitar a la autoridad responsable de la llevanza del registro central, del registro mercantil o del registro de sociedades, respectivamente, que compruebe, sobre la base de una apreciación caso por caso, si está excepcionalmente justificado, por razones preponderantes y legítimas relacionadas con su situación particular, limitar, al expirar un plazo suficientemente largo tras la disolución de la empresa de que se trate, el acceso a los datos personales que les conciernen, inscritos en dicho registro, a los terceros que justifiquen un interés específico en la consulta de dichos datos”.*

