derecom

ISSN: 1988-2629. Nº. 26. Nueva Época. Marzo 2019-Septiembre 2019

Cómo citar este texto:
Pilar Dopazo Fraguío. (2019). Protección de datos y derechos digitales: arquitectura del nuevo binomio regulatorio. *Derecom*, 26, 17-48, http://www.derecom.com/derecom/

PROTECCIÓN DE DATOS Y DERECHOS DIGITALES: ARQUITECTURA DEL NUEVO BINOMIO REGULATORIO[1]

DATA PROTECTION AND DIGITAL RIGHTS: THE ARCHITECTURE OF THE NEW REGULATORY BINOMY

© Pilar Dopazo Fraguío
Universidad Complutense de Madrid (España)
mdopazo@ucm.es

Resumen

En este trabajo se exponen y analizan las principales novedades regulatorias que en materia de protección de datos ha incorporado el Reglamento General de Protección de Datos (RGPD, 2016) en vigor, -con plenos efectos desde mayo de 2018-, y, con ello, son examinados los principios rectores aplicables al tratamiento de datos. Asimismo, en España, en desarrollo y completando dicha normativa europea, -común y de carácter vinculante-, ha sido promulgada la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que ha entrado en vigor el pasado 7 de diciembre. Esta Ley incorpora a su vez un innovador catálogo de derechos digitales, lo que supone un hito jurídico, al reconocer los precitados y sentar las bases para reforzar la tutela fundamental de esta tipología específica de derechos, caracterizados por la sensibilidad identificativa de sus objetos -bienes jurídicos intangibles cada vez más apreciados-, por lo que requieren disponer de una digna protección y garantías *ad hoc.*

Summary

In this paper we present and analyze the main regulatory developments relating to data protection that have been incorporated by the General Data Protection Regulation [Spanish acronym RGPD] (2016) enacted, with full effect since May 2018, and considered a summup of the guiding principles applicable to data processing. Also, in Spain, developing and completing this European law, -binding and shared law by the 27 UE members-, there has been promulgated the Organic Law 3/2018, of December the 5th, on Personal Data Protection and Guarantee of Digital Rights. It has entered into force in December, the 7th. The latter also incorporates an innovative catalogue of digital rights which is a legal milestone, recognizing the aforementioned rights, and lays the groundwork for strengthening the fundamental protection of this specific type of rights, characterized by their sensitive identifying objects – increasingly appreciated non-tangible legal goods- that require a dignified protection and *ad hoc* guarantees.

Recibido: 10/12/2018 Revisado: 05/03/2019
Aceptado: 06/03/2019 Publicado: 15/03/2019

Palabras clave: Protección de datos. Derechos digitales. Límites al derecho de acceso a la información.

Keywords: Data protection. Digital rights. Limits on the right of access to information.

1.Introducción

En la actualidad, la protección de datos es reconocida como un derecho fundamental, y como tal precisa disponer de la necesaria tutela por parte del ordenamiento jurídico. En este sentido, el Derecho de la Unión Europea (UE) así lo ha estimado, siendo de forma expresa declarado en la Carta de los Derechos Fundamentales de la Unión Europea (artículo 8 CDFUE). Asimismo, en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE).

Con base en dicho reconocimiento, ha sido de igual modo preciso establecer un régimen regulatorio común y de carácter vinculante, aplicable en todo el ámbito europeo, asegurando, con ello, disponer de un marco jurídico básico y uniforme que, a su vez, pueda ser completado por cada Estado miembro, lo cual responde a la pretensión principal de reforzar la protección de este derecho, fijando para ello un cuadro de medidas de obligatorio cumplimiento, así como evitar que la diversidad normativa -preexistente en esta materia- pudiera impedir o mermar la efectividad de la tutela conferida a este derecho en la práctica actual (y futura o previsible).

Por ende, ha sido dictado el actual Reglamento General de Protección de Datos (en adelante, RGPD, 2016),[2] que, conforme a la finalidad precitada, actualiza la normativa en este ámbito y, además, dicta un sólido régimen jurídico cuyo contenido supera a la precedente Directiva 1995/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos.[3] Pues lo cierto es que este acto normativo no fue suficiente para la finalidad pretendida, más aun considerando la complejidad del contexto presente, donde resulta evidente que la protección de datos ha de ser incrementada, sobre todo ante los nuevos riesgos o amenazas que de forma progresiva surgen, conforme avanzan las tecnologías de la información y comunicación (TIC), así como el uso de los entornos digitales habilitados para la prestación de múltiples servicios, entre otros presupuestos y factores que ilustran el proceso de tránsito –en el que estamos incursos- hacia un nuevo paradigma económico, que se caracteriza, entre otras cuestiones, por el creciente interés con que son apreciados los datos, por su potencial valor como activo, siendo así ya estimado, de hecho, por diversos operadores y sectores.

Dicha realidad, sin duda, supone asumir con eficacia nuevos retos jurídicos; por lo que -a nuestro juicio- el regulador europeo ha de estar atento, prevenir y vigilar cómo evoluciona este progresivo cambio de modelo en la era digital, considerando sus posibles efectos. Y, en consecuencia, parece evidente que es clave afrontar con éxito dicha dinámica, para lo cual resulta esencial adoptar óptimas medidas comunes de disciplina, supervisión y control en lo relativo a esta materia (y en especial, aquellas destinadas al tratamiento y gestión responsable de datos), por su incidencia en el tráfico jurídico y económico, así como en otros órdenes sociales, culturales o educativos.

Al respecto, a modo de ejemplo, cabe observa el alto impacto producido por el uso generalizado de las (actuales) tecnologías de la información y comunicación (TIC) en distintos campos y, con ello, la aparición de nuevos fenómenos que surgen asimismo en escenarios

(virtuales) complejos donde el Derecho aún ha de afrontar importantes fenómenos. A esta realidad hay que sumar otros factores precitados, resultado de la globalización y el desarrollo del nuevo horizonte previsible hacia lo que se denomina una *economía de datos*.

A tenor de lo expuesto hay que significar la valiosa aportación que supone el RGPD 2016, en vigor, así como, en nuestro Ordenamiento nacional, la recientemente promulgada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y de Garantía de los Derechos Digitales (BOE núm. 294, de 6 de diciembre de 2018), que desarrolla, y asimismo completa, dicho Reglamento europeo. Por el interés que este innovador marco regulatorio presenta, en este trabajo se exponen y analizan sus principales aspectos y contenidos, con el propósito de aproximar el conocimiento sobre cuáles son sus innovaciones, e invitar a la reflexión acerca de esta temática y sus posibles implicaciones en la práctica, desde una perspectiva técnica y jurídica.

2. Los datos personales como derecho y bien jurídico digno de especial tutela jurídica.

Ante este mencionado proceso de cambio de paradigma económico, y su lógica proyección en la práctica jurídica -en particular, en lo relativo a las relaciones que operan en el tráfico jurídico mercantil, actual y futuro-, resulta evidente el alto valor que adquieren los datos como bien intangible, por lo que cabe inferir que la protección de este derecho precisa en el presente ser reforzada, asegurando disponer de garantías jurídicas satisfactorias a dicho fin.

Este contexto queda vinculado a los propios avances tecnológicos generados en los últimos años y promovidos por la sociedad de la información, donde se intensifica el empleo de las diversas herramientas para la comunicación electrónica, tanto en el ámbito de la información, como en otros relativos a la prestación de servicios, contratación, etc.

Ello es ilustrativo de la dinámica disruptiva que acontece, y en donde cada vez más adquieren relevancia los medios electrónicos y entornos digitales, frente a los tradicionales instrumentos o recursos de comunicación e información y, a la vez, pone de manifiesto que es necesario guiar y observar buenas prácticas o conductas responsables, por parte de agentes y operadores (privados y públicos). A dicho efecto, la regulación europea ha centrado la tutela del derecho a la protección de los datos personales entre sus prioridades normativas, lo que evidencia la significativa importancia de esta materia (en especial, en orden a las peculiares propiedades características del bien objeto de este derecho) y reconociéndolo así digno de una protección jurídica específica.

2.1. La necesaria configuración de los datos personales como *bien jurídico protegido*.

El diseño de una arquitectura legal satisfactoria al propósito mencionado, la protección de datos, conlleva integrar medidas reguladoras y autorreguladoras, dotando a éstas de fuerza preceptiva una vez han sido incorporadas a textos positivos. Este es el caso del vigente RGPD (y, en el mismo sentido, nuestra L.O. 3/2018, conforme se detalla en epígrafe ulterior), lo que, por tanto, justifica la oportuna convivencia de técnicas de regulación y autorregulación integradas o incorporadas en textos normativos vinculantes (esta formulación mixta de igual modo se observa en la última generación de distintas normativas europeas y nacionales que asimismo han sido dictadas en otros ámbitos como –por ejemplo– en materia de buenas prácticas de gobernanza, responsabilidad social corporativa y medioambiente, entre otras).

En este caso, -en lo relativo a la temática que nos ocupa en este trabajo-, cabe considerar el interés jurídico de este aspecto por cuanto -en nuestra opinión- para lograr un régimen jurídico eficaz en protección de datos es fundamental combinar sistemas técnicos y jurídicos que comprendan ambas medidas, si bien, con base en la construcción de un marco legal sólido que establezca con rigor medidas vinculantes. De este modo, así opera el actual RGPD 2016 que, aunque tenga *alma de Directiva*, es, a todos los efectos, una norma europea de directa aplicación en toda la UE y de obligado cumplimiento. Dicho rigor a la hora de ordenar o fijar una disciplina común es presupuesto esencial cuando, como éste es el supuesto, se trata de dotar de protección a un derecho fundamental, a fin de facilitarle las oportunas garantías jurídicas. Pues no cabe interpretar de otro modo la posible tutela de este tipo de derechos.

Y, por lo que respecta a la positiva integración en esta normativa de medidas autorregulatorias, resulta coherente a fin de centrarse en aspectos como son la proactividad y la corresponsabilidad requerida así con base en lo dictado por el Reglamento. En virtud del mismo, ambos enfoques son exigibles hoy, en el ámbito del tratamiento de datos, a los agentes u operadores que actúan o emplean este tipo de bien o activo, v.gr., en el ejercicio de actividades económicas, empresariales o profesionales.

Así, se estima que la incorporación en este texto normativo de tales medidas ha sido muy oportuno y nuclear, conforme a la motivación y finalidad del mismo; y ello, porque, en primer lugar, esta norma básica y general obliga al cumplimiento de unos concretos deberes, así como a la implementación de sistemas de gestión de datos eficientes que. además, resulten oportunos para asegurar el adecuado tratamiento que debe ser dispensado a los datos personales, observando su tipología y calidad. De igual modo, se hace hincapié en el deber de adoptar medidas de gestión, prevención de riesgos y de seguridad específicas en cada caso (así como informar al respecto), entre otras cuestiones que son examinadas con detalle en el epígrafe 3 de este texto. Todo ello, por ende, ha de ser relevante para trazar un régimen jurídico protector y garante del derecho a la protección de datos, tal y como muestra el RGPD.

A lo expuesto hay que añadir que, en este ámbito, la configuración legal de derechos y obligaciones se amplía, y además queda reforzada su observancia obligatoria al incluir este RGPD un régimen de supervisión por parte de las autoridades competentes (nacionales y europeas), así como un régimen sancionador *ad hoc.*

Lo indicado, sin duda, resulta muy importante con el fin de asegurar una digna protección legal a este derecho y en aras de su *sensible* objeto, reconociendo así que los datos son un bien jurídico muy específico, por la identidad de sus características (entre otras, su posible vulnerabilidad) y, como tal, parte del patrimonio privativo de cada individuo.

En este sentido, hay que recordar que el derecho a la protección de datos está vinculado directamente con el derecho fundamental a la intimidad, reconocido por nuestra Carta Magna (artículo 18 de la Constitución Española, CE 1978) junto con otros derechos asimismo fundamentales. De igual modo, llama la atención que ya en dicho año nuestro Texto Fundamental avanzara la consagración de una serie de derechos y garantías que hoy se demuestran esenciales en un Estado de Derecho. Por ello, la doctrina valora como un hito relevante lo citado .[4] Y, en concreto, haciendo referencia al contenido del artículo 18.4 CE, que determina el amparo del derecho fundamental a la protección de datos personales ante eventuales impactos informáticos o tecnológicos. En el mismo sentido, este derecho también dispone de rango constitucional en el Derecho Europeo, en virtud del precitado art. 8 CDFUE.

A su vez, en el presente, no puede ignorarse –tal y como ha sido avanzado en este trabajo-, que nos encontramos en un modelo económico globalizado, en donde los datos se configuran como un activo intangible cada vez más valorado; por lo que el Derecho ha de asegurar un óptimo marco regulatorio al respecto, cuya aplicación resulte eficaz en orden a prestar una tutela satisfactoria del derecho a la protección de datos, ofreciendo las oportunas garantías jurídicas. Por ello, la protección de datos ha de ser completada por otra parte, con el reconocimiento de los denominados *derechos digitales*, lo que así se motiva por el legislador español, en atención a que éstos se vinculan con el precitado derecho fundamental [cfr, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD y GDD].[5]

En efecto, con la promulgación de esta L.O., nuestro Ordenamiento positivo ha completado el contenido general del vigente RGPD, declarando asimismo un catálogo (básico) de *derechos digitales* con la pretensión de que puedan ser garantizados cabe estimar la reciente promulgación de la LOPD y GDD, en vigor desde el pasado 7 de diciembre de 2018, lo que sin duda supone un destacado hito. Si bien, queda pendiente observar –como es lógico- sus posibles desarrollos, y, sobre todo, será necesario esperar para poder realizar una valoración acerca de la eficacia en su aplicación.

En todo caso, en este contexto global, cabe advertir sobre la complejidad y dificultades que implican las TIC, la generación de diversos fenómenos y nuevos escenarios, a lo que sin duda el Derecho ha de saber responder (prevenir y, en su defecto, afrontar con éxito) con el fin de asegurar que los datos son protegidos protegidos con eficacia. En su defecto, los buenos propósitos del RGPD y de nuestra LOPD y GDD no resultarán efectivos en la práctica; por tanto, habrá que esperar un tiempo prudente hasta poder observar su/s posible/s desarrollos, y también para evaluar cuáles son los resultados reales de su aplicación. Y, con todo, hay que admitir que se presentan importantes desafíos desde la perspectiva técnica y jurídica; se plantean así retos estratégicos, sociales y culturales, en donde el derecho a la protección de datos se convierte en una pieza esencial, identificado por las propiedades específicas de su objeto, estimado como un bien jurídico digno de especial tutela pública. Y, como tal, se justifica el interés del Derecho Administrativo en este orden, ya que –en todo caso- era necesario y urgente dotar a este derecho y bien jurídico de una disciplina regulatoria *ad hoc,* que ofreciese las debidas garantías, y con el fin de salvaguardar tan preciado valor, siendo así también interpretado como una cuestión en interés general.

En efecto, estimamos que el tratamiento jurídico de esta materia constituye un tema de actualidad jurídica, clave y prioritario, tanto a nivel interno, como europeo y asimismo internacional. Pues hoy no cabe desconocer que además de las ventajas operativas que ofrecen las TIC e internet, también conlleva algunos problemas y eventuales riesgos, sobre todo, aquellos que afectan a la privacidad y la protección de datos. Dichas amenazas se vinculan al uso mayoritario y/o indiscriminado de la Red o redes, sin disponer de la previa formación y de los medios oportunos de asesoramiento, pero también es debido a cierta impunidad regulatoria. En consecuencia, el ordenamiento jurídico ha de reforzar la disciplina y ofrecer óptimas garantías antes de fomentar los medios electrónicos de comunicación y relación, como cabe interpretar que propicia la denominada *Administración electrónica*, así como otros proyectos que surgen en el ámbito privado y que pudieran interesar al sector público. De tal suerte, v.gr., podría acontecer al promover –en exceso- esta vía como medio idóneo para la prestación de servicios y/o desarrollo de relaciones jurídicas, con motivo de la aparición de la denominada “contratación inteligente” (o nuestras estructuras contractuales

por bloques o *blockchain),* cuando por otra parte aún queda por diseñar una arquitectura legal apropiada o eficaz a dicho fin. Por ello estimamos que lo más razonable es seguir el principio de precaución y reflexionar, preparar nuestro marco regulatorio y las oportunas medidas de supervisión, antes de alentar o propiciar cualquier aplicación o desarrollo atípico (no específicamente previsto vía norma jurídica).

Con todo, en nuestros días, es evidente la realidad de la transformación digital, y con ello, la generación de *ecosistemas digitales*, donde navegan relaciones jurídicas, información y comunicación de datos, configurándose éstos como el nuevo valor económico, o monetario;

Si bien no siempre se disponen las medidas previas necesarias con el fin de asegurar su protección y procurar un tráfico seguro, esto es, bajo la debida tutela o supervisión de las autoridades competentes. Por ende, cabe insistir en este aspecto.

2.2. Principal doctrina jurídica sobre protección de datos, intimidad y privacidad.

En el ordenamiento español, la protección de los datos de las personas físicas es un derecho fundamental protegido por el artículo 18.4 de la Constitución española (CE, 1978), dictando que *la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

El Tribunal Constitucional, en Sentencia 94/1998, de 4 de mayo, interpretó que como tal se garantiza a la persona el control sobre cualquier tipo de datos personales y sobre su uso y destino, evitando el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados. Posteriormente, completando la precitada doctrina consolidada, la Sentencia 292/2000, de 30 de noviembre, declara que se trata de un derecho autónomo e independiente, que comprende el poder de disposición y de control sobre los datos personales, y, por tanto, toda persona respecto a sus datos puede decidir acerca de su tratamiento y posible cesión a terceros, incluido el Estado. En consecuencia, el titular de los datos tiene el derecho de conocer quién dispone de los mismos, cuál es su tratamiento y finalidad, pudiendo, en su caso, oponerse a la posesión o empleo dado a los mismos.

El reconocimiento del derecho a la protección de datos (DPD) dispone hoy de base jurídica declarativa suficiente, tanto en el ámbito internacional como europeo, 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: la Resolución 45/1995 de la Asamblea General de las Naciones Unidas, versión revisada de los Principios Rectores para la Reglamentación de Ficheros Computerizados 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 1995/46, 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 CDFUE); 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).

De este modo, en el ámbito europeo, de forma progresiva, se ha procedido a consolidar positivamente 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. Pues, hasta ser adoptado el RGPD, en el Derecho europeo no se disponía de una base normativa común suficiente, ya que la precedente Directiva 1995/46/CE no resultó suficiente, siendo, con todo, su objeto principal procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión Europea (UE).

Por tanto, cabe afirmar que el vigente RGPD (2016), en vigor con plenos efectos desde mayo de 2018, 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). Ergo, 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 todo 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. Sin duda, dicha consolidación, a su vez, ha sido fruto del avance cultural, socio-económico y jurídico promovido en nuestro entorno, lo que demuestra que concurre una mayor sensibilidad hacia esta cuestión y su tratamiento jurídico.

En España, conforme ha interpretado el TC (sentencia 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.

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 los considerandos 36, 55, 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 común de la Unión, ídem de sus Estados miembros. Y, 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 tanto, en un sentido extensivo, sobre toda información relativa a su persona. Además, en esta línea conviene precisar otro aspecto relevante, como es el hecho de que el DPD queda vinculado -de forma necesaria- a la noción de *privacidad*.

La privacidad es, sin duda, un preciado 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[6] con sumo acierto. Con todo, en la actualidad, existe consenso acerca de que, en efecto, se trata de un bien 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 cuanto de 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.[7] 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.[8]

De igual forma, conviene puntualizar que la noción de privacidad es más amplia, tiene mayor alcance, y, por consiguiente, va más allá que el propio concepto de intimidad, tal y como ha declarado el Tribunal Europeo de Derechos Humanos.[9] En consecuencia, hay que diferenciar privacidad y derecho a la intimidad, admitiéndose en todo caso la concurrencia lógica de vínculos existentes entre ambas nociones. Y, 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 (derecho a la protección de datos personales); y con ello, facilitar el eficaz ejercicio del mismo, a fin de garantizar que este pueda ser alegado frente al posible empleo o difusión de datos -no autorizado- en tanto pudiera ser generador de graves perjuicios o efectos adversos para el titular de los mismos.[10]

3. Marco regulatorio general en la Unión Europea para la tutela de la protección de datos: principales aportaciones del Reglamento General de Protección de Datos (RGPD).

En los últimos años, el tratamiento de datos ha sido una cuestión principal para la Unión Europea, por su interés jurídico, y también por la incidencia que mantiene en relación con el esperado buen desarrollo del mercado. Por esta razón, era preciso diseñar una normativa que permitiera conciliar la protección de datos y el ejercicio del derecho a la libertad de información (veraz).[11]

Al respecto, se cuenta con precedentes en el Derecho comunitario, ya que el tratamiento y circulación de información relativa a datos personales fue objeto de la Directiva 1995/46/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.[12] De forma expresa el vigente RGPD, en su artículo 1.3., dice que L*a 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.

Ahora bien, ya se conoce que la realidad evoluciona más rápido que la legislación, y, así, 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 derecho fundamental a la protección de datos.
En este camino evolutivo y procurando avanzar en dicho propósito, ha sido fundamental el papel desempeñado por la doctrina jurisprudencial; por cuanto, gracias a su labor, en la actualidad, han sido incorporadas destacadas consideraciones en lo relativo al tratamiento de datos. De este modo, el artículo 4 del RGPD 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, se 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 su ejecución adecuada, vid. artículo 5, principios relativos al tratamiento, y en particular, en los artículos 6 a 11.

En suma, la precedente Directiva 1995/46 CE[13] 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 advierte sobre nuevos riesgos, por lo que ha sido preciso diseñar un régimen jurídico común más actualizado y que con rigor (efectos directos y vinculantes) lograra reforzar la tutela pública del derecho a la protección de datos.

3.1. Limitaciones.

De este modo, reconociendo que no fue suficiente con la precedente Directiva para el fin previsto propiciar un régimen armonizado, y que fuera óptimo en orden a cumplir con el objetivo común y necesario de protección, ha sido preciso dictar el nuevo Reglamento General de Protección de Datos (RGPD, 2016),[14] cuyo marco jurídico vinculante ya significa un derecho a la protección de datos (DPD) configurado con entidad propia, y, a su vez, haciendo hincapié en el deber de respetar todos los derechos fundamentales, libertades y principios reconocidos en la 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).

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 en instrumentos y medidas que se dictarán por cada Estado respetando unos criterios uniformes -conforme a lo establecido por dicho régimen jurídico-, asimismo garantizando, en todo caso, el principio de legalidad y seguridad jurídica, así como el principio de transparencia informativa.

En este aspecto insiste el RGPD, y también en relación con el régimen de control y supervisión que opere en cada Estado, así como en lo relativo a fijar vías para posibles reclamaciones y recursos, la articulación de un régimen sancionador específico, entre otras posibles herramientas que podrán ser habilitadas por cada Estado para la tutela del DPD[15] asegurando, además, que todas ellas puedan ser accesibles para el/los interesado/s, así como sus efectos o consecuencias previstas. De igual modo, se precisa que dichas restricciones han de ser motivadas, ponderando su aplicación en cada caso y exponiendo su justificación, ya que –como se sabe- en una sociedad democrática procede razonar la aplicación de cualquier limitación relativa a derechos/libertades fundamentales, observando así que sea congruente e indispensable, cumpliendo con el principio de proporcionalidad.[16]

En este contexto es evidente que aún el Derecho de la UE ha de afrontar con éxito los nuevos fenómenos que surgen en los nuevos entornos donde se opera diversos servicios, -como ya ha sido señalado en este texto-, analizando beneficios vs. amenazas, o posibles riesgos generados por el uso de herramientas telemáticas o electrónicas. En este sentido, se pronuncia el considerando 6 del RGPD.

Y, en consecuencia, 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 (conciliando derechos, bienes e intereses dignos de tutela). 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 a la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas*.

Lo expresado, en consecuencia, 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.*

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 que sí caben 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 si 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 o pensiones, entre otros. (vid., considerandos 52, 54, 55 y 56).

Por tanto, si cierto es que concurre un interés general o colectivo, éste ha de ser atendido de una forma satisfactoria 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 sumo interés tanto desde su perspectiva técnica y jurídica, como desde la cultural, social y económica. Esto no impide reconocer que precisará de los oportunos desarrollos mediante normativa interna o nacional con el fin de concretar su adecuada aplicación en determinados supuestos amén de trazar políticas públicas y actuaciones específicas.

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 expresados 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, un Reglamento europeo, por ende, de aplicación directa y vinculante en todos los Estados miembros de la UE.

A su vez, cabe significar que el actual 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, relativa al Tratamiento de

los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas.[17]

En concreto, este Reglamento ha incorporado relevantes novedades, dictando un marco regulatorio europeo común más sólido, para, así, garantizar una eficaz tutela del DPD 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 nuevo paradigma de la economía digital. Pues, con todo, no se puede ignorar que los datos personales suponen un valioso activo, detectado como tal por los principales operadores y sectores en el actual mercado global y competitivo. Por ello, ahora más que nunca -cabe inferir- el DPD ha de contar con una tutela pública reforzada, no siendo ésta una cuestión casual o de menor importancia frente a otros temas.

3.2. Arquitectura regulatoria innovadora en materia de tratamiento de datos.

El vigente Reglamento (RGPD) fija las normas específicas que podrán garantizar un alto nivel de protección de los datos de las personas físicas y, a su vez, se pretende evitar las posibles barreras que supongan obstáculos a la libre circulación de información y datos personales dentro de la UE (si bien, estimamos que, en la práctica, este objetivo conciliador entre ambas finalidades no resultará una cuestión sencilla). Al efecto, es clara la premisa de 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, evitando legislaciones dispares y/o insuficientes, y conforme a seguir unas reglas básicas uniformes y comunes, 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 así como vigilar la práctica operada por las personas físicas y jurídicas. Al respecto, cabe agregar que, en especial, han de dar buen ejemplo de cumplimiento, los principales operadores económicos, y las autoridades insistir en ello.

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 se exige a 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, a dicho fin, 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 deseables.

Promover sistemas de gestión y tratamiento de datos *corresponsables*, en donde de forma proactiva colaboren todos los actores y sectores (privados y público) implica contar con un deber de vigilancia especializada que, en efecto, supervise que se realizan buenas prácticas; y a dicho efecto, se han de habilitar recursos e implementar procedimientos de autoevaluación, de prevención de riesgos y de seguridad, además de los correspondientes de auto-evaluación y evaluación imparcial (por tercera parte independiente), acreditación y verificación. Pues no se puede ignorar la especial naturaleza que caracteriza y precisa el tratamiento de datos, en el que concurren elementos técnicos y jurídicos (entre otros posibles, así, los reputacionales), suponen consideraciones que también son estimadas, de forma

progresiva, por la actual legislación dictada en esta materia.[18] No obstante, y aunque el avance ha sido favorable, aún cabe admitir que resta por hacer en este sentido a fin de afrontar con éxito nuevos retos jurídicos.

3.2.1. Régimen jurídico aplicable.

El RGPD (2016) entró, con plenos efectos en vigor el 25 de mayo de 2018 (art. 99)[19] 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, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y, en su desarrollo, el Real Decreto 1720/2007, de 21 de diciembre. Este Reglamento 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 hace mayor hincapié en 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).

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, por lo que respecta a dos aspectos claves, a saber,

(a) el tratamiento de datos personales y
(b) la disposición o (libre) circulación de estos datos.

Y, 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 identifica 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; asimismo 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.

Y, en virtud de lo dictado, todas las entidades y profesionales que traten datos de carácter personal han de cumplir con esta nueva disciplina; lo cual, implica 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.

3.2.2. Presupuestos y principios rectores.

El régimen jurídico (general) aplicable a la PDP establece los presupuestos esenciales que han de regir el tratamiento de datos en la Unión Europea. De este modo, se establece un cuadro preceptivo de *principios de la protección de datos*,[20] que permiten concretar el DPD en la práctica de su ejercicio, así como cuáles son las facultades, obligaciones y aspectos que deben ser observados 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.

El 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, se trata de principios preceptivos, cuyo cumplimiento es obligado. Hacer hincapié en este aspecto es importante, tanto desde una perspectiva estratégica y, sobre todo a efectos de poder acreditar el óptimo cumplimiento legal (*compliance*), por parte de entidades, empresas y profesionales.

De este modo, el artículo 5 del RGPD enuncia estos seis principios, que son desarrollados con precisión en los artículos 6 a 11, siendo por tanto premisas clave del régimen vigente, y, como tales, han de ser considerados en el empleo, tratamiento y almacenamiento de datos de carácter personal.

En síntesis, estos seis principios determinan lo siguiente

(i) Los datos personales han de ser tratados de forma lícita, leal y transparente.
(ii) Los datos personales deben ser recogidos con fines concretos, explícitos y legítimos.
(iii) Los datos personales deben ser adecuados, pertinentes y limitados a la finalidad que motiva su tratamiento.
(iv) Los datos personales deben ser veraces, exactos y actualizados.
(v) 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.
(vi) Los datos personales han de ser tratados de forma que se garantice su seguridad (gestión y prevención de riesgos).

Entre este cuadro de principios declarados, cabe subrayar el contenido del *principio de finalidad*,[21] según el cual los datos han de ser recogidos para fines determinados (art.5.1.b. RGPD), y únicamente aquellos datos que fueran precisos para aquellas finalidad o efectos sobre los que se hubiera comunicado, previamente, a su titular cedente, al que asimismo se le debió informar y, además, solicitar autorización expresa para disponer de (y ceder) sus datos, debiendo hacer constar todo ello por el operador al que se han cedido dichos datos a los efectos informados. Este principio, en consecuencia, supone un presupuesto preliminar que resultará idóneo para evaluar la adecuación (o no) de cada práctica en este terreno; y, en particular, resulta importante en orden a poder valorar (o acreditar) el grado de cumplimiento que sigue cada operador u operadores obligados (entidad, empresa o profesional) conforme al vigente RGPD[22] En el mismo sentido, lo dictado por la actual Ley española 2018, LOPD y GDD, vid. Título II. Principios de protección de datos, arts. 4 a 10, y art. 11 dentro del Título III. Derechos de las personas).

3.2.3. Deberes para los operadores.

Entre las obligaciones que afectan a los sujetos u operadores responsables del tratamiento de datos (v.gr., entidades, empresas y profesionales), cabe destacar:

- La incorporación necesaria de la figura del *Delegado de Protección de Datos* (DPD). Este 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 protección de datos como en análisis de riesgos y medidas de seguridad de la información, que podrá ser personal interno o externo a la entidad.[23]

- 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).

- El tratamiento de datos personales *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 las empresas u operadores quedan obligados a solicitar dicho consentimiento y a 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.

- Son reforzados los deberes de *transparencia informativa.*

- Se establece la *obligación de notificar cualquier tipo de vulneración de los sistemas de seguridad* implementados relativos a los datos personales. Así, en el plazo máximo de 72 horas deberá ser comunicada 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.

- Revisión o re-configuración de *modelos contractuales.* Conforme dicta el 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 a lo relativo a las facultades de acceso a datos por terceros (respetando lo previsto como *contenido mínimo necesario*).

Asimismo, conviene precisar 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.

3.2.4. 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.*

Con respecto al *derecho al olvido*, hay que señalar que, 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.

Asimismo, 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 éstas 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.

3.2.5. Especial referencia a la inclusión de la doctrina del "derecho al olvido" y posibles restricciones (justificadas) al ejercicio del derecho de acceso a información pública.

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 vs. Agencia Española de Protección de Datos (AEPD).[24] 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, hoy mantiene su interés y actualidad jurídica.

Con este pronunciamiento del Alto Tribunal, concerniente a la interpretación del Derecho europeo e interno, se 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 particular, se dictan los siguientes presupuestos: (a) 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. (b) 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 cuando se realizara una actividad que se dirija a los ciudadanos de dicho Estado.[25] (c) Se reconoce el ejercicio del derecho de las personas a solicitar del motor de búsqueda que se supriman referencias a información o datos que les afecten, incluso 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. Y (d) se declara la preferencia del DPD. Ello 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 asunto, se dicta que prevalece dicho derecho fundamental sobre el mero interés económico del gestor del motor de búsqueda. Si bien, también cabe admitir como posibles excepciones, aquellos supuestos en que el interesado fuera persona de relevancia pública y/o el acceso a la información quedara justificado con base en el interés público.

En consecuencia, cada caso, en la práctica futura, supone ponderar los derechos que colisionan e intereses afectados, para evaluar cuál ha de primar, y evitando daños o perjuicios injustificados o innecesarios. Con todo, cabe concluir estimando que este pronunciamiento ha supuesto una importante aportación de la jurisprudencia europea, al consolidar la denominada doctrina del *derecho al olvido* (en la actualidad, ya integrado en el texto del vigente RGPD). Si bien, al respecto digno es recordar que, en España, ya la Agencia Española de Protección de Datos (AEPD) había defendido dicha argumentación,[26] 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 había focalizado el fundamento del derecho al olvido, que se infiere de los propios principios y valores enunciados en el artículo 10.1 de la Constitución.[27]

En suma, cabe afirmar que con esta sentencia del Tribunal de la Unión Europea (STJUE, 2014), y conforme a la Directiva 1995/46/CE, se establece 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*, lo 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 éstos pudieran afectar o producir lesión en sus derechos, sin justificación suficiente.

No obstante, hay que tener en cuenta que el derecho al olvido no supone un derecho absoluto, por cuanto 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).

Agregado a lo anterior, hay que significar que con motivo de este litigio, también se puso de manifiesto la necesidad de fijar una normativa europea común, más sólida, que resultara eficaz para asegurar la protección de datos. A su vez, 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, cuando 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.[28]

De igual modo, con esta resolución (STJUE, 2014) 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),[29] 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 servicios de forma globalizada.[30]

Con todo, esta doctrina del "derecho al olvido" ha supuesto una relevante 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.[31] Agregado a ello cabe advertir que no siempre la información divulgada es con base en fuentes de calidad, o pudiera contener sesgos o no ser veraz.[32] Por eso, esta STJUE fue determinante para estimar que era necesario fijar una regulación eficaz con el fin de tutelar el DPD en la Unión Europea; esto es, fijando un régimen jurídico que disciplinara con rigor esta materia. Y, en este sentido, esta STJUE ha sido valiosa, propiciando una doctrina jurisprudencial 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.[33]

Con posterioridad, ha sido completada esta doctrina del *derecho al olvido* (STJUE 2014), mediante otros pronunciamientos; así, cabe citar la Sentencia del Tribunal de Justicia Europeo (TJUE), Sala Segunda, de 9 de marzo de 2017, asunto C-398/15, S. Manni vs. Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce.[34] Esta STJUE 2017 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. Con todo, cabe insistir en 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).[35]

A su vez, resulta ilustrativa pues 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.

En todo caso, es importante advertir que, conforme a dicha resolución, el TJUE adopta una postura flexible que pretende ser conciliadora; al declarar, de forma expresa, que no cabe excluir la adopción de 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 (por ejemplo, supuestos suficientemente razonados que, a su vez, siendo debidamente ponderados, pudieran limitar de hecho el ejercicio del derecho de acceso a determinada información, o que establezcan posibles restricciones temporales, u otras decisiones o protocolos que pudiera habilitar cada Estado miembro al respecto). Así, cabe destacar que con base en este pronunciamiento, la decisión definitiva al respecto corresponderá, en cualquier caso, a los Estados miembros, conforme a la aplicación del artículo 14, párrafo primero, letra a), de la Directiva 1995/46 (obsérvese que esta sentencia se dicta con base en la aplicación de la normativa precedente al vigente RGPD). [36]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 datos personales.

Por tanto, corresponderá al legislador interno/nacional regular esta cuestión y establecer la previsión de posibles excepciones o limitaciones. De igual modo, 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 en motivos legítimos, estimando cada caso concreto *salvo cuando la legislación nacional disponga otra cosa*.[37]

4. Protección de datos y derechos digitales en el Derecho español (Ley Orgánica 3/2018, de 5 de diciembre).

Tal y como ordena el Reglamento general de protección de datos (RGPD, 2016), los Estados miembros disponían de dos años para proceder a la revisión de sus respectivas legislaciones en materia de protección de datos, con el fin de actualizarlas y adecuarlas así a las bases legales dictadas por este nuevo régimen jurídico europeo.

De este modo, en España, ha sido promulgada la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD y GDD). Este texto legal ha sido aprobado por nuestras Cortes Generales por unanimidad, esto es, demostrando la concurrencia de pleno consenso al respecto. Si bien, cierto es que ha sido

dictada con posterioridad al plazo de dos años precitado, que era así previsto por el Reglamento europeo (Art. 99 RGPD) para adaptar las legislaciones nacionales al RGPD, que con plenos efectos entró en vigor el 25 de mayo de 2018.

Nuestra Ley demuestra ser conforme e innovadora, pues desarrolla y complementa al RGPD. Además, como novedad, incluye -por vez primera en nuestro Ordenamiento- la declaración de una serie de derechos digitales que incorpora en el Título X *Garantía de los derechos digitales.* Ello supone, sin duda, un hito jurídico relevante que podrá servir de modelo asimismo para otros ordenamientos, ya que dicha consagración opera a modo de catálogo legal o *Carta declarativa de derechos digitales*.

La LOPD y GDD atiende así de forma positiva al contenido previsto por el Sistema Común Europeo, y, con ello, a las habilitaciones que de forma específica otorga dicho Reglamento europeo, con el propósito de regular aquellas materias previstas por el mismo. En este sentido, cabe observar como el considerando 8 permite que cada Estado miembro pueda *incorporar al Derecho nacional previsiones contenidas específicamente en el Reglamento, en la medida en que sea necesario por razones de coherencia y comprensión,* tal y como se expone y motiva en el Preámbulo de esta Ley.

Eso supone una excepcionalidad a la regla general del Derecho de la Unión Europea, por cuanto -como se sabe- los reglamentos constituyen una fuente normativa o acto normativo de carácter preceptivo y directamente aplicable, no precisando su desarrollo por parte de los derechos nacionales. No obstante, en este caso, sí se ha estimado necesario habilitar a los Estados miembros para que puedan dictar otras normas internas complementarias con el fin de asegurar la aplicación del nuevo sistema jurídico común que fija el RGPD, esto es, con plena efectividad. Al respecto, en la práctica, ya se advertía en este sentido en la STJUE 2017 precitada sobre la conveniencia de completar algunos de los contenidos del RGPD por parte de los Estados y establecer los oportunos protocolos que facilitaran la práctica de lo ordenado por dicha normativa europea (RGPD 2016) y permitieran vigilar su eficaz cumplimiento.

En nuestro país, una de las cuestiones objeto de debate previo fue la relativa a si resultaba necesario (o no) elaborar una nueva Ley orgánica, que sustituyera a la precedente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (modificada por Ley 2/2011, de 4 de marzo, de Economía Sostenible, DF. 56ª, y por 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); o bien, hubiera sido suficiente con proceder a la reforma y actualización de la misma.[38] Finalmente, la decisión ha sido configurar una ley innovadora que ha sido aprobada por unanimidad. Y dicha opción ha sido motivada por nuestro legislador, en aras de los principios de buena regulación, y al estimarse que era así lo óptimo *al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica* (cfr. Preámbulo de la Ley).

Por otra parte, hay que resaltar la nueva *Carta de derechos digitales* declarados en el Título X de esta Ley. Con esta incorporación innovadora se pretende promover que los poderes públicos implementen los oportunos desarrollos y acciones que permitan dar efectividad a este tipo de derechos de la ciudadanía en la era digital, sobre todo ante el mayoritario empleo de internet, y de forma que sea posible *y seguro* el pleno ejercicio de los derechos fundamentales en la red (o, en general, en los actuales entornos tecnológicos). Esto es, supone

una consideración jurídica que no podía ser ignorada en el presente, ya que, con esta declaración de derechos, nuestro legislador ha centrado -(y , precisamente, en relación con el derecho fundamental a la protección de datos)- lo que desde la perspectiva jurídica implica la transformación digital, y, de este modo, era necesario aportar seguridad jurídica ante la dinámica que ya opera en la práctica (v.gr., amplio uso de internet y nueva generación de relaciones sociales y jurídicas *electrónicas*). Pues, como se conoce, éste es el contexto actual donde cada vez más se opera (herramientas de comunicación, información y prestación de servicios).

En consecuencia, el Título X (artículos 79 a 97) contiene la declaración de los siguientes derechos digitales: Artículo 80. *Derecho a la neutralidad de Internet*. - Artículo 81. *Derecho de acceso universal a Internet*. - Artículo 82. *Derecho a la seguridad digital*. - Artículo 83. *Derecho a la educación digital*. - Artículo 84. *Protección de los menores en Internet*. - Artículo 85. *Derecho de rectificación en Internet*. - Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales*. - Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.* - Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.* Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.* - Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.* - Artículo 91. *Derechos digitales en la negociación colectiva.* - Artículo 92. *Protección de datos de los menores en Internet.* - Artículo 93. *Derecho al olvido en búsquedas de Internet*. Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.* - Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.* Artículo 96. *Derecho al testamento digital.* - Artículo 97. *Políticas de impulso de los derechos digitales.*

Con la incorporación de este título específico, la actual Ley española de protección de datos es pionera en el reconocimiento de esta nueva generación de derechos relativos al entorno virtual. No obstante, debe observarse que algunos de estos derechos ya constan en otras disposiciones normativas, o bien, suponen adaptaciones o reformulaciones al presente entorno digital de derechos fundamentales ya consagrados por nuestro ordenamiento. En todo caso, sí parece oportuno que en este texto vigente (2018) se haya procedido a reconocer este conjunto de derechos, ofreciendo tal formulación legal integradora o *Carta de derechos digitales específicos*, aportando así mayor seguridad jurídica.

Al respecto, se sintetizan las principales novedades que caracterizan a este catálogo declarativo de derechos, a saber,

(i) Derecho a la neutralidad de Internet (artículo 80). El principio de neutralidad determina que los paquetes de datos que ofrecen los operadores o proveedores de servicios en la Rred deben ser tratados de la misma forma, y no dar prioridad a aquellos a los que por intereses comerciales o económicos pudiera interesar dar preferencia (v.gr., vía canales más accesibles u ofrecidos a mayor velocidad que otros). Así, este precepto señala que *los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.*

(ii) Protección de los menores ante los riesgos de Internet (art. 84). Con ello, se trata de insistir en los deberes de tutela del menor que corresponden a los titulares de la patria potestad, tutores legales y análogas figuras en lo relativo al posible empleo de internet, redes y uso de instrumentos o dispositivos digitales y, en relación con asegurar la debida protección de datos personales e información relativa a menores. Por tanto, supone reforzar la diligencia

debida que ya nuestra legislación ordena en el marco del Código Civil (artículos 154 a 171), y, por otra parte, en la vigente Ley Orgánica de Protección del Menor (cfr., Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil). Por otra parte, en cuanto a la prestación del consentimiento expreso, el art. 7 LOPD y GDD señala la edad de 14 años como límite que el responsable del menor ha de observar. Además, en lo relativo a la protección de datos, de forma específica, se refiere a la protección de la imagen del menor como datos de categoría especial, y, por tanto, se exige su especial tratamiento (art. 9 LOPD y GDD). Y, por último, la Disposición Adicional 19ª de esta Ley concede al Ejecutivo el plazo de un año para elaborar un proyecto de ley que precise y desarrolle los derechos de los menores considerando eventuales impactos de la Red.

(iii) Derecho a exigir que la información publicada sea actualizada por los medios de comunicación digitales (art. 86). Cabe interpretar que este derecho amplía el ámbito del derecho de rectificación, ya declarado por la normativa precedente; pues, en la actualidad, -conforme al texto literal de este precepto-, no solo se trataría de aquélla relativa en estricto sentido a datos personales, también, por ejemplo, cualquier otra información que fuera sesgada o que precisara ser actualizada por constar editada en medios digitales, bases o registros electrónicos, *salvo en el caso de decisiones judiciales.* No obstante, al respecto, hay que tener en cuenta lo ya expuesto en este trabajo sobre la doctrina del derecho al olvido, en tanto éste no se trata de un derecho absoluto, y, por consiguiente, procederá ponderar cada caso concreto que fuera planteado, ya que ante ciertos supuestos, pudiera ser preferente el derecho fundamental a la libertad de información, o el derecho de acceso a la información y la transparencia informativa, en interés público (conforme a lo previsto por nuestro ordenamiento vigente).

(iv) Derechos digitales reconocidos en el ámbito de las relaciones laborales (o *derechos digitales laborales*). En este ámbito, son declarados varios derechos, en lo que afecta al campo de la negociación colectiva (art. 91), y, con ello, se abre la posibilidad de incluir vía convenio colectivo el reconocimiento de determinadas garantías para el trabajador; asimismo, en relación con el relativo a la desconexión digital (v.gr., cuando el empleado finalizara su jornada laboral, respetar períodos de descansos o vacaciones), todo ello conforme al modelo de contratación y calendario laboral que opere. También se hace referencia al derecho del trabajador en cuanto al posible empleo de dispositivos electrónicos y otros medios digitales, así como en lo relativo al uso de sistemas de videovigilancia y de geolocalización en el entorno laboral. Con todo ello se trata de asegurar el pleno respeto al derecho fundamental a la intimidad (cf., arts. 87, 88, 89, 90 LOPD y GDD).

(v) Derecho al olvido en servicios de redes sociales y servicios equivalentes (art. 94). Supone una concreción del derecho al olvido también en el ámbito de las redes de comunicación actuales, ampliando, por tanto, el ámbito que ya comprende dicho derecho al olvido y es aplicable a los servicios que prestan los buscadores vía internet (artículo 93). *Derecho al olvido en búsquedas de Internet*, tal y como ha sido analizado en este trabajo *(supra*). En consecuencia, la declaración de este derecho implica una modalidad extensiva, formulada sobre la base del previamente reconocido *derecho de supresión* de información o datos accesibles en internet, y que pudieran perjudicar a su titular.

(vi) Derecho de portabilidad en servicios de redes sociales y servicios equivalentes (art. 95). Con este derecho se amplía el ámbito de una facultad ya posible para servicios de telefonía móvil, y que ahora sería asimismo aplicable a contenidos que figuren en las redes

sociales, aplicaciones o herramientas análogas. Aunque la propia Ley aclara que el ejercicio de este derecho dependerá de su viabilidad técnica.

(vii) Derecho al testamento digital (art. 96). En este precepto se enumeran una serie de reglas que deberán ser observadas por los prestadores de servicios de la sociedad de la información con relación a determinados contenidos, gestionados por estos agentes acerca de personas fallecidas. En puridad, con este precepto, se trata de tutelar la identidad digital de personas fallecidas con respecto a las cuentas que pudieran disponer de correo electrónico y en redes sociales, o análogos medios (por ej., servicios de mensajería como *whatsapp* u otras aplicaciones). Y, a dicho efecto, los herederos o persona designada por el causante, podrá solicitar a los prestadores de servicios el acceso a los datos relativos al perfil y *vida digital* del mismo, y obtener la disposición sobre los contenidos de cuentas o servicios de este tipo (incluyendo, la modificación o la supresión de datos), sin necesidad de contratar con otras posibles empresas que ofrecen servicios tecnológicos, como el denominado *albacea digital*.

A su vez, hay que observar que esta Ley, en su artículo 3, regula lo relativo a los *datos de las personas fallecidas.*

Por último, la Ley dicta que el Gobierno, en colaboración con las Comunidades Autónomas, ha de elaborar un Plan de Medidas de Actuación relativo al *Acceso a Internet*, conforme a los objetivos que esta Ley detalla, con la finalidad de promover próximas *Políticas de impulso de los derechos digitales* (art. 97). Asimismo, le encomienda la aprobación de un Plan de Actuación destinado a fomentar acciones formativas/educativas y de sensibilización para que

> *los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales*.

Por otra parte, el apartado 3 de este mismo artículo señala que el Gobierno deberá elaborar el correspondiente Informe Anual acerca de la aplicación de esta Ley, que remitirá a la Comisión Parlamentaria pertinente del Congreso de los Diputados, con el fin de poder valorar la evolución de la misma y sobre las posibles medidas propuestas en materia de derechos digitales.

Corolario

La tutela del derecho a la protección de datos adquiere especial relevancia en el contexto actual y futuro de la Unión Europea, tal y como en los últimos años ya había sido advertido tanto por la doctrina científica como por la jurisprudencia. Ello ha impulsado una significativa evolución normativa en esta materia; y, en consecuencia, con el propósito de establecer un marco regulatorio básico, común y vinculante para todos los Estados miembros, se dictó el vigente Reglamento General de Protección de Datos (RGPD, 2016), cuyas principales aportaciones han sido expuestas en el presente estudio.

Al respecto, se significa que este Reglamento establece el nuevo marco regulatorio básico y común aplicable en la Unión Europea en materia de protección de datos, actualizando así el contenido de la precedente Directiva; asimismo pretende reforzar la protección otorgada

a este apreciado bien jurídico. Los datos personales son, así, dotados de una tutela específica en la era digital, ya que, además, no puede ignorarse que los datos y la información personal, en el presente (y a futuro) se configuran como valiosos activos. Por lo tanto, como tales son reconocidos, y su tratamiento ha de ser lícito y conforme al cumplimiento de determinados deberes por parte del operador u operadores. A su vez, disponer o ceder dicha tipología de datos ha de ser previamente autorizado *de forma expresa* por su titular (ya que es el único que puede decidir al respecto o acerca de su posible cesión a terceros). Todo ello, asimismo, implica el deber de facilitar la correspondiente información al titular de los datos acerca de cómo procede dicho tratamiento, finalidad para la que se solicitan los datos, así como otros aspectos tal y como ordena la legislación vigente analizada en este trabajo. En suma, haciendo especial hincapié en lo mencionado, es necesario el previo consentimiento expreso del titular de los datos (antes de cualquier empleo o tratamiento de los mismos).

De este modo, en la actualidad, en el Derecho de la Unión Europea, el derecho a la protección de datos cuenta con pleno reconocimiento, quedando ligado a la privacidad, y, en consecuencia, al propio derecho fundamental a la intimidad. De igual modo, el RGPD ha incorporado destacadas aportaciones en esta materia. Además, este Reglamento posibilita que cada Estado miembro pueda proceder a dictar aquella legislación nacional que desarrolle o complete los contenidos básicos dictados por esta normativa europea, habilitando a dicho fin a los Estados. Y ello, se considera esencial, con objeto de asegurar la plena eficacia de esta regulación, así como para que puedan ser adoptadas medidas específicas, destinadas a garantizar una eficaz protección de los datos personales.

En España, de este modo, ha sido recientemente promulgada la nueva Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (Ley 3/2018, de 5 de diciembre), en vigor desde el pasado 7 de diciembre de 2018. Esta Ley constituye un hito jurídico destacado, ya que además de desarrollar el régimen jurídico fijado por el precitado RGPD, lo complementa. Y, además, de forma específica, incorpora un Título X *Garantías de los derechos digitales*, en el que se declara un catálogo de nuevos derechos digitales, que, en todo caso, precisarán de posterior desarrollo.

No obstante, pese al avance regulatorio que supone el RGPD, y nuestra Ley 3/2018, lo cierto es que aún quedan por resolver cuestiones de interés en esta materia. Pues, abordar desde una perspectiva jurídica –y con eficacia– esta temática no es una labor sencilla, ya que en la misma confluyen diversos factores, entre otros, el amplio impacto y la rápida proyección global que muestra hoy la comunicación y, en general, los servicios digitales, todo ello a través de ágiles entornos tecnológicos, diversos productos y aplicaciones.

Aun así, cabe concluir afirmando que adoptar una normativa común europea y, en consecuencia, actualizar nuestra legislación nacional en materia de protección de datos, queda plenamente justificado en interés general o colectivo. De igual modo, se estima clave la incorporación por la Ley 3/2018 de una declaración programática o catálogo de derechos digitales. Si bien en este sentido también hay que reconocer que aún queda por concretar y desarrollar algunos de los contenidos previstos al respecto, así como implementar las oportunas medidas de actuación -conjuntas y coordinadas- para asegurar la efectiva aplicación de este texto legal.

[1] Este trabajo ha sido elaborado en el marco del proyecto de investigación titulado "El régimen jurídico-público de los drones". Ref.: DER2017-87981-P. - 2018-2020. Proyecto de I+D+i (Conv. 2017. MEIC, Programa Estatal de Investigación, Desarrollo e Innovación orientada a los Retos de la Sociedad).

[2] 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 1995/46/CE (Reglamento General de Protección de Datos). DOUE L 119/1, de 4.5.2016.

[3] DOCE núm. 281, de 23 de noviembre de 1995.

[4] Conforme señala RALLO LOMBARTE,

> *La Constitución de 1978 fue pionera en la constitucionalización de garantías frente a la revolución tecnológica emergente en la medida que la sincrética referencia del art. 18.4 CE amparó la consagración del derecho fundamental a la protección de datos personales. Pero resulta de pura justicia reconocer que el decidido impulso de este derecho fundamental ha procedido de instancias europeas hasta el punto que el art. 8 CDFUE lo elevó a rango constitucional europeo y, a partir del mismo, la Unión Europea ha optado por una inequívoca europeización del derecho de protección de datos a través de su regulación uniforme para toda la Unión europea mediante el Reglamento General de Protección de Datos*.

RALLO LOMBARTE, A. (2018). "Protección de datos y derechos digitales", en *Registradores de España* nº 84. p.16.

[5] BOE núm. 294, de 6 de diciembre de 2018.

[6] 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%20%20curso%2008-09%20USP.pdf (Fecha última consulta: 02/12/2018)

[7] Al respecto, HERRRÁN ORTIZ precisa que 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. (2003). "El derecho a la protección de datos en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, nº. 26, Universidad de Deusto (Bilbao). p.12.
Disponible en: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf

[8] En este sentido, REBOLLO DELGADO, L. (2000). *El derecho fundamental a la intimidad.* Madrid: Dykinson. p. 78 y 79.

[9] La doctrina sobre esta cuestión y la noción de privacidad, en STEDH de 28 de enero de 2003, asunto Peck vs. 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. (2008). *¿Existe la privacidad?*, Universidad CEU San Pablo, Madrid 2008 (en concreto, vid., p.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 (Fecha última consulta: 06/06/2018).

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

[11] Con respecto al 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.

[12] Vid. referencia expresa realizada por HERRRÁN ORTIZ en este sentido, -en concreto pág. 22-, exponiendo lo relativo al propósito de la Directiva 1995/46/CE, dentro del estudio que dedica a la protección de datos de carácter personal y su evolución en el Derecho Comunitario. HERRRÁN ORTIZ, A.I. (2003). "El derecho a la protección de datos en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos*, *op. cit.*, p. 22-51.

[13] Directiva 1995/46/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 Reglamento General de Protección de Datos (RGPD, 2016).

[14] Cfr. artículos 94 y 99 Reglamento (UE) 2016/679, aplicable a partir del 25 de mayo de 2018.

[15] Véase al respecto, v.gr., lo expresado en considerando 129.

[16] En este sentido, se ha pronunciado la jurisprudencia y de forma expresa el TEDH. Al respecto, vid. BARNÉS VÁZQUEZ, J. (1998). "El principio de proporcionalidad", *Cuadernos de Derecho Público*, 5, MadridD: Instituto Nacional de Administración Pública.

[17] 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.

[18] APARICIO SALOM, J. (2013). *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal.* Navarra: Aranzadi; HERNÁNDEZ LÓPEZ, J.M. (2013). *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*. Navarra: Aranzadi. PIÑAR MAÑAS, J.L. (Dir.) (2016). Reglamento General de Protección de Datos. Hacia un Nuevo Modelo Europeo de Protección de Datos. Madrid: Reus.

[19] 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 1995/46/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

[20] Cf. artículo 4 LOPD Calidad de los datos; y, en la actualidad, son 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»)*.

[21] 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

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

[23] Sobre la funcionalidad y el perfil de esta figura, vid. LOZANO, S. 2018. "El Delegado de Protección de Datos, el profesional más buscado", *Revista AENOR* nº 340, septiembre. p.24-27.

[24] Vid. RALLO LOMBARTE, A. (2014). *El derecho al olvido en Internet. Google versus España*, Madrid: Centro de Estudios Políticos y Constitucionales; y SILVA DE LA PUERTA, M. (2014)."El «derecho al olvido»

como aportación española y el papel de la Abogacía del Estado", *Actualidad Jurídica Uría Menéndez*. nº. 38. octubre – diciembre. Pp. 7-12.
Disponible en: http://www.uria.com/es/publicaciones/listado-revistas/44/numero38.html

[25] En relación con esta cuestión, vid. estudios doctrinales previos: GUICHOT, E. (2005). *Datos personales y Administración Pública*. Madrid: APDCM / Thomson-Civitas. p. 230-233.

[26] 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. Y vid. SILVA DE LA PUERTA, M. (2014). "El «derecho al olvido» como aportación española y el papel de la Abogacía del Estado", *Actualidad Jurídica Uría Menéndez*. nº. 38. octubre – diciembre, p .7-12.

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

[28] Cabe, en relación con esta cuestión, tener en cuenta la doctrina sentada asimismo sobre el derecho a la información, entre otras aportaciones, vid. 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. nº 58. P. 211-242. Y, haciendo referencia expresa al derecho a la información frente al derecho fundamental a la protección de datos, vid. MARTÍNEZ MARTÍNEZ, R. (2007). "El derecho fundamental a la protección de datos: perspectivas", p. 54-56, en *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, IDP, nº 5.
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, M. (2003). *El derecho a no ser molestado: información y vida privada*. Navarra:Thomson-Aranzadi.

[29] 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*.

[30] 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*.

[31] En consecuencia, se advierte que nos encontramos ante nuevos entornos, escenarios que aún plantean destacados retos jurídicos. Al respecto, RALLO LOMBARTE, A. (2017). "De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018)", p. 639-669; CAPODIFERRO CUBERO, D. (2017)."La libertad de información frente a Internet", p. 701-737, ambos

trabajos en *Revista de Derecho Político*. nº 100, Monográfico con motivo del XL aniversario de la Constitución Española (I).

[32] 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 "noticiables" y exige veracidad, mientras que la segunda supone manifestar opiniones, ideas o pensamientos.

[33] Al respecto, resulta de interés la lectura del considerando 66 del mismo, 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*.

[34] Texto íntegro de la sentencia, 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

[35] 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. 1.ª, 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.

[36] Directiva 1995/46/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.

[37] Resulta de interés lo dictado por el Tribunal de Justicia (Sala Segunda) cuando 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*.

[38] Al respecto, vid. opiniones ofrecidas en el número monográfico de la publicación *Registradores de España (RE)*, "Protección de datos, intimidad, libertad", RE nº 84, julio-septiembre, 2018.

Bibliografía

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, AEPD. (2018). "Guía del Reglamento General de Protección de Datos para responsables de tratamiento". Madrid.
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.* Navarra: Aranzadi.

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

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

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

CAPODIFERRO CUBERO, D. (2017). "La libertad de información frente a Internet", *Revista de Derecho Político*. nº. 100, Monográfico con motivo del XL aniversario de la Constitución Española (I), p. 701-737.

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

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*, vol. 115, nº 4, p. 939-976.

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

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

HERRRÁN ORTIZ, A.I. (2003). "El derecho a la protección de datos en la sociedad de la información", *Cuadernos Deusto de Derechos Humanos,* nº 26, Bilbao: Universidad de Deusto
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*, nº 93.
Disponible en: http://revistas.uned.es/index.php/derechopolitico/article/view/15140. (Fecha consulta: 30/05/2018).

LOZANO, S. (2018)."El Delegado de Protección de Datos, el profesional más buscado", *Revista AENOR,* nº 340, septiembre. p. 24-27.

LUCAS MURILLO DE LA CUEVA, P. (2008). "El derecho a la autodeterminación informativa y la protección de datos personales". *Azpilcueta: Cuadernos de Derecho,* nº 20, p. 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, nº 58, pág. 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, nº 5, p. 47-61.
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: 30/05/2018).

NÚÑEZ LÓPEZ, M. y FERREIRO, M. (2013). "Una aproximación para empresas a la Ley Orgánica de Protección de Datos", en *Derecom,* nº 15. Nueva Época. septiembre-noviembre, p. 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*. Madrid: Real Academia de Ciencias Morales y Políticas.

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,* nº 2. enero-abril, p. 305-332.

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

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,* nº 215, p. 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,* nº 49, p. 1-19.

PIÑAR MAÑAS, J.L. (2008). "¿Existe la privacidad?", Madrid: Universidad CEU San Pablo. (p.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 (Fecha consulta: 02/06/2018).

RALLO LOMBARTE, A. (2018). "Protección de datos y derechos digitales", en *Protección de datos, intimidad, libertad,* Registradores de España nº 84. p.16.

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, p. 639-669.

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

REBOLLO DELGADO, L. y SERRANO PÉREZ, M. (2014). *Manual de protección de datos. Madrid:* Dykinson.

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

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, p. 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.* Valencia: Tirant lo Blanch, p. 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,* nº 54.