LA PROTECCIÓN DE DATOS EN EL DERECHO EUROPEO: PRINCIPALES APORTACIONES DOCTRINALES Y MARCO REGULATORIO VIGENTE. (NOVEDADES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS)

Mª PILAR DOPAZO FRAGUÍO

Profesora de Derecho Administrativo,
Universidad Complutense de Madrid

Revista Española de Derecho Europeo 68
Octubre – Diciembre 2018
Págs. 113 – 148

RESUMEN: En este texto se examina cuál es la configuración actual del derecho a la protección de datos y su tratamiento jurídico en el Derecho de la Unión Europea, con base a la evolución normativa procurada, y en aras de reforzar la tutela de este derecho en la práctica. En especial, se pone de manifiesto la innovación jurídica que en esta materia ha supuesto el nuevo Reglamento General de Protección de Datos (RGPD), y, al respecto, se significan sus principales aportaciones. Asimismo, se analizan aquellas contribuciones más relevantes realizadas en virtud de recientes sentencias del Tribunal de Justicia de la Unión Europea (TJUE).

PALABRAS CLAVE: Reglamento General de Protección de Datos (RGPD)– Protección de Datos Personales (PDP)– Derecho al olvido– Derecho de acceso a la información

ABSTRACT: This text examines the current configuration of the right to data protection and its legal treatment in European Union Law, based on the normative evolution sought, and in order to strengthen the protection of this right in practice. In particular, it highlights the legal innovation that in this matter has meant the new General Data Protection Regulation (GDPR), and, in this respect, its main contributions are meant. In the same way, the most relevant contributions made by recent judgments of the Court of Justice of the European Union (CJEU) are analyzed.

KEYWORDS: General Data Protection Regulation (RGPD)– Protection of Personal Data (PPD)– "Right to be forgotten"– Right of access to information

Fecha de recepción: 16-7-2018
Fecha de aceptación: 24-9-2018

I. INTRODUCCIÓN Y MOTIVACIÓN DEL ESTUDIO

El presente estudio tiene como principal objeto examinar y valorar la configuración jurídica actual del derecho a la protección de datos (en adelante, DPD) en el marco del vigente Derecho de la Unión Europea. A dicho fin, se ofrece un análisis de la evolución que ha seguido la regulación comunitaria europea en materia de protección de datos, destacando sus actos normativos básicos, así como aquellos aspectos técnicos y jurídicos que caracterizan al régimen jurídico hoy aplicable en este ámbito en virtud del nuevo Reglamento General de Protección de Datos (RGPD, 2016)[1], vigente en la actualidad.

Conforme a dicha motivación, en este trabajo se analizan las principales aportaciones de este RGPD, sintetizando su contenido, finalidad y funcionalidad. Asimismo, se reflexiona sobre algunos aspectos destacados que se plantean acerca del DPD, y que conviene considerar por su proyección y actualidad jurídica; en concreto, aquellos relacionados con las nuevas implicaciones que conlleva el tratamiento de datos y los deberes que exige el cumplimiento de dicha normativa. También se observan otras cuestiones jurídicas sobre las que se reflexiona por el interés práctico que adquieren, como demuestran recientes pronunciamientos judiciales. En este sentido, cabe afirmar que la contribución de la Jurisprudencia ha sido muy importante, en aras de consolidar doctrina,

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

que hoy ya ha sido positivizada al quedar integrada en el texto del RGPD (2016), vigente en la actualidad. A dichas aportaciones nos referimos de forma expresa en este trabajo. En particular, hay que destacar recientes Sentencias del Tribunal de Justicia de la Unión Europea (TSJUE); entre otras, cabe significar, la STJUE de 13 de mayo de 2014 (TJCE 2014, 85), «asunto Google», sentando la doctrina del «derecho al olvido», así como otra sentencia posterior, STJUE de 9 de marzo de 2017 (TJCE 2017, 76), que complementa a la precitada.

Sin duda, esta temática adquiere especial relevancia en el actual Derecho de la Unión Europea (UE), y con ello, se suma valor al ya reconocido DPD como derecho fundamental, confirmándose así que su objeto supone un apreciado bien jurídico, muy sensible y, por ende, digno de especial tutela. A su vez, este derecho se vincula con otros asimismo consagrados como fundamentales por nuestro Ordenamiento, en el mismo sentido en otros países de la UE. En consecuencia, puede afirmarse que el vigente RGPD supone un destacado hito jurídico, en tanto el Derecho de la UE se dota de un régimen común y vinculante, que pretende reforzar la tutela de este derecho, y a dicho fin, asegurar un adecuado tratamiento de los datos personales con base a la configuración de una normativa uniforme y de obligado cumplimiento. De este modo, se disciplina esta materia y su práctica, determinando un cuadro de principios y medidas concretas, que han de ser adoptadas e implementadas por todo operador o responsable de datos.

Por otro lado, y pese al avance regulatorio que supone el RGPD, aún quedan por resolver nuevos desafíos en esta materia. Pues, el abordar desde una perspectiva jurídica –y con eficacia– de la protección de datos no es una labor sencilla, ya que en torno a la misma confluyen diversos factores, incluido el impacto de los avances tecnológicos empleados en comunicación y para la prestación de servicios a través de la Red, entre otros. Las implicaciones que conllevan estos últimos, por ejemplo, van más allá del ámbito de la UE, por lo que convendrá observar asimismo el contexto regulatorio internacional en lo referente a esta cuestión. Además, al respecto, es necesario considerar los nuevos riesgos que se han puesto de manifiesto, en los últimos años, como los relativos a ciberseguridad. Lo que, en efecto, agrega dificultad a la hora de abordar esta temática con éxito desde la Unión Europea.

Con todo, y a tenor de lo mencionado, en el marco de la UE ha sido preciso focalizar la regulación europea relativa a protección de datos con rigor. Y, con esta pretensión, cabe estimar la destacada aportación que supone el RGPD, junto a otra normativa europea dictada –también en 2016– y relacionada con esta materia (a la que se hace referencia en este trabajo). De este modo, hay que poner en valor esta nueva generación de normas europeas, resultando así sumamente oportuna, ya que articula las bases de una arquitectura legal común, necesaria en este ámbito y con celeridad. Dicha disciplina regulatoria ha de procurar tanto prevenir como, en su defecto, enfrentar eventuales amenazas, que pudieran afectar o vulnerar el DPD. Asimismo, admitiéndose la complejidad descrita, resultaba esencial hacer mayor hincapié en el deber de garantizar una tutela pública del DPD especializada, a cargo de autoridades europeas y nacionales, así como exigiendo la proactividad de otros sujetos públicos y privados, en especial de los operadores responsables de datos. A dicho propósito, –conforme dicta el RGPD– es preciso implementar

múltiples medidas, ya que el régimen jurídico europeo trazado supera lo previsto por la precedente Directiva 95/46/CE, actualizado sus contenidos e incorporando nuevos derechos y, sobre todo, obligaciones. Con ello, el actual RGPD 2016 predispone un régimen preceptivo, sólido y uniforme, que con rigor determina un conjunto de principios y criterios vinculantes, –derechos y deberes de obligada observancia-, con aplicación directa en todo el ámbito de la Unión Europea (con plenos efectos desde el pasado 25 de mayo de 2018).

En este contexto, por otra parte, no puede ignorarse el impacto que también en esta materia, ha supuesto la globalización económica e informativa, pues es un hecho cierto que a través de los nuevos entornos digitales o tecnológicos se facilita la comunicación y difusión de información, asimismo la prestación de servicios sin requerir la presencia de establecimientos físicos de distribución o comercialización. Pero, con ello, también surgen nuevos riesgos, que pueden afectar al DPD. Y como tales, ante estas eventualidades resulta preciso adoptar las previsiones jurídicas y gerenciales oportunas; lo que en ocasiones –como demuestra la práctica– implica adoptar medidas que trascienden del propio espacio europeo, y que además requieren posiciones consensuadas internacionales. Por tanto, el avance del Derecho de la Unión Europea en esta materia también precisa de otras acciones, observando al respecto el contexto regulatorio internacional. Y, en consecuencia, el legislador europeo habrá de insistir en adoptar las oportunas medidas colaborativas y de coordinación, con el fin para prevenir o enfrentar nuevos riesgos, como por ejemplo en lo relativo a ciberseguridad. Por cuanto, esta problemática detectada, se sabe que también tiene su causa en insuficientes o inadecuados procesos de tratamiento de datos (por falta de prevención, falta de diligencia o deficientes sistemas de seguridad, etc.), y por ello, cabe exigir hoy máxima atención en torno a estas cuestiones.

Pues, lo que sí se pone de relieve con lo mencionado, es que desde el Derecho se ha de ofrecer una respuesta (preventiva y sancionadora), eficaz y eficiente, ante determinadas conductas no responsables o prácticas ilícitas que puedan atentar o conculcar el DPD. Y ello, no es una cuestión baladí, sobre todo en atención a supuestos acontecidos, como ya ha puesto de relieve la Jurisprudencia. Al respecto, cabe advertir del impacto sobre el DPD de los actuales medios, plataformas y entornos digitales, donde de forma mayoritaria se opera a través de la Red (o redes), empleando tecnologías de la información y comunicación (TIC) que aseguran una alta proyección e inmediata difusión de la misma. Ello supone reconocer sus muchos beneficios, pero también los riesgos que puede conllevar dicho uso, si no se adoptan las medidas de precaución y gestión oportunas. En cualquier caso, siendo conscientes de la concurrencia de estos nuevos riesgos, y en tanto pueden afectar a la eficaz protección de datos que se pretende facilitar, también conviene considerar su posible efecto –asimismo pernicioso– en el desarrollo del tráfico jurídico y del mercado interior. Por ende, el Derecho de la UE, con la adopción del RGPD, pretende intensificar la disciplina aplicable, en aras de reforzar el nivel de exigencia y, con todo, el cumplimiento de deberes en lo relativo al tratamiento de datos, fijando a su vez, –en dicho Reglamento–, un régimen sancionador específico.

Si bien, y a tenor de lo expuesto en esta introducción, cumple admitir lo ya avanzado, que esta es una temática compleja de abordar desde la perspectiva técnica y jurídica,

por lo que, además de instrumentos normativos como el RGPD, también podrá ser preciso hacer mayor hincapié en programas educativos, formativos y de sensibilización destinados a la ciudadanía, empresas, profesionales y Administraciones.

Y, con todo, cabe inferir que si bien se reconoce que el DPD implica un derecho fundamental, y como tal ha de ser tutelado como merece, ofreciendo plenas garantías jurídicas a dicho efecto. También se ha de velar por acreditar conductas y prácticas adecuadas, con especial atención a los posibles escenarios o eventos adversos; esto es, las autoridades competentes, en desarrollo del vigente RGPD, han de habilitar las oportunas medidas para actuar con inmediatez y eficacia frente a aquellos supuestos u operadores que, vulnerando dicha normativa, ejerciten conductas no responsables o ilícitas (v.gr., por ser estas desleales o no conformes a Derecho), no cumplieran con sus obligaciones, y causaran de forma injustificada daños o perjuicios al afectado o titular de los datos. Todo ello, tal y como exige el nuevo RGPD.

Obsérvese, en esta cuestión, que en algunos casos, los operadores no responsables reiteran su mala praxis con base a fines comerciales o intereses económicos, ya sea de forma directa o indirecta. En otros supuestos, la posible vulneración del DPD trae causa en la falta de la debida diligencia profesional o empresarial, por lo que convendrá ponderar cada caso concreto.

En suma, hay que apreciar la relevante aportación que supone el RGPD, que ha de ser completada o desarrollada por cada Estado miembro, con el fin de asegurar su óptima aplicación. Si bien, como ya se ha señalado, esta norma es básica, de preceptivo cumplimiento y con directa aplicación en todos los países de la UE, vigente y con plenos efectos desde el pasado 25 de mayo de 2018. Dicha norma ha incorporado novedades de sumo relieve, tanto por la innovación jurídica que implican, como también por el rigor con que se establecen un conjunto de deberes exigibles en materia de tratamiento de datos. Y, conforme a este interés, en este trabajo se detallan sus principales aportaciones, asimismo se analizan las principales contribuciones que al respecto provienen de la doctrina jurídica y jurisprudencia europea.

II. LA PROTECCIÓN DE DATOS Y SU EVOLUCIÓN EN EL DERECHO COMUNITARIO EUROPEO

En la actualidad, el Reglamento General de Protección de Datos (RGPD 2016) incorpora relevantes novedades, dictando un marco regulatorio europeo común, más sólido y reforzado que el previsto por la precedente Directiva 95/46/CE[2], para garantizar con ello una eficaz tutela del DPD, y cuya preceptiva ejecución genere confianza y seguridad; lo que, por otra parte, es clave para el desarrollo del mercado interior de la UE, asimismo en pos de encaminar buenas prácticas (lícitas y respetuosas) ante el paradigma de la economía global y digital.

2. Sobre la Directiva 95/46/CE y el proceso de evolución normativa, hasta el RGPD, vid., PIÑAR MAÑAS, J.L. (Dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*. Editorial Reus, Madrid 2016. (pp. 13-14).

Pues, a su vez, no se puede ignorar que los datos personales suponen un *valioso activo económico*, identificado así por los principales operadores y sectores en un mercado altamente competitivo. Los datos de carácter personal se han constituido como un interesante activo al proyectar negocios empresariales, sobre todo para actividades de promoción, comercialización de productos y/o servicios, así como para identificar el perfil de potenciales clientes. Por ello, ahora más que nunca, –cabe inferir– el DPD ha de contar con una tutela pública reforzada. No siendo esta una cuestión casual o de menor importancia frente a otros temas.

Tal y como se ha señalado, el RGPD entró con plenos efectos en vigor el 25 de mayo del 2018 (art. 99 RGPD). Y deroga de forma expresa a la previa Directiva 95/46/CE (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, vigente hasta la fecha, ha sido la Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de carácter personal (LOPD), y en su desarrollo el Real Decreto 1720/2007, del 21 de diciembre.

Este RGPD nace con la intención del Parlamento europeo y del Consejo europeo de unificar criterios y la 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.

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

Lo mencionado, por tanto, conlleva promover modelos de tratamiento y gestión responsable de los datos personales, lo que se propugna como un deber para los operadores (entidades o empresas y profesionales) que actúen en el ámbito de la UE, asimismo es posible su exigencia a entidades internacionales interesadas o con establecimiento en la misma (físico o virtual), que prestaran 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 DPD (v.gr., establecer los oportunos desarrollos normativos y medidas de control y supervisión, así como otros instrumentos que permitan atender posibles reclamaciones o recursos, entre otros protocolos de acción).

1. ESTADO DEL ARTE Y ANÁLISIS DE LA INNOVACIÓN JURÍDICA PROCURADA (DESDE LA DIRECTIVA 95/46/CE AL RGPD 2016)

Conforme se ha señalado, hay que poner en valor el vigente RGPD, en tanto este nuevo acto normativo europeo pretende actualizar y perfeccionar la Directiva 95/46 sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos[3]. El nuevo Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016, y ha sido aplicable a partir de mayo de 2018. Pues, como se sabe al tratarse de un Reglamento, es una norma directamente aplicable en todos los Estados miembros (sin requerir para ello de normas internas de trasposición). La previsión de este período transitorio de dos años, en el que han seguido vigentes las disposiciones de la Directiva 95/46 y las correspondientes normas nacionales de desarrollo, ha tenido como fin facilitar que pudieran ir habilitándose la medidas oportunas para cumplir con el régimen previsto por el RGPD, llegada la mencionada fecha para su eficaz aplicación[4].

Lo cierto es que esta Directiva no resultó suficiente a los fines precitados, y era necesario procurar armonizar la diversidad de legislaciones existentes en los Estados miembros. A dicho fin, ha sido preciso dictar un régimen jurídico común y vinculante que discipline la protección de datos, fijando un cuadro básico de principios y medidas de obligado cumplimiento (objeto de exposición en ulterior epígrafe, destacando aquellas –a nuestro juicio– más relevantes). Y, además, en virtud del nuevo RGPD se han tenido en cuenta otros aspectos e implicaciones que la protección de datos conlleva en la práctica, pues junto a la defensa de los derechos privativos que corresponden al ciudadano, también se considera la tutela de información por su impacto en el orden económico, la defensa de la competencia y, con todo, en aras de asegurar el buen desarrollo del mercado interior. Este aspecto también se subraya en el texto del propio RGPD vigente, por cuanto, –cabe inferir–, el procurar la seguridad jurídica en el tráfico de información o datos es asimismo una cuestión que no puede ser ignorada a la hora de diseñar políticas estratégicas claves a los fines mencionados.

El RGPD, si bien contiene nociones, principios y medidas análogas a las ya previstas por la Directiva 95/46 y por las normas nacionales dictadas conforme a la misma, incorpora nuevos contenidos, derechos y deberes, entre otros aspectos (detallados en ulterior epígrafe VI de este trabajo). Y, a su vez modifica algunas cuestiones relativas al régimen precedente. En especial, actualiza el cuadro de obligaciones exigido que, en todo caso, han de ser implementadas por cada organización o entidad en atención a sus propias

3. DOCE núm. 281, de 23 de noviembre de 1995.
4. La Agencia Española de Protección de Datos (AEPD), señala que «los responsables deben ante todo asumir que la norma de referencia es el RGPD y no las normas nacionales, como venía sucediendo hasta ahora con la Directiva 95/46. No obstante, la ley que sustituirá a la actual Ley Orgánica de Protección de Datos (LOPD) sí podrá incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permite». AEPD, «Guía RGPD». Disponible en: *https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf*(Fecha última consulta: 10/07/2018).

características, actividad y riesgos. En este sentido, como innovación del RGPD, cabe destacar dos presupuestos claves para asegurar el cumplimiento efectivo de lo dictado:

i. *El principio de responsabilidad proactiva,* exige una conducta consciente, previsora y diligente por parte de la entidad u operador responsable, y respecto al tratamiento de datos personales que desarrollara. Lo que implica que el responsable del tratamiento adopte las oportunas medidas y recursos (técnicos, organizativos, formativos,...) con el fin de asegurar que el modelo o fórmulas de tratamiento es conforme con lo establecido por el RGPD. En la práctica, lo mencionado supone que las empresas y profesionales han de habilitar procesos de análisis, evaluación y acreditación (previa identificación de tipología de los datos que tratan, finalidades y operaciones o actividades que comprende dicho tratamiento). Y en congruencia con ello, han de informar sobre el sistema de tratamiento y los medios empleados, de forma que además puedan probar que las medidas adoptadas son las adecuadas ante los interesados y las autoridades de supervisión.

ii. *El enfoque de riesgo*. La gestión del riesgo es un elemento esencial en el tratamiento de datos, tal y como dicta el RGPD. Y ello con el fin de prevenir eventuales riesgos para los derechos y libertades de los ciudadanos. Además, conforme a este nuevo enfoque, esta normativa ordena una serie de medidas que sólo son exigibles cuando concurra un alto riesgo para los derechos y libertades, sin embargo que otras han de ser moduladas con base a observar tipología, grado o nivel de riesgo que implicara el (o los) tratamiento/s. Con ello, se pretende que las medidas previstas por el RGPD sean aplicadas adaptándolas a cada entidad u organización, tipo y finalidad de actividad, tipología de datos (más o menos sensibles), volumen de datos y fórmulas de tratamiento que puedan ser desarrolladas.

2. RECONOCIMIENTO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS Y PROBLEMÁTICA DE SU CONFIGURACIÓN JURÍDICA

Queda fuera de toda duda, que hoy es patente el amplio reconocimiento jurídico de que dispone el derecho a la protección de datos como derecho fundamental en el Ordenamiento de la Unión Europea (UE). En este sentido, hay que destacar lo ya declarado en el texto de la Carta de los Derechos Fundamentales de la Unión Europea (artículo 8 CDFUE)[5]. Dicha consagración, junto con su posterior tratamiento normativo, ha sido fruto del avance cultural, socioeconómico y jurídico promovido en nuestro entorno; lo que demuestra que concurre una mayor sensibilidad hacia esta cuestión y su tratamiento jurídico; estimando así que la información relativa a datos personales, *per se,* constituye un valor digno de especial protección. Y, en este sentido, la UE ha procedido a consolidar de forma positiva la regulación común en esta materia, con el propósito de armonizar la disciplina aplicable en los Estados miembros, y asimismo reforzar el deber de tutela

5. Cfr., Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), DOCE C 364/1, de 18.12.2000. *http://www.europarl.europa.eu/charter/pdf/text_es.pdf*

pública que requiere la protección de datos. Sin duda, esto ha supuesto un importante proceso de innovación jurídica, en el que ha destacado la aportación de la Jurisprudencia europea e interna, sobre todo en virtud de recientes pronunciamientos a los que en este estudio se hace expresa referencia (siendo objeto de análisis específico aquellos que –a nuestro juicio– son más significativos en esta materia).

Conforme a este proceso de evolución normativa, los datos personales adquieren hoy una consideración específica por parte del Ordenamiento vigente, identificados por su valor y funcionalidad como potenciales activos intangibles, en términos económicos, y a su vez, constituyen un bien jurídico protegido, objeto del reconocido derecho fundamental precitado. De este modo, este derecho fundamental, –entre otros, (v.gr., derecho a la intimidad)–, mantiene una singularidad propia, que lo identifica por su objeto: la información personal, y, por ende, vinculada o relativa a la privacidad del individuo. Como tal se reconoce, se trata de un bien jurídico sumamente sensible, por lo que es factible su posible vulneración mediante, –por ejemplo–, la difusión de datos no veraces, erróneos o inexactos, el uso no autorizado por terceros, etc.

Ilustra sobre el resultado de este avance jurídico, –procurado en aras de lograr un efectivo y sólido reconocimiento del DPD–, el vigente Reglamento General de Protección de Datos (precitado). Este acto normativo vinculante, responde a la necesidad detectada por el legislador europeo de ofrecer un eficaz marco común para la tutela pública de este singular derecho en el ámbito de la UE. La cuestión no es baladí, pues con ello también se trata de atender a los nuevos desafíos que plantea la dinámica informativa y de comunicación que se desarrolla en la actualidad, de forma global y generalizada por medios electrónicos y diversas redes. Por ende, era necesario actualizar la legislación europea en materia de protección de datos, determinando al efecto, un régimen jurídico básico común y preceptivo que conforme a unos criterios uniformes sea aplicable en todos los Estados miembros. Con ello, se pretende disciplinar el tráfico o circulación de información en la UE, y a su vez, mediante el RGPD, ha sido positivizada la reciente doctrina jurisprudencial del TJUE dictada en materia de protección de datos (v.gr., «derecho al olvido»), entre otras novedades incorporadas en el mismo (que se detallan con posterioridad en este trabajo).

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

De este modo, el Derecho de la Unión Europea ha identificado de forma satisfactoria el valor y la funcionalidad del DPD, observando además *el valor económico y estratégico que los datos adquieren en el tráfico jurídico y comercial;* y, por ende, la necesidad de

prevenir y afrontar con éxito los nuevos riesgos y desafíos que conlleva la circulación generalizada y accesible de información. Y, al respecto, también al ordenar esta materia y su tutela, *se trata de hacer compatible dicha protección (DPD) con el ejercicio del principio de transparencia informativa,* que de igual modo constituye un pilar que ha de ser garantizado en los Estados democráticos y de Derecho, en aras de mayor seguridad jurídica.

En este sentido, la diversidad de supuestos, situaciones y entornos añade dificultad a esta temática, y por ende, a la aplicación eficaz de toda normativa. Por lo que se infiere que se ha de ponderar cada caso planteado, observar incluso posibles supuestos extraordinarios que de forma justificada puedan implicar excepciones (v.gr., restringir el derecho de acceso a determinados datos o información pública), así como establecer medidas adecuadas con el propósito de conciliar intereses y resolver posibles conflictos. Por ejemplo, habilitar protocolos ante supuestos en que se produzca una colisión entre derechos fundamentales o intereses (privado/público), y en los que se deba proceder a tratar de equilibrar intereses privativos con otros colectivos. En su defecto, se dictaminará cuál es el preferente, v.gr., cuando existiera un interés público o colectivo que ha de primar frente a otro u otros de carácter privado.

3. RETOS JURÍDICOS ANTE LOS NUEVOS ENTORNOS Y CIBERRIESGOS (REFERENCIA A LA «DIRECTIVA SOBRE CIBERSEGURIDAD»)

A la complejidad de esta materia, añade dificultad el fenómeno de la globalización internacional que hoy caracteriza al impacto y medios empleados en la comunicación vía digital, así como el incremento de la actividad comercial prestada a través de la Red (internet) o redes y diversas plataformas tecnológicas, cuyo uso es hoy mayoritario. De este modo, a través de estas herramientas se prestan diversos servicios y se divulga información, que no siempre es veraz o actualizada. Pues, como se sabe, estas técnicas empleadas en comunicación permiten un acceso abierto y generalizado, que no siempre cuenta con un control suficiente. Por tanto, lo cierto es que en la era de la sociedad de la información digitalizada, la protección de datos adquiere un especial valor y significado[6]. Por lo que la normativa ha de ser óptima para asegurar la protección de los mismos, ofreciendo máximas garantías de tutela e implementando ágiles medidas de reacción o sanción.

En esta misma dinámica, también conviene observar el propio desarrollo de la Administración electrónica, por lo que cabe hacer hincapié en máximo rigor y prevención

6. En este sentido, la doctrina científica advierte que la mayoría de las innovaciones tecnológicas «tienen directa (las más de las veces) o indirecta relación con el tratamiento de datos de carácter personal. Ya hace años se habló de las RFID, las *cookies* o más recientemente del *cloud computing.* Hablamos ahora también de *big data,* Internet de las cosas, *wearables, bitcoin, block chain,* robótica, drones, inteligencia artificial, *gene drive technology, data driven innovation,* ciudades inteligentes… Cualquiera de estos conceptos es imposible sin el uso de datos». PIÑAR MAÑAS, J.L., «Sociedad, innovación y privacidad», *El cambio digital en la economía. Un proceso disruptivo*, Revista de economía ICE, N.º 897, Julio-Agosto 2017. pp. 67-75 (p. 70). Disponible en: *http://www.mineco.gob.es/stfls/mineco/ministerio/ficheros/libreria/ICE_897.pdf*; (fecha consulta: 15/07/2018).

de riesgos también en este ámbito, conforme a lo precitado. Pues, en este sentido, si bien hay que reconocer las muchas ventajas que ofrece Internet y el empleo de TIC (tecnologías de información y comunicación), pero también precisa prevenir y actuar con rigor desde el Derecho frente a nuevas amenazas (v.gr., ciberriesgos).

En este contexto, hay que subrayar los principales objetivos del RGPD: mejorar el nivel de protección de los datos personales de los ciudadanos en la Unión Europea, así como modernizar la normativa aplicable con el fin de adaptarla a la nueva era digital y sus tecnologías (v.gr., internet, redes sociales, nubes, etc.). Y, junto a ello, se pretende concretar el marco de responsabilidades de operadores, gestión de datos, tratamiento y almacenamiento de datos, sistemas de evaluación y medidas de prevención.

En relación con lo exigido por el RGPD, su finalidad y funcionalidad, también hay que referir otros aspectos en los que la Unión Europea hace hincapié, tal es el caso de la coordinación entre Estados miembros para la lucha contra los denominados «ciberdelitos», que a su vez precisa de la colaboración público privada. Al respecto, desde el Derecho europeo se ha dado un importante paso con la Directiva sobre seguridad de las redes y de los sistemas de información de la Unión (2016) [7], relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, también conocida como *Directiva RSI*, o, por sus siglas en inglés, *Directiva NIS (Network and Information Systems)*, y por la que los Estados miembros de la Unión Europea quedaban obligados a transponerla a sus Ordenamientos nacionales antes del 9 de mayo del 2018.

Dicha normativa implica adoptar una estrategia europea común en el ámbito de la ciberseguridad, facilitando la colaboración y coordinación de acciones conjuntas frente a posibles ataques. En este sentido, resulta clave el intercambio de información. Y, conforme a esta normativa europea, los Estados miembros deberán diseñar una estrategia nacional de seguridad e implementar medidas técnicas y recursos organizativos para prevenir, gestionar y reaccionar frente amenazas y ciberriesgos (v.gr., atentados o ataques a bases de datos, redes y sistemas de información). También se pretende que las empresas que presten servicios esenciales mejoren su capacidad de defensa para enfrentar posibles ataques informáticos[8].

En particular, estos deberes implican la responsabilidad que en materia de la seguridad ha de recaer sobre todo en aquellas entidades o empresas que gestionan

7. Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. DOUE L 194/1, de 19-7-2016.

8. Vid., sobre Directiva sobre seguridad de las redes y de los sistemas de información de la Unión, el análisis jurídico elaborado/ofrecido por LISSÉN ARBELOA, J.M., y Crespo Vitorique, I., «Publicada la directiva sobre ciberseguridad: obligaciones para los gestores de infraestructuras críticas y servicios esenciales», en *Análisis GA&P*, Julio 2016 (27/07/2016). Disponible en: *http://www.gomezacebo-pombo.com/index.php/pt/conhecimento/analises/item/2411-publicada-la-directiva-sobre-ciberseguridad-obligaciones-para-los-gestores-de-infraestructuras-criticas-y-servicios-esenciales* (Fecha última consulta: 15/07/2018).

infraestructuras críticas y servicios esenciales, como son los relativos a fuentes de suministro de energía, agua y otros recursos básicos, servicios de telecomunicaciones, redes y plataformas digitales, transporte, servicios y mercados financieros, sector sanitario, etc. Siendo cada Estado miembro el que ha de identificar cuáles son los servicios y qué sectores o empresas son fundamentales (por su actividad, servicio prestado o impacto en la sociedad o la economía). Estas entidades han de actualizar sus modelos de gestión y sistemas de prevención, implantar programas específicos para evitar riesgos y saber enfrentar ataque, minimizando riesgo y asegurando una respuesta inmediata caso de generarse posibles eventos. Y, han de comunicar cualquier incidente a las autoridades nacionales, del mismo modo, esta Directiva NIS dicta la obligación, en su caso, para dichas entidades y operadores de servicios estratégicos, de informar a los Reguladores Europeos sobre aquellas amenazas o incidentes de seguridad que fueran graves o significativos.

El establecimiento de esta estrategia nacional y europea, con base a normas comunes de ciberseguridad, unida a intensificar la acción coordinada y colaborativa entre los Estados de la UE, permitirá también a las entidades o empresas a protegerse frente ataques, además de prevenir atentados que afectaran a infraestructura básicas e interconectadas con otros países de la UE. A dicho fin, se establece un nivel de seguridad de la información y las bases de datos, lo que facilitará una ágil consulta e intercambio de información, ya que gran parte de las amenazas en ciberseguridad proceden de agentes externos, siendo así transfronterizas.

III. LA PROTECCIÓN DE DATOS Y EL EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

1. MARCO EUROPEO Y CONTEXTO INTERNACIONAL

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

Con todo, puede afirmarse con certeza que el reconocimiento del DPD dispone hoy de base jurídica declarativa suficiente, quedando consagrado como derecho fundamental, lo que ha sido fruto de un proceso evolutivo y mediante su declaración en distintos instrumentos internacionales y europeos principales, como son: Resolución 45/95 de la Asamblea General de las Naciones Unidas, versión revisada de los Principios Rectores para la Reglamentación de Ficheros Computadorizados de Datos Personales (ONU), Resolución de Naciones Unidas A/C.3/68/L.45/Rev.1 «El Derecho a la Privacidad en la Era Digital (2013); Convenio para la Protección de las Personas respecto al Tratamiento

Automatizado de Datos de Carácter Personal (Estrasburgo, 28 de enero de 1981), y a tenor de las recomendaciones de la Asamblea del Consejo de Europa, Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos; Carta de Derechos Fundamentales de la Unión Europea (artículo 8); Tratado de Funcionamiento de la Unión Europea (artículo 16 TFUE). Y, determinando el actual marco regulatorio específico aplicable en la UE, el vigente Reglamento UE 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de datos personales)».

Centrado este estudio, de forma principal, en el estudio del derecho a la protección de datos y su configuración en el marco del Derecho europeo, en primer lugar, cabe mencionar que el DPD se reconoce como un valor digno de especial protección por el precitado Artículo 8 de la Carta de los Derechos Fundamentales (2000/C 364/01), donde de forma expresa se proclama que «*Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan*»; de igual modo, dicta el Artículo 16 del Tratado de Funcionamiento de la Unión Europea (Art. 16.1 TFUE), precepto que a su vez otorga competencias normativas a la Unión Europea sobre esta materia.

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

Al respecto, también conviene advertir que el ámbito objetivo del DPD es amplio, quedando identificado como tal la información personal (objeto de tutela específica), que de igual modo integra aquellos datos sujetos a información pública; esto es, que fueran, –en principio–, de libre acceso para cualquier interesado. Ya que no por el hecho de ser «pública» dicha información (por ejemplo, vía su constancia en registro público, base de datos o análogas fuentes, o bien por otro cualquier otro medio de comunicación) dejaría de estar bajo la facultad de disposición que es reconocida al titular de dichos datos (afectado).

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

Tal es el caso, v.gr., del denominado «derecho de autodeterminación informativa», reconocido por el Tribunal Constitucional (STC 292/2000, de 30 de noviembre (RTC 2000, 292))[9], y asimismo en relación con el mismo, el derecho fundamental que ha sido acuñado como «libertad informática» (cfr., STC 254/1993, de 20 de julio (RTC 1993, 254), 94/1998, de 4 de mayo (RTC 1998, 94), y STC 202/1999, de 8 de noviembre (RTC 1999, 202))[10]; de igual modo, más recientemente, en virtud de otros pronunciamientos relevantes ha sido configurado el «derecho al olvido». En particular, esta doctrina sobre el derecho al olvido ha sido sentada por el Tribunal de Justicia de la Unión Europea (TJUE) en la Sentencia de 13 de mayo de 2014 (TJCE 2014, 85) «asunto Google», y posteriormente, también queda completada por otras, como la STJUE de 9 de marzo de 2017 (TJCE 2017, 76). En el mismo sentido, en España, STS 545/2015, de 15 de octubre de 2015 (RJ 2015, 4417), reconoce el «derecho al olvido digital», y, por otra parte, también con motivo de otros asuntos, han sido dictadas decisiones judiciales que han rechazado su aplicación en otros casos planteados (cfr., Auto TS Civil 4 abril 2018 (JUR 2018, 94850)). Todo ello, pone de relieve que el derecho al olvido, siendo así hoy doctrina consolidada, no implica reconocer que este sea un derecho absoluto, ni universal, por lo que se ha de evaluar y ponderar cada supuesto en concreto.

Esta doctrina del «derecho al olvido» por su interés y actualidad jurídica, es analizada de forma específica en este texto (vid., ulterior epígrafe V), procediendo así a ofrecer un examen acerca de dos de las sentencias europeas que estimamos destacan en esta cuestión, al perfilar la interpretación de este derecho y su delimitación, a saber, STJUE 2014 (TJCE 2014, 85) y STJUE 2017 (TJCE 2017, 76) (precitadas). En efecto, podemos hoy manifestar que estas resoluciones, sin duda alguna, han impulsado la configuración jurídica del DPD en el vigente Derecho positivo europeo. Siendo prueba de lo mencionado, el propio texto normativo del nuevo Reglamento general de protección de datos (RGPD), que ha incorporado esta doctrina, entre otras novedades, que de igual modo son expuestas –en síntesis– en este trabajo.

2. APORTACIONES DOCTRINALES DEL TRIBUNAL CONSTITUCIONAL ESPAÑOL

Completando lo señalado, y antes de analizar –de forma específica– la jurisprudencia europea precitada, es necesario hacer referencia a la doctrina del Tribunal Constitucional español dictada en relación con esta materia; por estimar que facilita conocer el

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

10. Sobre la configuración doctrinal de este derecho fundamental, véase ORTI VALLEJO, A., «El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio (RTC 1993, 254))», *Derecho Privado y Constitución,* núm. 2. Enero-Abril, 1994, pp. 305-332.

ámbito del DPD, cómo se interpreta y cuál ha sido su proyección jurídica. De este modo, en nuestro Ordenamiento cabe significar la STC 292/2000 (RTC 2000, 292), en la que se expone con suma claridad el contenido y la delimitación del «derecho a la protección de datos», y, además, detalla su diferenciación con respecto al «derecho a la intimidad» del Artículo 18.1 Constitución Española (vid., F.J. 5.º y 6.º)[11]. Asimismo, en esta sentencia, el TC señala que si bien ambos derechos son fundamentales, hay que admitir *la propia singularidad del derecho a la protección de datos* frente a aquel; y ello, porque el objeto del DPD es más amplio que el del derecho a la intimidad. De este modo, se razona lo expuesto, «(...) *ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el* art. 18.1 *C.E., sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal* (STC 170/1987, de 30 de octubre (RTC 1987, 170), F.J. 4), *como el derecho al honor, citado expresamente en el* art. 18.4 *C.E., e igualmente, en expresión bien amplia del propio* art. 18.4 *C.E., al pleno ejercicio de los derechos de la persona*».

11. Cfr., F.J.5.º, último párrafo, « *Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del* art. 18.1 C.E., *con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al* art. 18.4 *C.E. debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos* (art. 18.1 *C.E.), bien regulando su ejercicio* (art. 53.1 *C.E.). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran».*

Y, a continuación, se detalla dicha diferenciación, al señalar, *«6. La función del derecho fundamental a la intimidad del* art. 18.1 *C.E. es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas* STC 144/1999, de 22 de julio (RTC 1999, 144*), F.J. 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal* (SSTC 134/1999, de 15 de julio (RTC 1999, 134*), F.J. 5; 144/1999 (RTC 1999, 144), F.J. 8; 98/2000, de 10 de abril (RTC 2000, 98), F.J. 5; 115/2000, de 5 de mayo (RTC 2000, 115), F.J. 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.*» (F.J.6.º, párr. 1.º). *El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado».*

Sentada esta doctrina, sin embargo, lo cierto es que abordar esta temática del DPD en la práctica, exige un análisis ponderado en cada caso, y, además, es preciso hacer hincapié en la evaluación de algunos aspectos relativos a su ámbito de ejercicio y limitaciones, entre otros. De forma específica, por ejemplo, convendrá examinar la delimitación del «derecho al olvido» en determinados supuestos, en los que el ejercicio de esta facultad puede colisionar con otros derechos fundamentales, o principios reconocidos por el Ordenamiento, sobre todo en atención a observar si concurre o ha de primar el interés público (v.gr., transparencia, publicidad registral, etc.), frente al interés privado que pudiera alegarse por el titular de datos afectado.

3. NOCIONES JURÍDICAS BÁSICAS: DATOS PERSONALES, INTIMIDAD Y PRIVACIDAD

En España, conforme ha sido expuesto (STC precitada), el objeto del derecho fundamental a la protección de datos no sólo se refiere a los datos íntimos de la persona, sino «*a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales*», por lo que el ámbito digno de protección aquí no es sólo la intimidad individual, –ya dotada de tutela por el art. 18.1 CE–, sino que de forma específica son los datos de carácter personal. Y como tales, también lo son aquellos datos personales públicos, «accesibles al conocimiento de cualquiera», y que no por ello han de quedar fuera del poder de disposición del afectado (STC 292/2000 (RTC 2000, 292), F.J.6.º, párrafos 2.º 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 Considerandos 55, 36, 73 y 154 RGPD (actividades electorales, acceso del público a documentos oficiales, información en registros públicos, entre otros supuestos posibles). Esto es, en atención a objetivos importantes de interés público general de la Unión o de un Estado miembro.

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

La *privacidad* es, sin duda, un apreciado valor intangible, consustancial a la personalidad humana y factor determinante de una adecuada calidad de vida. Por ello, hoy adquiere una identidad jurídica propia, y así se configura como un bien jurídico digno de especial protección, por ser sumamente sensible a impactos externos adversos (que la perturben o vulneren). Por tanto, este concepto jurídico «de nueva generación» ligado al reconocimiento de los derechos de la personalidad y a la dignidad humana, se añade como un aspecto más que cabe estimar y observar por su directa relación con el DPD. En

este sentido, también se ha pronunciado la doctrina (PIÑAR MAÑAS, 2008 y 2017)[12]. Con todo, en la actualidad, existe consenso acerca de que, en efecto, se trata de un bien sensible que precisa del máximo grado de tutela jurídica pública, al ser consustancial a la dignidad humana, y como tal constituye un presupuesto esencial ligado al derecho fundamental a la intimidad.

A su vez, cabe recordar que el *derecho a la intimidad*, expresamente consagrado junto con el derecho al honor y a la propia imagen por la Constitución Española (Artículo 18 CE, 1978), se asienta en la necesidad de disponer por toda persona de una esfera interior protegida frente a posibles injerencias externas; esto es, no se trata tanto de un derecho a ocultar aspectos personales, sino más bien un deber de respeto hacia un ámbito de libertad individual que es esencial para el pleno desarrollo de la personalidad y para garantizar la dignidad humana (HERRÁN ORTIZ, 2003)[13]. 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[14].

Ahora bien, mencionado lo anterior, conviene puntualizar que la noción de privacidad es más amplia, tiene mayor alcance, y, por ende, va más allá que el propio concepto de intimidad, tal y como ha declarado el Tribunal Europeo de Derechos Humanos[15]. En consecuencia, hay que diferenciar privacidad y derecho a la intimidad, admitiéndose en todo caso la concurrencia lógica de los vínculos existentes entre ambas nociones. Y, por

12. PIÑAR MAÑAS, J.L., *«¿Existe la privacidad?»,* Universidad CEU San Pablo, Madrid 2008 (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 consulta: 02/06/2018). Asimismo, este autor se pronuncia sobre el valor del derecho a la privacidad en la era digital, en el estudio elaborado titulado «Sociedad, innovación y privacidad», *El cambio digital en la economía. Un proceso disruptivo*, op. cit., en concreto, pp. 70-73.
13. Así concluye HERRÁN ORTIZ, «En definitiva, el derecho a la intimidad no se asienta sobre la ocultación de determinados aspectos de la personalidad del individuo al conocimiento ajeno, sino sobre la necesidad de un ámbito de libertad interior, como instrumento imprescindible para el pleno desarrollo de la personalidad individual y como garantía de respeto a la dignidad personal». HERRÁN ORTIZ, A.I., «El derecho a la protección de datos en la sociedad de la información», *Cuadernos Deusto de Derechos Humanos*– Universidad de Deusto (Bilbao), n.º 26, 2003 (p. 12). Disponible en: *http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf* (Fecha consulta: 30/06/2018).
14. Tal y como señala, REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*. Dykinson, Madrid 2000. (pp. 78 y 79).
15. La doctrina sobre esta cuestión y la noción de privacidad, cita STEDH de 28 de enero de 2003 (JUR 2003, 50030), asunto Peck c. Reino Unido, epígrafe/apartado 57), asimismo, en España, el Tribunal Constitucional, STC 233/2005 de 26 de septiembre (RTC 2005, 233) (F.J.4.º), 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 (STC 70/2002, de 3 de abril (RTC 2002, 70), F.J. 10.º, y STC 231/1988, de 2 de diciembre (RTC 1988, 231)). PIÑAR MAÑAS, J.L., *«¿Existe la privacidad?»,* op. cit., p. 6.

ende, el fundamento de la privacidad, en concreto, se ubica en el respeto a la intimidad y dignidad humana; 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 DPD, objeto principal de este estudio. Esto es, la privacidad opera como presupuesto que posibilita materializar la propia singularidad del DPD; y con ello, facilita el eficaz ejercicio del DPD, a fin de garantizar que este pueda ser alegado frente al posible empleo o difusión de datos –no autorizado– que generador de graves perjuicios o efectos adversos para el titular de los mismos[16].

IV. RÉGIMEN APLICABLE AL TRATAMIENTO DE DATOS PERSONALES

De forma específica, en lo relativo al tratamiento de datos, hay que destacar que en el ámbito del Derecho comunitario europeo ha sido un aspecto al que se ha prestado especial atención, diseñando así una normativa que permitiera conciliar la protección de datos con la dinámica que, por otra parte, supone el derecho a la libertad de información (veraz)[17]. En este sentido, el régimen en materia de tratamiento y circulación de información relativa a datos personales fue previsto por la Directiva 95/46/CE (cf., artículo 1.2), señalando que la libre circulación de datos entre los Estados no debía ser prohibida o afectada por restricciones –en principio-, por lo que ha de resultar compatible con la pretendida protección de datos.

Y, en la actualidad, de forma expresa, el vigente RGPD, en su artículo 1.3, dice, «*La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales*». De este modo, en este tiempo, ha sido preciso instaurar un régimen jurídico europeo más completo y eficiente en aras de asegurar el valor y la debida tutela del DPD.

En este camino evolutivo –y a fin de avanzar en esta cuestión– ha sido fundamental el papel desempeñado por la doctrina jurisprudencial, y, en la actualidad, queda previsto el texto actual del RGPD. Cuyo artículo 4 define «tratamiento»: «*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*»; y, además, precisa la noción de «limitación del tratamiento»: «*el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro*»; y, a continuación, establece los Principios aplicables

16. Sobre la noción de privacidad y DPD, vid., HERRÁN ORTIZ, A.I., «El derecho a la protección de datos en la sociedad de la información», op. cit., pp. 9 a 22.
17. Sobre el requisito exigido de la veracidad, es contundente nuestro Ordenamiento español al consagrar en la Constitución española el derecho fundamental a la información, cf., Artículo 20.1.d) del Texto Constitucional, 1978.

para proceder a la ejecución adecuada, artículo 5, «Principios relativos al tratamiento», y en los artículos 6 a 11, desarrolla cada uno de los mismos).

1. NOCIÓN JURÍDICA DE TRATAMIENTO DE DATOS

Hay que recordar que la Directiva 95/46/CE[18] 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 (como ha sido señalado en el epígrafe II.3.), por lo que ha sido preciso diseñar un régimen jurídico, más actualizado, y que con rigor (efectos directos y vinculantes) reforzara la tutela pública del DPD en la Unión Europea.

De este modo, adoptado el RGPD 2016, cuyo marco jurídico vinculante ha permitido significar el valor del DPD y el objeto del mismo, que a su vez conlleva el deber de respetar todos los derechos fundamentales, libertades y principios reconocidos en la precitada Carta de Derechos Fundamentales, conforme asimismo declaran los Tratados. Así, el RGPD subraya, «*en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información (...)*». Y, a su vez, se señala la posible delimitación del derecho a la protección de datos, por cuanto este DPD no es un derecho absoluto; ergo, en su consideración y aplicación ha de proceder en equilibrio con otros derechos fundamentales, esto es, en atención al *principio de proporcionalidad* (Considerando 4).

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

En este aspecto insiste el Reglamento, también en relación con el régimen de control y supervisión que opere en cada Estado, vías para reclamaciones y recursos, y régimen sancionador, entre otras posibles herramientas que habilitara cada Estado para la tutela del derecho a la protección de datos[19]; asegurando que todas ellas puedan ser accesibles

18. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. (DOCE L núm. 281, de 23 de noviembre de 1995). Nota: disposición derogada por el vigente el Reglamento General de Protección de Datos (RGPD, 2016).
19. Véase al respecto, v.gr., lo expresado en Considerando 129, «*Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos (…)*».

para el interesado/s, así como sobre el conocimiento sobre sus posibles efectos o consecuencias previstas. De igual modo, se indica que dichas restricciones han de ser motivadas, ponderando su aplicación en cada caso y su justificación; ya que en una sociedad democrática se ha de asegurar que cualquier eventual limitación relativa a derechos/libertades fundamentales ha de ser razonada, congruente e indispensable, cumpliendo con el principio de proporcionalidad[20].

2. SIGNIFICACIÓN DE LA PROTECCIÓN DE DATOS EN EL ORDENAMIENTO ACTUAL

Expuesto lo previo, cumple afirmar que la configuración actual del DPD como derecho fundamental, –asimismo reconocido por su objeto como bien jurídico digno de una especial protección por parte del Ordenamiento europeo e interno (o nacional), ha sido fruto de una positiva evolución de la arquitectura legal europea, en gran medida impulsada por la reciente doctrina jurisprudencial y científica, como ya se ha expresado. A su vez, se admite la complejidad de esta materia, como viene demostrando la práctica jurídica en este campo, sobre todo ante los desafíos que plantean los actuales (y futuros) entornos tecnológicos globales, donde de forma generalizada opera la comunicación y dinámica informativa, tal y como ha sido expuesto.

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

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 (de ello, se infiere que sí cabe la aplicación de posibles excepciones al régimen general previsto por el vigente RGPD). En este sentido, se señala que cuando exista un interés público»deben» autorizarse excepciones a la prohibición de tratar ciertas categorías especiales de datos personales cuando así lo determinara el Derecho de la Unión o de los

20. En este sentido, se ha pronunciado la jurisprudencia y de forma expresa el TEDH. Al respecto, vid., BARNÉS VÁZQUEZ, J., «El principio de proporcionalidad», *Cuadernos de Derecho Público*, 5, Instituto Nacional de Administración Pública, Madrid, 1998.

Estados miembros, «siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales»; por ejemplo, por razones de seguridad, supervisión, investigación de infracciones o delitos, salud pública, y también en el ámbito de la legislación laboral, protección social, pensiones, entre otros. (vid., Considerandos 52, 54, 55 y 56).

En consecuencia, si concurre un interés general o colectivo 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 de este nuevo régimen general en materia de protección y tratamiento resulta de interés tanto desde su perspectiva técnica y jurídica, como cultural, social y económica. Lo que, por otra parte, no impide reconocer que precisará de los oportunos desarrollos mediante normativa interna o nacional con de fin de concretar su adecuada aplicación en determinados supuestos.

En este sentido, también el propio texto del RGPD reconoce la importancia de lo mencionado, al admitir e identificar con certeza que «La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales» (Considerando 6). Y, en consecuencia, se advierte que «*Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas*» (Considerando 7).

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

A su vez, el RGPD supone revisar y actualizar otras normativas europeas dictadas en tanto establecían directrices acerca del régimen aplicable a determinadas tipologías de tratamiento, este es el caso en particular de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[21].

Y, de este modo, en este escenario jurídico y estratégico, el vigente Reglamento (RGPD) fija las normas uniformes y específicas que podrán garantizar un alto nivel de protección de los datos de las personas físicas y, a su vez, evitar las posibles barreras que obstaculizasen la circulación de información y datos personales dentro de la UE. Al efecto, resulta claro que el grado de protección brindado a los derechos y libertades de las personas en lo relativo al tratamiento de sus datos ha de ser el mismo en todos los Ordenamientos nacionales; esto es, conforme a unas reglas básicas comunes y sin que

21. 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.

existan discrepancias entre las legislaciones de los Estados miembros. Y, en todo caso, el RGPD hace especial hincapié en una premisa que ha de resultar clave en esta disciplina: las personas físicas deben tener el control de sus propios datos personales, para lo cual debe ser reforzada la seguridad jurídica y la práctica operada por las personas físicas, los operadores económicos y las autoridades públicas. Lo expresado, por tanto, conlleva promover modelos de tratamiento y gestión responsable de los datos personales, lo que se propugna como un deber para los operadores que actúen en el ámbito de la UE, asimismo podrá ser para entidades internacionales interesadas o con establecimiento en la misma (físico o virtual), que prestaran 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 DPD (v.gr., establecer los oportunos desarrollos normativos y medidas de control y supervisión, así como otros instrumentos que permitan atender posibles reclamaciones o recursos, entre otros protocolos de acción).

Sin duda, con ello se trata de promover sistemas de gestión y tratamiento de datos «co-responsables», en donde de forma proactiva colaboren todos los actores y sectores (privados y público); lo que, en efecto, implicará vigilar buenas prácticas, implementar procedimientos de autoevaluación, de prevención de riesgos y de seguridad, además de los correspondientes de evaluación (por tercera parte independiente), acreditación y verificación. Pues, no se puede ignorar la especial naturaleza que caracteriza y es precisa el tratamiento de datos, en el que concurren elementos técnicos y jurídicos, (entre otros posibles, como los reputacionales), como ya ha sido puesto de relieve por la doctrina científica y por la propia jurisprudencia, asimismo estas consideraciones han sido estimadas, de forma progresiva, por la legislación dictada en esta materia[22]. No obstante, y aunque el avance ha sido favorable, aún cabe admitir que resta por hacer en este sentido a fin de enfrentar con éxito nuevos retos jurídicos.

V. DOCTRINA EUROPEA SOBRE «EL DERECHO AL OLVIDO» (STJUE DE 13 DE MAYO DE 2014 (TJCE 2014, 85))

El 13 de mayo de 2014 la Gran Sala del Tribunal de Justicia de la Unión Europea dictó Sentencia en el asunto *Google Spain S.L c. Agencia Española de Protección de Datos* (AEPD) (TJCE 2014, 85)[23], con este pronunciamiento se responde a la cuestión preju-

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

23. Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014 (TJCE 2014, 85). 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*. Al respecto, vid., RALLO Lombarte, A., *El derecho al olvido en Internet. Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid 2014; y, SILVA DE LA PUERTA, M., «El "derecho al olvido" como aportación española y el papel de la Abogacía del Estado», *Actualidad Jurídica Uría Menéndez*, n.º 38, octubre – diciembre

dicial 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[24]». Siendo este asunto de gran repercusión en los medios de comunicación europeos e internacionales, hoy mantiene su interés y actualidad jurídica.

1. LAS PREMISAS DEL «DERECHO AL OLVIDO»

Con este pronunciamiento del Alto Tribunal, concerniente a la interpretación del Derecho europeo e interno (en España, LOPD conforme a la Directiva 95/46/CE)[25], concreta de forma definitiva las responsabilidades de los buscadores de internet en relación con la protección de los datos personales, y asimismo otorga tutela ante la situación de indefensión generada, en este asunto, al no haber admitido la compañía Google que le era aplicable la normativa española y europea reguladora de la materia.

En esta sentencia se declaran entre otros aspectos fundamentales, los siguientes[26]:

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

---

2014, pp. 7-12. Disponible en: *http://www.uria.com/es/publicaciones/listado-revistas/44/numero38.html* (Fecha consulta: (Fecha consulta: 30/05/2018).

24. Al respecto, hay que señalar que en la práctica actual, ya la doctrina había puesto de manifiesto la problemática que plantea la difusión indiscriminada de información y datos vía plataformas y medios digitales. En este sentido, vid, GUICHOT, E., «La publicidad de datos personales en internet por parte de las administraciones públicas y el derecho al olvido», Revista española de derecho administrativo, n.º 154, 2012, págs. 125-169. Y, con posterioridad, se acuña la expresión «derecho al olvido digital» para hacer referencia a dicho fenómeno y, con todo, subrayando el interés jurídico de su consideración y la necesidad de disponer un régimen jurídico adecuado, así como de las debidas medidas de control y/o supervisión con el fin de evitar posibles abusos detectados en ciertos contenidos audiovisuales, lo que hace preciso reforzar la regulación y, en concreto, con referencia a la necesaria protección del derecho al olvido. Sobre esta cuestión, del mismo autor, « El derecho al olvido digital», en Boix Palop, A.; Martínez Otero, J.M.; y, Montiel Roig, G. (Coords.), *Regulación y control sobre contenidos audiovisuales en España*, Thomson Reuters-Aranzadi, Cizur Menor 2017 (pp. 117-144). En otro orden, digno es señalar que asimismo ya se puso de relieve el valor de los datos personales y lo esencial de observar protocolos específicos para su tratamiento en el marco de actuación de las Administraciones públicas, GUICHOT, E., *Datos personales y Administración Pública*. Aranzadi, Cizur Menor, 2005. Idem, «Datos personales y Administración Pública», en *Estudios de Protección de Datos*, Thomson-Civitas y Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), Madrid, 2005 (pp. 230-233).

25. Para mayor detalle sobre LOPD, vid., APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de carácter personal*. Aranzadi, Navarra 2013. NÚÑEZ LÓPEZ, M. Y DEL MAR FERREIRO, M., «Una aproximación para empresas a la Ley Orgánica de Protección de Datos», en *Derecom*, n.º 15. Nueva Época. Septiembre-Noviembre, 2013. págs. 93-109. Disponible en: *https://dialnet.unirioja.es/servlet/articulo?codigo=4399157* (Fecha consulta: 30/05/2018). REBOLLO DELGADO, L. Y SERRANO PÉREZ, M.ª., *Manual de protección de Datos*. Dikynson, Madrid 2014.

26. 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.

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 realiza una actividad que se dirige a los ciudadanos de dicho Estado.

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

Lo descrito ha supuesto una importante aportación, y configura la denominada doctrina del «derecho al olvido» (en la actualidad, este derecho a solicitar la supresión de datos ha sido integrado en el propio texto del vigente RGPD). Si bien, al respecto es oportuno recordar que ya, previamente, la AEPD había defendido dicha argumentación, interpretando que sí era aplicable en este caso, conforme a la legislación española y europea vigente en aquel momento. En este sentido, la doctrina española ya hace hincapié en el fundamento del derecho al olvido, que se infiere de los propios principios y valores enunciados en el Artículo 10.1 Constitución[27]. Si bien, de forma explícita la doctrina del derecho al olvido no se formularía –como tal– hasta dictar esta Sentencia 2014 (TJCE 2014, 85), que fue así favorable a la pretensión y argumentación defendida por España. Al respecto, digno es apreciar que fue relevante la labor de la AEPD y de la Abogacía del Estado en este procedimiento europeo, tal y como ha sido reconocida[28]. No obstante, se debe insistir en que el derecho al olvido, que confirma el TJUE con este pronunciamiento, no supone un derecho absoluto, y, por ende, mantiene un alcance limitado. En la práctica, supone un derecho a solicitar la supresión de datos, por lo que su ámbito de aplicación comprende el que ya era reconocido a los derechos de cancelación y oposición, y es a través de ellos como asimismo puede ser ejercitado por el afectado/s (titular de los datos).

En definitiva, en virtud de esta STJUE 2014 (TJCE 2014, 85), y conforme a la Directiva 95/46/CE, se dictó que los responsables de los motores de búsqueda en internet quedaban obligados a reconocer a los afectados lo que se denominó el «derecho al olvido», que suponía ejercer los derechos de oposición y de cancelación (en este caso aplicados a información disponible en la red), contenidos en dicha normativa europea y que integran el derecho fundamental a la protección de los datos personales. A dicho efecto,

27. Al respecto, SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch, Valencia 2012, pp. 115 y ss.. Y, del mismo autor, «El encaje constitucional del derecho al olvido digital en perspectiva comparada», en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n.º 54, 2012.

28. SILVA DE LA PUERTA, M., «El "derecho al olvido" como aportación española y el papel de la Abogacía del Estado», *Actualidad Jurídica Uría Menéndez*, n.º 38, octubre-diciembre 2014, págs. 7-12.

los interesados han de dirigirse al buscador y solicitar que cese la difusión de datos cuando estos pudieran afectar o producir lesión en sus derechos, sin justificación suficiente.

De igual modo, hay que significar que conforme a esta sentencia, se declara la *preferencia del DPD*. Lo que supone que, con carácter general (o, en principio), ha de prevalecer el derecho a la protección de datos de las personas frente al interés privativo de un operador o mercantil. Por ejemplo, en este caso, se dicta que prevalece dicho derecho fundamental sobre el «mero interés económico del gestor del motor de búsqueda». No obstante, también cabe admitir como *posible excepción* algunos supuestos, como aquellos en que el interesado fuera persona de relevancia pública y/o el acceso a la información quedara justificado con base al interés público.

En suma, dicho litigio permitió sentar la doctrina del derecho al olvido, y con ello se puso de manifiesto la necesidad de fijar una normativa europea común más sólida que resultara eficaz en aras de asegurar la protección de datos. A su vez, también ya se precisa que el derecho al olvido admite ciertos límites, justificados, en aras de hacer compatible su ejercicio con el respeto a otros derechos fundamentales reconocidos, y, de igual modo, en atención a la preferente tutela del interés público en determinados supuestos (por ejemplo, porque se tratara de una información relevante para la ciudadanía u opinión pública, entre otras razones, como ya hoy constan previstas en el texto vigente del RGPD, tal y como hemos referido supra). Recordando, en este sentido, la importancia del principio de transparencia y el derecho de acceso a la información pública, previstos en el Ordenamiento[29].

Además, con esta resolución STJUE 2014 (TJCE 2014, 85) donde se reconoce, –por vez primera de forma expresa–, el «derecho al olvido» frente a los motores de búsqueda, también resulta ilustrativa para otros planteamientos o argumentaciones relacionadas con esta cuestión; 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)[30], sin duda, motivados por una fácil y generalizada accesibilidad a la red, o el empleo masivo de otras redes

29. Véase al respecto, LUCAS MURILLO DE LA CUEVA, P., «Las vicisitudes del derecho de la protección de datos personales», en *Revista Vasca de Administración Pública*. Vol. 2, n.º 58, 2000, pág. 211-242. Y, haciendo referencia expresa al derecho a la información frente al derecho fundamental a la protección de datos, vid., Martínez Martínez, R., «El derecho fundamental a la protección de datos: perspectivas», págs. 54-56, en *Revista de los Estudios de Derecho y Ciencia Política de la UOC,* IDP, n.º 5, 2007. Disponible en: *https://dialnet.unirioja.es/descarga/articulo/2372613.pdf*; y *https://idp.uoc.edu/articles/10.7238/idp.v0i5.436/galley/3341/download/* (Fecha consulta: 10/05/2018). Citando in extenso el trabajo de CARRILLO LÓPEZ, Marc, *El derecho a no ser molestado: información y vida privada*. Thomson-Aranzadi, Navarra 2003.

30. 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*».

o vías electrónicas de comunicación para ofrecer o prestar de servicios global, etc.[31] Y, con todo, esta doctrina del «derecho al olvido» ha supuesto una importante aportación, que orienta la innovación jurídica en materia de protección de datos; al considerar de forma específica la no adecuación a Derecho de determinadas prácticas que se desarrollan en los entornos digitales[32]. Agregado a ello, cabe advertir que no siempre la información divulgada es con base a fuentes de calidad, o pudiera contener sesgos o no ser veraz[33].

Por ende, con todo, esta STJUE fue determinante para estimar que era necesario fijar una regulación eficaz con el fin de tutelar el DPD en la Unión Europea. Y en este sentido, esta STJUE ha sido valiosa, propiciando una doctrina jurisprudencial que ha sido clave en este ámbito, de utilidad para orientar o impulsar el nuevo RGDE, que de forma expresa integra esta doctrina; y a su vez para encaminar el diseño de protocolos de actuación[34].

2. DELIMITACIÓN Y EFECTOS DEL RECONOCIMIENTO DEL DERECHO AL OLVIDO (POSIBLES RESTRICCIONES DE OTROS DERECHOS)

Con posterioridad, ha sido completada esta doctrina del «derecho al olvido» (STJUE 2014 (TJCE 2014, 85)), mediante otros pronunciamientos; así, cabe citar la STJUE 2017 (TJCE 2017, 76) que ha permitido abundar en la configuración del «derecho al olvido», en concreto, en lo relativo a los posibles límites que pudieran resultar aplicables a este derecho. Si bien, es necesario precisar que el «derecho al olvido» no es absoluto, por lo que admite limitaciones, como así ya había declarado nuestro Tribunal Supremo (STS de 15 de octubre de 2015 (RJ 2015, 4417))[35].

---

31. Cf., Auto de la Audiencia Nacional de 27 de febrero de 2012 (RJCA 2012, 321), 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*».
32. Al respecto, RALLO LOMBARTE, A. «De la "libertad informática" a la constitucionalización de nuevos derechos digitales (1978-2018), págs. 639-669; CAPODIFERRO CUBERO, DANIEL, «La libertad de información frente a Internet», págs. 701-737, ambos trabajos en *Revista de Derecho Político*, N.º 100, 2017, «Monográfico con motivo del XL aniversario de la Constitución Española (I)».
33. En nuestro país, STC 104/1986, de 17 de julio (RTC 1986, 104), y en sentencias posteriores, STC 160/2003 (RTC 2003, 160), 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.
34. Cfr., Considerandos 66 y 67 RGPD.
35. En España, 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 (RJ 2015, 4417) (SP/SENT/827960). *https://blog.sepin.es/2015/10/derecho-olvido-tribunal-supremo-civil/* (Fecha consulta: 08/05/2018). 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 (RJCA 2014, 1065), 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.

2.1. Posibles límites al ejercicio del derecho de acceso a la información pública (STJUE de 9 de marzo de 2017 (TJCE 2017, 76))

La Sentencia del Tribunal de Justicia Europeo (Sala Segunda), de 9 de marzo de 2017 (TJCE 2017, 76), asunto C-398/15, S. Manni c. Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce, resulta ilustrativa en orden a ofrecer una delimitación del derecho al olvido en el ámbito de la información registral. De este modo, su análisis permite observar las implicaciones que el ejercicio del derecho al olvido puede conllevar observando su posible colisión con otros derechos (fundamentales); en este caso, el derecho de acceso a la información registral. El pronunciamiento dictado en este asunto, muestra una posición europea neutral y sumamente orientativa para los Estados, con carácter general, a fin de evitar dudas interpretativas o prevenir ante eventuales conflictos, que se suscitaran y pudieran afectar al deber de transparencia informativa.

En síntesis, lo que en esta asunto[36] se plantea es si procede la aplicación del derecho a olvido con respecto a datos publicados en el registro societario (en Italia), –lo que en España es el Registro mercantil–. En este asunto, el pronunciamiento estimó los argumentos del Abogado General, y sostiene que los Estados miembros no pueden garantizar a las personas físicas el derecho a obtener la supresión de datos (personales) que figuren por su relación con sociedades mercantiles; asimismo, se señala que esta cuestión podrá ser prevista por la normativa estatal, evaluando cada supuesto, y, en su caso, después de la liquidación de la entidad mercantil (o societaria) de que se tratara, a efectos de la posible supresión de datos personales que conciernen a personas, inscritos en el registro. Pero, *en todo caso, la Sentencia insiste en dar preferencia en interés general o público*; esto es, al derecho de acceso de información en relación con lo inscrito en el Registro, garantizando así la eficacia del principio de publicidad registral así como el cumplimiento de la legislación vigente. Por tanto, la postura adoptada por el TJUE es neutral y conciliadora. Y, de igual modo, con este pronunciamiento se hace especial hincapié en la necesidad de proteger los intereses de terceros en relación con las sociedades mercantiles, la seguridad jurídica, la lealtad de las transacciones comerciales y el buen funcionamiento del mercado interior.

Asimismo, se abre la posibilidad de ponderar situaciones particulares que puedan surgir, en las que fuera procedente estimar o considerar determinados motivos que justificaran adoptar resoluciones extraordinarias (v.gr., que pudieran limitar de hecho el acceso a determinada información, o que establezcan restricciones temporales, u otras decisiones o protocolos que habilitara cada Estado miembro al respecto). En este sentido, esta sentencia precisa que esta decisión corresponde, en cualquier caso, a los Estados miembros, conforme a la aplicación del Artículo 14, párrafo primero, letra a), de la Directiva 95/46. Luego, por vía del Derecho interno nacional, cabe establecer disposición

36. Esta sentencia fue dictada en el asunto C 398/15 y con objeto de resolver el planteamiento de una petición de decisión prejudicial, que fue presentada –conforme al artículo 267 TFUE– por la Corte Suprema di Cassazione (Tribunal Supremo de Casación de Italia), a través de Resolución de 21 de mayo de 2015, recibida en el Tribunal de Justicia el 23 de julio de 2015, en el procedimiento entre Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce, y Salvatore Manni.

en contrario, y, de esta forma cabe adoptar una decisión final sobre si las personas físicas pueden (o no) solicitar a la autoridad competente y/o responsable del registro la posible aplicación de dicho tipo de limitación de acceso a los datos personales. En definitiva, corresponderá al legislador interno/nacional regular esta cuestión y establecer la previsión de posibles excepciones o limitaciones. De igual modo, se señala que el Artículo 14 impone a los Estados miembros el deber de garantizar al interesado el ejercicio del «derecho de oposición», en los casos previstos en las letras e) y f) del Artículo 7. Recordando a su vez que dicha facultad se podrá ejercer en cualquier momento, y con base a motivos legítimos, estimando cada caso concreto y cuando los datos que le conciernan sean objeto de adecuado tratamiento, *salvo cuando la legislación nacional disponga otra cosa*[37].

VI. NOVEDADES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

Para concluir este estudio sobre el régimen jurídico aplicable en materia de tratamiento de datos personales, se estima oportuno, por su interés, dedicar un epígrafe a significar cuáles han sido las principales novedades incorporadas por el nuevo RGPD (2016). Con ello, se pretende ofrecer una detallada síntesis del marco regulatorio general vigente en el Derecho de la Unión Europea.

Los principales objetivos del RGPD, se centran en mejorar el nivel de protección de los datos personales de los ciudadanos en la Unión Europea, así como modernizar la normativa aplicable con el fin de adaptarla a la nueva era digital y sus tecnologías. Asimismo, se pretende concretar el marco de responsabilidades de operadores, gestión de datos, tratamiento y almacenamiento de datos, sistemas de evaluación y medidas de prevención. El cumplimiento de estos aspectos será clave para que las organizaciones puedan evitar incurrir en infracciones y sus posibles sanciones. Y para asegurar dicho cumplimiento han de establecer sistemas y protocolos de prevención de riesgos, respuesta y notificación, así como los necesarios procesos de evaluación mediante

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

auditorías[38]. Además, otras obligaciones suponen el deber de monitorizar comunicaciones y posibles transferencias de datos (transfronterizas)[39]. También se ha de revisar sus modelos contractuales y relaciones jurídicas con otras empresas o profesionales externos. Y, adaptar sus modelos de gestión y negocio, así como diseñar programas de formación destinados a sus empleados, informándoles en todo caso de sus obligaciones en relación con el acceso, uso y procesamiento de datos.

1. PRINCIPALES APORTACIONES

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

El RGPD con plenos efectos desde el 25 de mayo del 2018 (art. 99 RGPD), deroga de forma expresa la Directiva previa (art. 94), así como cualquier legislación anterior, europea y nacional, que pudiera ser contraria a la misma. En el caso de España, la normativa dictada: Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de carácter personal (LOPD), y en su desarrollo el Real Decreto 1720/2007, del 21 de diciembre. Como Reglamento europeo que es, tiene carácter vinculante y de aplicación directa en todos los Estados de la UE, regulando la protección de las personas físicas en lo que respecta: (i) al tratamiento de datos personales y (ii) a la libre circulación de estos datos. En concreto, este régimen es aplicable «*al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*» (Artículo 2.1); quedando *excluido*, de forma expresa, el tratamiento de datos que operase en los siguientes supuestos (Art. 2.2): «a) *en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de*

38. Las empresas y profesionales han de evitar o minimizar sus riesgos, trazando sus propios sistemas e implementando procedimientos conforme a las actividades y/o servicios que presten, con el fin de asegurar que los requerimientos de privacidad se cumplen. Asimismo, han de documentar el sistema y proceso de operaciones donde se emplearan datos personales, mediante el uso de «*Data Privacy Impact Assessments*» (DPIAs). Resulta esencial aplicar, documentar, evaluar y verificar las medidas de seguridad adecuadas –técnicas, físicas y administrativas– que han de ser coherentes con la tipología de riesgos identificados por el DPIAs.

39. Deben asegurar que la entidad tiene legitimidad para operar y transferir datos fuera de la UE, a países que carecieran de análogas normativas sobre DPD regulaciones de protección de datos adecuadas.

la Unión; b) *por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE*; c) *efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*; d) *por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención*».

Este sistema jurídico resulta innovador en algunas cuestiones, entre otras, por ejemplo, incorpora nuevos principios y deberes respecto a la precedente Directiva. Con ello, el marco regulatorio europeo queda completado y actualizado. Dicho régimen focaliza una serie de principios que han de regir en materia de PDP, y a su vez, dicta una serie de deberes que los sujetos obligados (entidades, empresas y profesionales) han de cumplir, en relación con el tratamiento y privacidad de información y datos. También refiere códigos de conducta y guía modelos autorregulatorios; establece un régimen de evaluación y verificación; autoridades y organismos competentes, a efectos de dictar desarrollos normativos y habilitación de medidas de control; y, por último, disciplina un régimen de responsabilidad y sancionador.

Conforme a lo señalado por el RGPD, todas las entidades y profesionales que traten datos de carácter personal han de tener adaptados sus sistemas y medidas de tratamiento de datos, herramientas y registros informativos, medios informáticos e instrumentos contractuales. En este sentido, con respecto a las obligaciones que corresponden a los sujetos responsables (y «encargados de datos»), 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. Y, además, por cada organización o entidad se ha de designar a la figura del Delegado de datos.

2. «PRINCIPIOS DE LA PROTECCIÓN DE DATOS»

Sumado a las nociones y consideraciones expuestas, cabe señalar que el régimen jurídico (general) aplicable a la PDP establece un cuadro preceptivo de «Principios de la protección de datos», que permiten concretar el DPD en la práctica de su ejercicio, así como cuáles son los aspectos, facultades y obligaciones que deben ser observadas en lo relativo al tratamiento de datos. El cuadro básico de estos principios ya quedaba previsto en la Directiva, pero, ha sido completado con otros en el actual RGPD. Aquí de nuevo digno es significar la aportación de la Jurisprudencia. De este modo, al vigente texto del RGPD dicta una serie de principios rectores (en concreto, se declaran seis) que en esta materia han de servir para disciplinar toda acción y proceso de gestión de la información y comunicación sobre datos personales; con ello, en el tratamiento de datos personales son de necesaria observancia dichos presupuestos.

El Artículo 5 del Reglamento General de Protección de Datos dicta seis principios, que son desarrollados con precisión a lo largo de este texto normativo, siendo por tanto

premisas claves del régimen vigente, y como tales han de ser consideradas en el empleo, tratamiento y almacenamiento de datos de carácter personal a. En síntesis, el enunciado y contenido de estos seis principios, es:

1. Los datos personales han de ser tratados de forma lícita, leal y transparente.
2. Los datos personales deben ser recogidos con fines concretos, explícitos y legítimos.
3. Los datos personales deben ser adecuados, pertinentes y limitados a la finalidad que motiva su tratamiento.
4. Los datos personales deben ser veraces, exactos y actualizados.
5. 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.
6. Los datos personales han de ser tratados de forma que se garantice su seguridad (gestión y prevención de riesgos).

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

3. DEBERES PARA LOS RESPONSABLES DE DATOS

El RGPD mantiene el principio recogido en la Directiva 95/46 de que todo tratamiento de datos precisa disponer de una base que lo legitime, que comprende: Consentimiento. Relación contractual. Interés/es del titular de los datos o de otras personas. Obligación legal para el responsable. Interés público o ejercicio de potestades públicas. Intereses legítimos preferentes.

En ese sentido, el RGPD no implica cambios para los responsables del tratamiento de datos. A modo de síntesis, entre las obligaciones que afectan a los sujetos responsables del tratamiento de datos (operadores), cabe destacar:

- La incorporación necesaria de la figura del Delegado de Protección de Datos (DPD). El Reglamento obliga a quienes realicen ciertos tratamientos, a designar un delegado, que ha de ser un profesional experto, que disponga de una formación específica y acreditada, tanto en PDP como en análisis de riesgos y medidas de seguridad de la información, que podrá ser personal interno o externo a la entidad.
- La obligación de registrar documentalmente las acciones y procesos de tratamiento. Dicho deber, corresponde tanto a los Responsables de ficheros como a los Encargados del tratamiento de datos (figuras definidas en el Artículo 4, apartados 7 y 8).

- Para el tratamiento de datos personales, se exige disponer del previo consentimiento expreso por parte del titular de los datos. En consecuencia, ya no es suficiente con un consentimiento tácito, por lo que los operadores o empresas quedan obligadas a solicitar dicho consentimiento y asegurar su constancia, también respecto a los datos previos de que dispongan (antes de la entrada en vigor del RGPD).
- Es necesario implementar métodos de evaluación de impacto y análisis de riesgos, haciendo especial referencia al tratamiento de cierta tipología de datos, medidas preventivas y de seguridad adoptadas.
- Quedan reforzados los deberes de transparencia informativa.
- Se establece la obligación de notificar cualquier tipo de vulneración de los sistemas de seguridad implementados relativos los datos personales. Así, en plazo máximo de 72 horas deberá ser comunicado cualquier eventualidad a la Agencia Española de Protección de Datos (AEPD), y de igual modo, en casos graves será necesario notificarlo a los afectados o interesados, con el fin de evitar mayores daños o perjuicios.
- Conforme al RGPD, será preciso revisar los instrumentos contractuales vigentes, así como diseñar nuevos modelos contractuales asegurando que cumplen con el RGPD. De igual modo, será necesario proceder a realizar nuevos contratos con los encargados de tratamiento, en cuyo clausulado se ha de prestar especial atención en lo relativo a las facultades de acceso a datos por terceros (respetando lo previsto como «contenido mínimo necesario»).
- Por otra parte, cabe señalar que –en principio– el RGPD no diferencia entre datos personales y datos profesionales. Por lo que las empresas han de adoptar las oportunas acciones en atención a cada perfil y categoría de datos.

4. 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 por el RGPD comprende los siguientes: derecho de acceso, derecho a la portabilidad de datos, derecho de cancelación, derecho de rectificación, derecho de oposición, y el «derecho al olvido». Este derecho al olvido, –expuesto con detalle en epígrafe previo–, en la práctica, supone una manifestación de los derechos de cancelación u oposición en el entorno digital u online. No obstante, este derecho tiene algunas limitaciones como son: la libertad de expresión, el derecho a la información, el interés público en el ámbito de la salud, la investigación, y la defensa de reclamaciones o recursos.

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

VII. A MODO DE COROLARIO

Conforme a todo lo expuesto y analizado en este estudio, hay que significar las aportaciones del nuevo Reglamento General de Protección de Datos (RGPD), en tanto aporta un régimen jurídico sólido y uniforme, aplicable en la Unión Europea; si bien, queda por evaluar cuál será su impacto en la práctica, v.gr., el grado de cumplimiento observado por parte de operadores y responsables de datos, así como otros eventuales conflictos que puede implicar el tratamiento de datos, o en lo relativo a la vulneración del DPD, entre otras cuestiones o efectos.

En todo caso, hay que reconocer la complejidad técnica y jurídica que conlleva la determinación de un régimen jurídico europeo común que pueda ser eficaz en materia de protección de datos; ello, entre otras razones por la problemática que en la práctica plantea el tratar de disciplinar las distintas tipologías de conductas que implican el tratamiento de datos, y sobre todo, considerando otros aspectos, como pueden ser: la diversidad de operadores y responsables, la problemática que surge en entornos globales y digitales, donde hoy de forma mayoritaria opera la prestación de servicios, asimismo la difusión de información y comunicación. Lo que, además, supone detectar y abordar nuevos riesgos, tanto los riesgos reputacionales como otros relativos a la ciberseguridad.

En suma, la evolución del régimen jurídico aplicable a la protección de datos (DPD) ha sido positiva en el Derecho comunitario europeo, actual Derecho de la Unión Europea. Y, con todo, existe mayor consciencia de la complejidad de esta materia, en especial, observando los deberes que supone el tratamiento de datos personales en la práctica, y a su vez la importancia que adquiere adoptar las medidas necesarias de gestión y prevención de los riesgos, así como de supervisión, lo que en esta materia resulta esencial. Y ello, porque además no se puede ignorar el posible impacto sobre la privacidad de los nuevos medios tecnológicos empleados en información y comunicación (TIC), y por otra parte, advirtiéndose que la información y datos difundidos a través de dichas herramientas no siempre es válida, ni actualizada (amén de considerar otros posibles eventos relativos a ciberseguridad).

VIII. BIBLIOGRAFÍA

Agencia Española de Protección de Datos (AEPD), «Guía del Reglamento General de Protección de Datos para responsables de tratamiento». Madrid 2018. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf (Fecha última consulta: 10/07/2018).

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». Madrid, 13 de mayo de 2014.

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

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

ASOCIACIÓN MEXICANA DE INTERNET A.C., «Estudio sobre el Valor Económico de los Datos Personales». Asociación Mexicana de Internet A.C. (AMIPCI) y la Secretaría de Economía, 2016. Disponible en: https://clustertic.org/wp-content/uploads/2016/06/valor_eco_Datospersonales_FINAL.pdf. (Fecha consultas: 14/07/2018).

BARNÉS VÁZQUEZ, J., «El principio de proporcionalidad», *Cuadernos de Derecho Público*, 5, Instituto Nacional de Administración Pública, Madrid 1998.

BOE, *Código del Derecho al Olvido* – BOE.es., 2018.

CAPODIFERRO CUBERO, D., «La libertad de información frente a Internet», Revista de Derecho Político, n.º 100, 2017. *Monográfico con motivo del XL aniversario de la Constitución Española (I)*. pp. 701-737.

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

DI PIZZO CHIACCHIO, A., «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», *Revista jurídica de Catalunya*, vol. 115, n.º 4, 2016. pp. 939-976.

GUICHOT, E., «La publicidad de datos personales en internet por parte de las administraciones públicas y el derecho al olvido», *Revista española de derecho administrativo*, n.º 154, 2012, pp. 125-169.

GUICHOT, E., « El derecho al olvido digital», en BOIX PALOP, A.; MARTÍNEZ OTERO, J.M.; Y, MONTIEL ROIG, G. (Coords.), *Regulación y control sobre contenidos audiovisuales en España*, Thomson Reuters-Aranzadi, Cizur Menor 2017 (pp. 117-144).

GUICHOT, E., *Datos personales y Administración Pública*. Aranzadi, Cizur Menor, 2005.

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

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

HERRÁN ORTIZ, A.I., «El derecho a la protección de datos en la sociedad de la información», Cuadernos Deusto de Derechos Humanos, Universidad de Deusto (Bilbao), n.º 26, 2003. Disponible en: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf (Fecha consulta: 30/06/2018).

LISSÉN ARBELOA, J.M., y CRESPO VITORIQUE, I., «Publicada la directiva sobre ciberseguridad: obligaciones para los gestores de infraestructuras críticas y servicios esenciales», en Análisis GA&P, Julio 2016 (27/07/2016). Disponible en: http://www.gomezacebo-pombo.com/index.php/pt/conhecimento/analises/item/2411-publicada-la-directiva-sobre-ciberseguridad-obligaciones-para-los-gestores-de-infraestructuras-criticas-y-servicios-esenciales (Fecha última consulta: 15/07/2018).

LÓPEZ PORTAS, M.B., «La Configuración Jurídica Del Derecho al Olvido en el Derecho Español a tenor de la doctrina del TJUE», *Revista UnED Facultad de Derecho*, n.º 93, 2015. Disponible en: http://revistas.uned.es/index.php/derechopolitico/article/view/15140. (Fecha consulta: 30/05/2018).

LUCAS MURILLO DE LA CUEVA, P., «El derecho a la autodeterminación informativa y la protección de datos personales», *Azpilcueta: cuadernos de derecho*, n.º 20, 2008, pp. 43-58.

LUCAS MURILLO DE LA CUEVA, P., «Las vicisitudes del derecho de la protección de datos personales», en *Revista Vasca de Administración Pública*. Vol. 2, n.º 58, 2000, pp. 211-242.

MARTÍNEZ MARTÍNEZ, R., «El derecho fundamental a la protección de datos: perspectivas», Monográfico «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas», Revista de los Estudios de Derecho y Ciencia Política de la UOC, IDP, n.º 5, 2007, pp. 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 DEL MAR FERREIRO, M., «Una aproximación para empresas a la Ley Orgánica de Protección de Datos», en Derecom, n.º 15. Nueva Época. Septiembre-Noviembre, 2013. pp. 93-109. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4399157 (Fecha consulta: 30/05/2018).

OECD (2013): «Exploring the Economics of Personal Data. A survey of methodologies for measuring monetary value», en: https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (Fecha consultas: 14/07/2018).

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

ORTI VALLEJO, A., «El nuevo derecho fundamental (y de la personalidad) a la libertad informática (a propósito de la STC 254/1993, de 20 de julio (RTC 1993, 254))», *Derecho Privado y Constitución*, núm. 2. Enero-Abril, 1994, pp. 305-332.

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

PIÑAR MAÑAS, J.L., «Sociedad, innovación y privacidad», El cambio digital en la economía. Un proceso disruptivo, Revista de economía ICE, N.º 897, Julio-Agosto 2017. pp. 67-75. Disponible en: http://www.revistasice.com/CachePDF/ICE_897_67-76__D7E83A07D3A91562598E4FFFF3D312E8.pdf (Fecha consulta: 15/07/2018).

PIÑAR MAÑAS, J.L., «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 (TJCE 2014, 85), Caso GOOGLE», en *Iuris: Actualidad y práctica del derecho*, n.º 215, 2014, pp. 20-23.

PIÑAR MAÑAS, J.L., «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*, n.º 49, 2014, pp. 1-19.

PIÑAR MAÑAS, J.L., «¿Existe la privacidad?», Universidad CEU San Pablo, Madrid 2008. 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., «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)*. N.º 100, 2017, pp. 639-669.

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

REBOLLO DELGADO, L. y SERRANO PÉREZ, M.ª., *Manual de protección de Datos*. Dikynson, Madrid 2014.

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

RUIZ MIGUEL, C., «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, n.º 14, 2003, pp. 7-43. Texto disponible en: https://dialnet.unirioja.es/servlet/autor?codigo=176117 (Fecha consulta: 30/05/2018).

SILVA DE LA PUERTA, M., «El "derecho al olvido" como aportación española y el papel de la Abogacía del Estado», Actualidad Jurídica Uría Menéndez, n.º 38, octubre – diciembre 2014, pp. 7-12. Disponible en: http://www.uria.com/es/publicaciones/listado-revistas/44/numero38.html (Fecha consulta: 30/05/2018).

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

SIMÓN CASTELLANO, P., «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*, n.º 54, 2012.

TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio*. Tirant lo Blanch, Valencia 2010. (pp. 914 y 920-937).