APROXIMACIÓN AL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EUROPA. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES A DEBATE

ANA ISABEL HERRÁN ORTIZ
Profesora Titular de Derecho civil. Universidad de Deusto

Fecha de recepción: 24 de mayo
Fecha de aceptación: 15 de junio

RESUMEN: Recientemente, se publicaba el esperado Reglamento General de Protección de Datos en la Unión Europea. Mucho tiempo se ha tenido que esperar hasta la aprobación de esta norma, y muchas han sido las expectativas jurídicas que este texto había generado. Pretendemos en este trabajo presentar unas breves notas que analicen algunas de las novedades más significativas de este Reglamento, que si bien no será aplicable hasta 2018, exigirá, como tendremos ocasión de explicar, un gran esfuerzo de los Estados miembros para adaptar su derecho nacional al nuevo contexto legal europeo en protección de datos personales.

ABSTRACT: Recently, the expected General Data Protection Regulation was published in the European Union. The approval of this regulation has been long awaited and the text had created high legal expectations. In this paper we intend to present some brief notes that analyze some of the most significant changes introduced by this Regulation which, although not applicable until 2018, will require, as we will explain, a great effort by the Member States to adapt their national laws to the new European legal context in data protection.

PALABRAS CLAVE: Datos personales Europa Reglamento principios derechos.

KEY WORDS: Europe Regulation personal data rights principles.

EL NUEVO MARCO NORMATIVO EUROPEO DE PROTECCIÓN DE DATOS. PERSPECTIVA GENERAL

Larga ha sido la espera hasta la reciente publicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, aprobado el 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 (en adelante, RGPD)[1]. Su entrada en vigor ha tenido lugar este reciente 24 de mayo de 2016, sin embargo, su aplicación deberá esperar hasta el 25 de mayo de 2018; en ese tiempo, los Estados deben apresurarse y adaptar su normativa a los nuevos dictados del RGPD en la regulación de la protección de datos de carácter personal, y la libre circulación de los mismos.

Su publicación ha puesto fin a varios años de incertidumbre jurídica sobre el rumbo que en el ámbito europeo tomaría el derecho a la protección de datos personales y su tutela. Al mismo tiempo, la aprobación de esta normativa satisfacía las exigencias expresadas tanto desde el sector público como del privado, reclamando una nueva normativa, que permitiera la consideración de la protección de datos desde una perspectiva más actual, acorde con los nuevos avances digitales, y que facilitara la aplicación uniforme de principios, normas y buenas prácticas en toda la Unión Europea.

En efecto, era preciso alcanzar la necesaria armonización legal, y lograr la aplicación de normas uniformes en todos los Estados miembros, garantizando de este modo un nivel de protección de los derechos y libertades de las personas físicas en lo que al tratamiento de sus datos personales se refiere equivalente en todos los Estados miembros, mediante la aplicación coherente y homogénea de normas de protección de datos personales en Europa.

En este sentido, coincide la doctrina en destacar que es una norma que regula el tratamiento de la información y la propia circulación de los datos, lo que justifica su trascendencia jurídica. Y además, que dicha norma adopte la forma de un Reglamento implicará que su aplicación sea más directa que la propia de cualquier directiva. Así lo explicita igualmente el propio RGPD, cuando en su art. 99 advierte que "El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro".

Ahora bien, tal y como resultará patente a lo largo de este trabajo, el citado RGPD es heredero de la Directiva 95/46/CE[2], de cuyas previsiones no se distancia, tal y como se

[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). Diario Oficial de la Unión Europea L 119/1, de 4 de mayo de 2016.

[2] 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, DOUE núm. L 281/31, de 23 de noviembre de 1995.

reconoce en el propio texto del Reglamento[3]. Al mismo tiempo se concede un amplio margen al derecho nacional de los Estados, con lo que la adaptación de dichas normas al nuevo texto representa un reto para los Estados, y genera no pocas incertidumbres jurídicas en relación con la aplicación coherente y uniforme de sus previsiones en cada Estado. En efecto, son numerosas las ocasiones en las que el RGPD cede a las legislaciones nacionales la posibilidad de establecer y delimitar garantías, medidas o facultades para la tutela del derecho a la protección de datos; entre otros, véase el art. 6.3 o el art. 9 del RGPD. Ciertamente, tal y como apuntan algunos autores, no es descabellado pensar que en breve el legislador español deberá acomodar la normativa española a los nuevos tiempos que nacen en el derecho a la protección de datos personales con la aprobación de este Reglamento europeo[4].

Por otra parte, ha sido definido el texto cuyo estudio abordaremos, como una norma compleja, minuciosa, de difícil interpretación, y cargada de conceptos jurídicos indeterminados, que sin duda complicará la labor de análisis y aplicación de un texto, cuya mayor virtud, a decir de los expertos, reside en la uniformidad legislativa que instaura en la UE en materia de protección de datos personales[5].

Con todo, sin embargo, no parece que inicialmente las expectativas que este texto generó se hayan visto cumplidas, y como tendremos oportunidad de exponer en el presente trabajo, son numerosas en nuestro país las voces críticas que se han alzado contra el RGPD. Solo el tiempo, y su posterior aplicación en mayo de 2018 determinarán el acierto de los Estados al adaptar a sus derechos nacionales los principios, derechos y obligaciones que la norma prevé; o por el contrario, lamentarán que la tan ansiada uniformidad en la aplicación de principios y derechos de protección de datos personales en Europa aún deba esperar.

¿HACIA UNA NUEVA CONFIGURACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EUROPA?

Sorprende la rotundidad con la que el legislador europeo configura en el RGPD la naturaleza del derecho a la protección de datos personales, cuando en el primero de los considerandos que abren el esperado texto, afirma que la protección de las personas físicas en relación con el tratamiento de sus datos personales "es un derecho fundamental". Cierto que antes la propia Carta Europea de los Derechos Fundamentales de la Unión Europea ya había anticipado en su art. 8 que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan"[6]. No se limita, sin embargo, el legislador europeo a proclamar dicha consideración, bien al contrario, extiende dicha protección a las personas físicas "cualquiera que sea su nacionalidad o residencia", vinculando directamente los principios y normas relativos a la protección de las personas físicas en el tratamiento de sus datos personales, con el respeto a las libertades y los derechos fundamentales.

A mayor abundamiento el art. 1 del citado RGPD establece como objeto de protección "los derechos y libertades fundamentales de las personas físicas, y en particular, su derecho

[3] Véase el Considerando 9 del RGPD, que proclama explícitamente la validez de los objetivos y principios de la Directiva 95/46/CE.

[4] PIÑAR MAÑA, José Luis. "Principales novedades del Reglamento". Jornada de ENATIC sobre el Reglamento General de Protección de Datos, Madrid, 29 de abril de 2016.

[5] C. FERNÁNDEZ HERNÁNDEZ, "El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales", *Diario La Ley*, núm. 8762, Sección Práctica Forense, 16 de Mayo de 2016.

[6] CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (2000/C 364/01), Diario Oficial de las Comunidades Europeas C 364/1, de 18 de diciembre de 2000. Continua diciendo el citado artículo 8 que "Estos datos se tratar en de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación".

a la protección de datos personales", siendo así que entonces la presente norma no solo tutela el derecho a la protección de datos personales, sino cualesquiera derechos y libertades fundamentales de la persona que pudieran verse afectados por el tratamiento de los datos personales.

En este sentido, si bien se contempla la necesidad de integrar al ser humano en el desarrollo técnico, ello no impide reconocer las carencias del actual marco normativo europeo de protección de datos personales, especialmente en las diferencias importantes que separan a las distintas normativas nacionales de protección de datos de los Estados miembros, y que constituyen a juicio del legislador europeo un importante obstáculo al ejercicio de las actividades económicas en la Unión, falsean la competencia y pueden dificultar la libre circulación de los datos personales en la Unión (véase el Considerando 9 del RGPD).

Por ello, la protección otorgada en materia de tratamiento de la información personal, debe aplicarse a las personas físicas, independientemente de su nacionalidad o lugar de residencia. De igual modo, advierte el RGPD en su Considerando 13 que es necesario un RGPD que proporcione seguridad jurídica y transparencia a todos los operadores económicos, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior.

Merece especial atención sobre el reconocimiento y ejercicio al interesado de los derechos en el marco del RGPD, la previsión establecida en el Considerando (142), por la cual, el interesado que considere vulnerados los derechos reconocidos en el Reglamento (repárese que no solo se alude a derechos a la protección de datos personales) deberá tener derecho a conferir un mandato a una entidad, organización o asociación sin ánimo de lucro[7].

En este sentido, representa una novedad legislativa, sin precedentes en el ámbito de la protección de datos personales, la posibilidad que conforme al art. 80 y de acuerdo con lo explicado en el Considerando 142 reconoce al interesado el derecho a conceder un mandato a entidad, organización o asociación, en los términos anteriormente señalados, para que presente en su nombre una reclamación, y ejerza, cuando corresponda, los derechos oportunos ante la autoridad de control o judicialmente (véase arts. 77, 78 y 79 del RGPD), así como el derecho a reclamar la correspondiente indemnización, si así se contempla en la legislación nacional del Estado miembro. En efecto, un derecho que al menos en la legislación española adopta la condición jurídica de personalísimo, y cuyo ejercicio, con las salvedades legales, corresponde al propio interesado, admite que, con las restricciones legales de cada derecho nacional, pueda ser ejercitado al menos en vía judicial y ante la autoridad correspondiente, por representación, mediante una asociación y no necesariamente cuando el interesado haya concedido un mandato, sino cuando así se disponga por el Estado miembro, exceptuando el derecho a indemnización y la reclamación de responsabilidad por el tratamiento de datos personales, que corresponde al interesado o a la persona jurídica en que quien se delegue expresamente.

[7] Conforme se explica en el citado Considerando (142), se trata de organizaciones sin ánimo de lucro que estén constituidas con arreglo al Derecho de un Estado miembro, tengan objetivos estatutarios que sean de interés público y actúen en el ámbito de la protección de los datos personales, para que presenten en su nombre una reclamación ante la autoridad de control, ejerzan el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerzan el derecho a recibir una indemnización en nombre de estos. Un Estado miembro puede reconocer a tal entidad, organización o asociación el derecho a presentar en él una reclamación con independencia del mandato de un interesado y el derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al presente Reglamento. Ahora bien, esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último.

El tiempo dirá en qué medida y con qué garantías los Estados miembros articulan esta facultad del interesado, y qué efectividad práctica alcanzará la posibilidad de que el interesado sea representado en sus reclamaciones judiciales o extrajudiciales por perjuicios a sus derechos como consecuencia de tratamientos de datos personales que le conciernen, e infringen las normas y principios del presente Reglamento general de protección de datos.

A VUELTAS CON LA DEFINICIÓN DEL ÁMBITO DE APLICACIÓN DEL RGPD

Se ha señalado como uno de los aspectos más destacados y novedosos del Reglamento general, la extensión de su ámbito de aplicación, en especial en el ámbito territorial[8]. Así, si el texto de la Directiva 95/46/CE el art. 4 c) se mostraba muy escueto, y restringía la aplicación de las disposiciones nacionales que se hayan aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales, entre otras circunstancias, cuando "el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea"; el RGPD, por el contrario, hace extensiva su aplicación a todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar o no en la Unión. Y entiéndase a los efectos del RGPD, que un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto (véase Considerando 22 del RGPD).

1. Ámbito de aplicación material

No representa ninguna novedad la delimitación del ámbito material de aplicación del RGPD, en relación con lo anteriormente previsto en la derogada Directiva 95/46/CE, por cuanto que ya el art. 3.1 de la citada norma expresaba que "las disposiciones de la presente Directiva se aplicarán 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".

Justifica el Considerando (15) esta decisión argumentando a tal efecto que la protección de las personas físicas por el tratamiento de sus datos personales no puede hacerse depender de las técnicas de tratamiento utilizadas en cada caso; si bien, excluye de la aplicación del reglamento a los ficheros o conjuntos de ficheros que no se encuentren estructurados conforme a criterios específicos. Ciertamente, si la información personal no se encuentra ordenada o estructurada de acuerdo a criterios o principios no constituye un fichero, con forme a la definición que ofrece el propio Reglamento, y según la cual, se entenderá por fichero "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

En otro orden de consideraciones, y en clara sintonía con lo previsto en la Directiva 95/46/CE, el Reglamento no se aplicará al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

[8] M. ARIAS POU, "Las 10 claves del Reglamento general de protección de datos (Reglamento 2016/679, de 27 de abril. DOUE del 4 de mayo de 2016)", *Diario La Ley,* núm. 8756, 6 de Mayo de 2016, pp.1-7.

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.

Como consecuencia de la dispersión legislativa que impera en materia de protección de datos personales en el ámbito de la UE, se encuentra obligado el legislador comunitario a establecer principios y normas que concilien la aplicación de este Reglamento, como norma general de protección de datos, con otros textos europeos ya en vigor, y de aplicación sectorial. Tal es el caso de las normas contempladas en el Reglamento (CE) nº 45/2001 de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. Así, el Reglamento (CE) nº 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98[9]; así como la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15[10].

2. El ámbito de aplicación territorial

Coinciden los expertos en señalar que se ha extendido significativamente el ámbito de aplicación territorial del RGPD, en relación con lo anteriormente previsto en la Directiva[11]. Así, con carácter general, el presente RGPD, tal y como ha sido indicado anteriormente, se aplica al tratamiento de datos personales en el contexto de las actividades de un

[9] Justifica el propio texto del RGPD en su Considerando 17 la necesidad de adecuar ciertos actos jurídicos de la Unión, al señalar que "otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión…".

[10] No son estas las únicas oportunidades en el que el Reglamento se refiere a la necesidad de garantizar la coherencia normativa en la aplicación de los principios y normas de protección de datos, una vez aprobado en reglamento general. Así, el Considerando 173 , a cuyo tenor, el Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo (2), incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas, con el propósito de esclarecer la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia; de este modo, una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento.

[11] Explica la AEPD que el "Reglamento se aplicará como hasta ahora a responsables o encargados de tratamiento de datos establecidos en la Unión Europea, y se amplía a responsables y encargados no establecidos en la UE siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento. Esta novedad supone una garantía adicional a los ciudadanos europeos. En la actualidad, para tratar datos no es necesario mantener una presencia física sobre un territorio, por lo que el Reglamento pretende adaptar los criterios que determinan qué empresas deben cumplirlo a la realidad del mundo de internet. Ello permite que el Reglamento sea aplicable a empresas que, hasta ahora, podían estar tratando datos de personas en la Unión y, sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea. AEPD. El Reglamento de protección de datos en 12 preguntas. Nota de prensa. Véase https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php (última consulta: 30/05/2016)

.

establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no (art. 3.1 Reglamento general). Y es en este punto donde se observa un significativo giro en la política de protección de datos, en cuanto a la aplicación de las normas europeas, cuyo ámbito no se restringe al territorio de la UE, sino que alcanzará al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no, e independientemente también de las modalidades jurídicas que pudiera adoptar dicho establecimiento (sea sucursal, filial..). Se pretende, de este modo, impedir que entidades cuya actividad se desarrolla territorialmente en un Estado miembro, no queden obligadas por el RGPD, habida cuenta que el tratamiento de datos personales se efectúa fuera del territorio de la UE. Asimismo, el presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Por otra parte, el RGPD se aplicará igualmente al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

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

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

En este sentido, explica el Considerando 23 del citado texto normativo que para determinar si dicho responsable o encargado "ofrece bienes o servicios a interesados que residan en la Unión" debe precisarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión; y así, la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no son suficientes para determinar dicha intención, hay factores, que a juicio del legislador comunitario pueden revelar que el responsable proyecta ofrecer bienes y servicios a interesados en la UE, y así, se citan a modo ejemplo: el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión.

Por su parte, y conforme la interpretación que se prevé en el Considerando 24, para determinar si se puede considerar que una actividad de tratamiento de datos personales controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

Lo anteriormente expresado, a nuestro juicio, constituye un intento más del legislador europeo por someter a los principios y normas de protección de datos europeos a las grandes multinacionales que, intentan soslayar la aplicación de las normas de protección de datos personales la UE, operando desde territorios no pertenecientes a la UE, y realizando los tratamientos de la información en terceros países, cuando, sin embargo, se dirigen a los consumidores europeos con sus productos y servicios.

LA EVOLUCIÓN DE LOS PRINCIPIOS Y DERECHOS EN LA PROTECCIÓN DE DATOS PERSONALES EN EUROPA

Por todos es conocido que el imparable desarrollo tecnológico hacía necesario contemplar el derecho a la protección de datos personales desde una nueva perspectiva más dinámica, y menos tradicional. En efecto, la irrupción de las redes sociales, el avance de la tecnología móvil, el Big Data y las nuevas formas de tratamiento de la información personal pronto demostraron que los tradicionales derechos ARCO vinculados a la protección de datos personales no permitirían por sí solos articular suficientemente la protección del ciudadano en el tratamiento de datos personales en este nuevo contexto tecnológico.

En consecuencia, se incorporan al elenco de derechos y garantías tradicionales en el tratamiento de la información personal, otros más novedosos, y acordes con la realidad tecnológica que nos rodea, así: el derecho de transparencia de la información (art. 12 RGPD), el derecho de supresión o "derecho al olvido" (art. 17 RGPD), el derecho a la limitación del tratamiento (art. 18 RGPD) o el derecho a la portabilidad de los datos (art. 20 RGPD).

Por todo ello, es evidente que la entrada en vigor del RGPD conllevará la ampliación de los tradicionales derechos ARCO que hasta ahora se reconocían al ciudadano en el derecho español, y la incorporación de nuevos derechos para la protección de los datos personales del interesado, vinculados con el principio de control de los propios datos personales que reconoce el RGPD (véase Considerando 7).

1. A propósito de los nuevos principios de protección de datos personales

1.1. El principio de transparencia en el tratamiento de datos personales

Explica el art. 5 del RGPD que los datos serán tratados de manera "lícita, leal y transparente en relación con el interesado". Y es precisamente en la necesidad de transparencia, donde encontramos la primera novedad en la proclamación de los nuevos principios que inspiran y orientan el tratamiento de datos personales a partir de la recién aprobada normativa europea.

Y entonces la pregunta que surge es: ¿en qué se concreta legalmente el reconocimiento y aplicación de este nuevo principio de transparencia? Todos seguramente coincidiremos en señalar que el principio de transparencia exige que la información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y comprensible, y que se utilice un lenguaje sencillo y claro. Este principio de transparencia, conforme expresa el art. 12 del RGPD, debe regir en todas las actuaciones de información que el responsable del tratamiento dirija al público o al interesado, de tal forma que se indica que la comunicación:

a) Sea en forma concisa, transparente e inteligible
b) Fácilmente accesible,
c) Fácil de entender, en el caso de menores
d) Utilizándose un leguaje claro y sencillo.

Este principio encuentra concreción legal, en la regulación del derecho de transparencia y sus modalidades, que en el art 12 del RGPD se contempla como una auténtica obligación legal del responsable del tratamiento, que deberá cumplirse, salvo petición expresa el interesado, por escrito o por otros medios, inclusiva loe electrónicos.

Claro que el contenido del mencionado derecho no se limita a facilitar el acceso e información sobre el tratamiento de datos personales; bien el contrario, el apartado 2 del propio art. 12 RGPD afirma que el responsable del tratamiento, facilitará al interesado "el ejercicio de sus derechos en virtud de los arts. 15 a 22", en el plazo de un mes a contar desde la solicitud. Cierto es que dicho plazo es susceptible de prorrogarse otros dos meses más, en caso de necesidad y siempre teniendo en cuenta la complejidad y el número de solitudes. El ejercicio de este derecho así como toda actuación, comunicación o información que se facilite

al interesado será gratuita. Excepcionalmente, podrá reclamarse un canon razonable en función de los costes administrativos ocasionados para facilitar la información o la comunicación, o realizar la actuación; o en su caso, negarse a actuar respecto de la solicitud.

Si el responsable rechazare la solitud del interesado, deberá informar de ello sin dilación, y en un plazo máximo de un mes desde la recepción de la solitud, argumentando las razones de dicho rechazo, y señalando al interesado la posibilidad de presentar reclamaciones ante la autoridad de control o ante autoridades jurisdiccionales.

Sorprende la precisión y el detalle con que el legislador europeo configura este derecho, señalando plazos de respuesta, o incluso limitando la posible ampliación de los mismos. Esta circunstancia únicamente se explica desde el manifiesto temor que expresa el RGPD a repetir errores propios de normas anteriores, y por las cuales se desvirtuaba en cada Estado miembro la aplicación de las normas comunitarias, con interpretaciones divergentes, y normas internas ambiguas.

1.2. El principio del consentimiento. Nuevas condiciones de validez

De la lectura de la definición del consentimiento en el art. 4 11º del RGPD, se desprende que el consentimiento es "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le concierne". Puede concluirse a partir de esta declaración que, en esencia, el consentimiento presenta en el RGPD idénticas características que en la normativa española, y en la Directiva 95/46/CE; esto es, se ha de tratar de una declaración de voluntad "libre, específica, informada e inequívoca". Y siendo esto cierto, no lo es menos, que hay aspectos en los que el Reglamento se distancia de la normativa española vigente en materia de protección de datos, y prevé nuevas exigencias para la validez del consentimiento, coherentes con el principio de responsabilidad "proactiva" que el propio Reglamento proclama. En primer lugar, debe ser capaz de demostrar el responsable del tratamiento que el interesado ha prestado su consentimiento al tratamiento; en segundo lugar, el carácter específico del consentimiento queda suficientemente garantizado en el Reglamento, y no se permite disimular o esconder la solicitud de consentimiento en el contexto de una declaración escrita referida a otros asuntos, distintos del propio tratamiento de la información personal.

Y así, la solicitud del consentimiento para el tratamiento de datos personales deberá diferenciarse claramente de los demás aspectos, se aspira, conforme expresa el propio Reglamento, a garantizar que "que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace" (Considerando 42).

Igualmente, el consentimiento debe prestarse libremente, y es por ello, que conforme expone el RGPD, deberá tenerse en cuenta a tales efectos, entre otras circunstancias, "si la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato". Ello porque como advierte el Considerando 42 del RGPD "El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno"[12].

Recapitulando, no parece admisible con la aplicación del RGPD la prestación tácita del consentimiento, y tampoco será válida cualquier otra declaración de voluntad que no conste específicamente, y de forma separada; igualmente, la libertad en la prestación del consentimiento tiene como fundamento legal la libre elección del interesado, y la ausencia de perjuicio para quien dedica denegar o retirar el consentimiento. A tenor de lo expresado

[12] Tanto es así, que conforme al Considerando (43), se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento.

es acertado pensar que el legislador español pronto abordará una reforma normativa, que facilite la aplicación de estas nuevas previsiones en nuestro derecho interno.

1.3. El principio de privacidad desde el diseño y por defecto

Han destacado los expertos la incorporación del principio de *Privacy by design* en el Reglamento como una muestra evidente de la evolución en la regulación de la protección de datos personales, de forma que la privacidad por diseño constituirá una obligación legal exigible cuando entre en vigor el Reglamento Europeo de Protección de Datos.

No puede decirse, sin embargo, que este principio se consagre en el RGPD por vez primera y constituya una novedad en el ámbito de la protección de datos personales. Antes al contrario, debemos recordar que en los años 90 la Dra. Cavoukian acuñó el concepto y desarrolló sus principios fundamentales[13]; después, y más recientemente, en la 32nd International Conference of Data Protection and Privacy Commissioners celebrada en Jerusalén, en 2010, se adoptó una Resolución sobre *Privacy by Design*[14]. Dicho concepto se ha desarrollado a partir de siete principios que lo articulan y aplican en el tratamiento de datos personales. La auténtica novedad reside en su formulación legal y en su configuración como obligación jurídica del responsable del tratamiento.

Por su parte, garantiza el RGPD en su art. 25 que el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

Ahora bien, son numerosas las dudas e incertidumbres que rodean a dicho reconocimiento; y así, el desarrollo de los principios exigibles de privacidad por defecto y desde el diseño, ofrece ciertas dudas e incertidumbres , en cuanto a su aplicación práctica, al tiempo que dicha implementación exigirá a las Administraciones Públicas dotar a las organizaciones de los recursos necesarios para llevar a cabo acciones orientadas a sensibilizar y facilitar la capacitación y el conocimiento práctico necesario, para implementar las medidas preventivas desde el propio diseño de la actividad, el proceso, o el negocio, al objeto de incorporar las garantías suficientes para proteger la privacidad y el derecho fundamental a la protección de datos personales.

La incorporación de este principio, como obligación legal del responsable, debe valorarse positivamente, y es de esperar que actúe como instrumento jurídico que permita sensibilizar a las empresas y a las organizaciones sobre la necesidad de establecer medidas de control y prevención adecuadas, garantizando el mantenimiento de un entorno digital más seguro y sólido respecto a gestión de la información y la seguridad de los sistemas informáticos. En efecto, la entrada de esta buena práctica a la normativa europea, viene a fortalecer el carácter preventivo del RGPD, y a impulsar un marco de confianza en el tratamiento de datos personales, al tiempo que se establecen principios para garantizar el control de la información personal por el propio usuario.

Al amparo del principio de minimización de los datos, previsto en el art. 5, y como manifestación práctica del mismo, el art. 25 del RGPD exige que "el responsable del tratamiento aplique las medidas técnicas y organizativas apropiadas con miras a garantizar que, *por defecto*, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento". Asimismo, se garantizará

[13] A. CAVOUIKIAN, Privacy by Design. The 7 Foundational Principles, 2011. Véase documento revisado en https://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/ (última consulta: 20/05/2016)
[14] Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalen (Israel), 27-29 October, 2010.

que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

2. La consagración legal de nuevos derechos del interesado en la protección de datos. En especial , el derecho de supresión y el derecho a la limitación del tratamiento

2.1. La configuración del "derecho al olvido" en el RGPD

Otra de las novedades más significativas ha sido la regulación en el RGPD del derecho de supresión, también conocido como "derecho al olvido". Y a tal efecto, prevé el art. 17 RGPD que el interesado tendrá derecho a obtener, sin dilación indebida, del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

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

b) el interesado retire el consentimiento en que se basa el tratamiento, y éste no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento;

d) los datos personales hayan sido tratados ilícitamente;

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

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

Varias son las observaciones que pueden introducirse a propósito de los conceptos jurídicos indeterminados que se introducen en esta previsión legal. Por un lado, si bien el legislador no determina un plazo, como el caso del derecho a la transparencia, establece con reiteración que deberá procederse por el responsable del tratamiento "sin dilación indebida" a la supresión de los datos personales del interesado cuando se aprecie cualquier de las circunstancias a tal efecto establecidas. De igual manera, el responsable del tratamiento, cuando haya hecho públicos los datos personales y estén obligados a su supresión, deberá adoptar las "medidas razonables" para informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a dichos datos personales, o de copia o replica de los mismos[15].

Excepcionalmente, no procederá la supresión de los datos personales cuando el tratamiento sea necesario, entre otras circunstancias, para la formulación el ejercicio o defensa de reclamaciones; para ejercer el derecho a la libertad de expresión e información[16];

---

[15] A este respecto, el TJCE en 2014 declaró que conforme al derecho de acceso y al derecho de oposición reconocidos en los artículos 12, letra b) y 14, párrafo primero, letra a), de la Directiva 95/46, deben interpretarse en el sentido de que, "para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita". Cfr. SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala), de 13 de mayo de 2014.

[16] Más recientemente, el TS ha explicado que "El llamado "derecho al olvido digital", que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos

o con fines de archivo en interés público, fines de investigación científica, histórica o fines estadísticos, en la medida en que dicha supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento[17]. Así lo entendió también nuestro alto tribunal al expresar que "La primera de las medidas adoptadas (la eliminación de sus datos personales del código fuente de la página web que contiene la noticia) supone un sacrificio desproporcionado, por excesivo, del derecho a la libertad de información. El llamado "derecho al olvido digital" no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día. Las hemerotecas digitales gozan de la protección de la libertad de información, al satisfacer un interés público en el acceso a la información. Por ello, las noticias pasadas no pueden ser objeto de cancelación o alteración… Por tanto, la integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión (en el sentido amplio del art. 10 del Convenio de Roma, que engloba la libertad de información), que excluye las medidas que alteren su contenido eliminando o borrando datos contenidos en ellos, como puede ser la eliminación de los nombres de las personas que aparecen en tales informaciones o su sustitución por las iniciales"[18].

2.2. *El derecho del interesado a la limitación del tratamiento y a la portabilidad de los datos*

Conforme expresa el art. 18 RGPD, el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos[19], entendido este

---

personales cuando se asocian a hechos que no se consideran positivos. Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, "posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. … Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse a un tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad, inserción que se vería obstaculizada por el rechazo que determinadas informaciones pueden causar en sus conciudadanos". Véase STS (Sala de lo Civil), de 5 de abril de 2016, Recurso Nº. 3269/2014. Ponente Excmo. Sr. D : Rafael Saraza Jimena.

[17] Recuérdese en este sentido, lo dispuesto por el TJCE, que al analizar los requisitos de aplicación de estos derechos, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate. Cfr. SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala), de 13 de mayo de 2014.

[18] Véase STS. Sala de lo Civil, de 15 de octubre de 2015. Nº de Recurso: 2772/2013, Ponente: Excmo. Sr. Rafael Saraza Jimena

[19] Conforme expresa el Considerando (67) , entre los posibles métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos

derecho como "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro" cuando:

> a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;
> b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
> c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;
> d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Excepcionalmente, si el interesado obtuvo el derecho a la limitación del tratamiento de sus datos, solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

En otro orden de consideraciones, un entorno digital en el aparecen nuevos retos para el derecho fundamental a la protección de los datos de carácter personal, y en el que los ciudadanos deben seguir teniendo la posibilidad de ejercer un control efectivo sobre su información personal, cobra especial relevancia jurídica el derecho del interesado a la portabilidad de sus datos personales.

En efecto, se reconoce también en el RGPD el derecho de interesado a la portabilidad de los datos, de forma que la persona tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando se cumplan dos condiciones:

> a) el tratamiento sea lícito por estar fundamentado en el consentimiento del interesado o en un contrato, y
> b) el tratamiento se efectúe por medios automatizados.

A juicio de la AEPD, el nuevo derecho a la portabilidad, representa un avance en el control de los ciudadanos sobre sus datos personales, si bien, lamenta dicha autoridad que el derecho haya quedado ligeramente mermado, de suerte que se limita la auténtica portabilidad, esto es, los datos podrán ser transferidos desde un responsable a otro, a petición del interesado y sin necesidad de la intervención de este, únicamente en los casos en que sea "técnicamente viable"[20].

Al igual que en la propuesta de Reglamento, se mantiene el criterio general de gratuidad para el ejercicio de los derechos relacionados con la protección de datos de carácter personal, incluyendo el derecho a la portabilidad de los datos; tan solo cuando se produzcan solicitudes claramente excesivas, especialmente en cuanto a su reiteración, el responsable del tratamiento podrá aplicar una tasa por facilitar la información, ahora bien,

---

personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

[20] AEPD. "El futuro de la protección de datos" en http://www.apep.es/aepd-el-futuro-de-la-proteccion-de-datos/ (última consulta: 07/06/2016)

la carga de demostrar el carácter «manifiestamente excesivo» de la solicitud deberá asumirla, en todo caso, el responsable del tratamiento.

Como se apuntaba anteriormente, el derecho a la portabilidad de los datos se concreta en dos facultades: por un lado, la posibilidad de obtener, «en un formato electrónico estructurado y comúnmente utilizado», una copia de los datos que están siendo objeto de tratamiento, formato que debe permitir que puedan seguir siendo utilizados por la persona interesada (se entiende que en otro sistema o aplicación informática). Y por otro lado, también se podrá optar por transmitir los datos a otro sistema (bien a otro proveedor o prestador de servicios), siempre que los datos sobre los que se pretenda realizar la trasmisión se encuentren sometidos a tratamiento automatizado, para lo que también se prevé que sean transmitidos en un "formato electrónico comúnmente utilizado".

Y es que a nadie se le escapan las dificultades de naturaleza práctica que pueden desprenderse del ejercicio de este derecho, cuando su necesidad no debería ser objeto de controversia, considerando el actual contexto digital, en el que extraordinaria cantidad de información personal circula por las diferentes redes sociales, o por los servicios de "cloud computing", donde a los prestadores de estos servicios se les confía el almacenamiento y procesamiento de información personal, lo que obliga a prever mecanismos que eviten, la apropiación de la información personal o la vinculación perpetua de los interesados como "rehenes digitales" a un proveedor de servicios determinado.

Inicialmente, el derecho a la portabilidad de los datos garantiza mecanismos efectivos de protección frente al desarrollo de servicios y modelos de negocio que se han generado en torno a internet, y respecto de los cuales la regulación actual no ofrece una respuesta satisfactoria para el interesado, lo que justifica el reconocimiento de estos nuevos derechos al olvido, o a la portabilidad de los datos. Ahora bien, conforme expresa el propio Considerando 68 del RGPD, el ejercicio del derecho a la portabilidad de los datos, no deberá menoscabar el derecho del interesado a obtener la supresión, reconocido en el artículo 17 del presente RGPD. De esta forma, tal derecho no se aplicará al tratamiento cuando sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Finalmente, varias son las dificultades a las que alude la doctrina cuando aborda la eficacia práctica del derecho a la portabilidad de los datos personales, y así se censura la falta de delimitación jurídica de aspectos tan importantes para el efectivo ejercicio de este derecho como: la ausencia de definición de los formatos electrónicos que han de permitir el ejercicio material del derecho a la portabilidad de los datos; la obligación de implementación de los mecanismos necesarios para facilitar el ejercicio material del derecho a la portabilidad de los datos, con lo que pueda significar de inversiones en el desarrollo de esas funcionalidades; y por último, la ausencia de una valoración racional del impacto que puede tener el derecho a la portabilidad sobre el mercado y la competitividad de los servicios electrónicos[21].

EL RESPONSABLE DEL TRATAMIENTO Y EL ENCARGADO. NOTAS DISTINTIVAS DE SUS OBLIGACIONES

1. El registro de las actividades de tratamiento

Conforme exige el art. 30 del RGPD, cada responsable y en su caso, su representante llevarán un registro por escrito de las actividades de tratamiento efectuadas bajo su responsabilidad, dicho registro deberá contener al menos la información prevista en el citado precepto, como por ejemplo la identificación del responsable, y si procede del

[21] R. MIRALLES. "El derecho de la portabilidad de los datos personales". En http://www.abogacia.es/2012/11/15/el-derecho-de-la-portabilidad-de-los-datos-personales/ (última consulta: 27/05/2016)

represente o del delegado; finalidad de tratamiento, categorías de interesados y de datos personales… Ciertamente, pueden observarse similitudes entre el registro de actividades que regula el presente RGPD, y la obligación de inscripción de los ficheros prevista en la normativa española. No obstante, aquel registro se presenta más exhaustivo, y su obligación para las organizaciones es de mera llevanza, y no de declaración ante la autoridad de control competente, al tiempo que únicamente obliga a determinadas organizaciones, o en relación con concretos tratamientos. En efecto, dicho registro deberá estar a disposición de la autoridad de control que lo solicite, luego no debe enviarse, o presentarse, si no es requerida para ello la organización.

Bien es cierto que dicha obligación no se aplicará a empresa u organización que emplee menos de 250 personas, a no ser el tratamiento puede significar un riesgo para los derechos y libertades de los interesados y no sea ocasional o incluya categorías especiales de datos personales.

Entonces la duda que se suscita, a tenor del silencio del Reglamento es si en el derecho español seguirá siendo exigible la inscripción de ficheros al amparo de la LOPD, o por el contrario, es posible interpretar que la aplicación del Reglamento significará la derogación tácita de esta obligación. Ello no obstante, resulta esclarecedor a estos efectos, y sin duda, contribuye a establecer la correcta interpretación del RGPD en este punto, lo dispuesto en el Considerando 89, cuando lamenta que la obligación general de notificación de los ficheros a la autoridad de control no haya contribuido en este tiempo a mejorar la protección de datos personales en la Unión; para afirmar, a continuación, explícitamente que dicha obligación de notificación general debe "eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas".

Cabe esperar entonces que el legislador español tome buena nota de estas observaciones, y proceda a la necesaria modificación normativa para el establecimiento de nuevas garantías, coherentes con las previsiones del RGPD, y adaptadas a los nuevos retos que para la protección de datos personales plantea la incesante evolución tecnológica.

2. La evaluación de impacto relativa a la protección de datos y la consulta previa la autoridad de control

Cuando aún no había entrado en vigor el RGPD, y en Europa se estaba trabajando con los textos de las diferentes propuestas de Reglamento, que ya auguraban la importancia de reforzar la protección de datos personales desde el momento inicial del tratamiento, la AEPD se anticipó a las previsibles disposiciones legales del RGPD, y publicó una Guía para una evaluación de impacto en la protección de datos personales[22]. Consciente la AEPD de la necesidad de fortalecer la responsabilidad proactiva de quienes tratan datos personales en los sectores público y privado defiende desde esta Guía que los aspectos de protección de datos y privacidad se tomen en consideración desde la fase inicial, desde el momento mismo del diseño de un producto o servicio. Y así, reclama que entre las herramientas más útiles para avanzar en la privacidad desde el diseño se encuentran las Evaluaciones de Impacto en la Privacidad o en la Protección de Datos[23], que se han desarrollado fundamentalmente en países anglosajones.

[22] AEPD. Guía para una evaluación de impacto en la protección de datos personales. Madrid, 2014. Véase el documento en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf (última consulta: 27/04/2016)

[23] Según definición que aporta la propia AEPD, una Evaluación de impacto "…es un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos".

Claro que en nuestro país el concepto no es nuevo, si bien no constituye conforme a nuestra normativa actualmente en vigor una obligación legal, lo que a juicio de la AEPD no impide reconocer a esta herramienta el valor de una metodología cuya aplicación mejorará las garantías para los derechos de las personas en aquellas organizaciones que las incorporen a sus sistemas y procedimientos de gestión de la privacidad, y al mismo tiempo contribuirá a generar más confianza en los usuarios y clientes de las mismas.

Por ello, si bien la evaluación de impacto ya era conocida en materia de protección de datos personales en España, especialmente, por el empeño de la AEPD, puede decirse, sin embargo, que constituye una novedad su configuración en el RGPD como obligación legal del responsable del tratamiento de datos personales. Y así, conforme expresa el art 35 del RGPD, "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales". Claro que la evaluación de impacto relativa a la protección de los datos se requerirá en particular en caso de:

> a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
>
> b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
>
> c) observación sistemática a gran escala de una zona de acceso público.

Obsérvese que el RGPD concede un protagonismo especial a las autoridades de control nacionales en la aplicación de esta herramienta; y así, corresponde a la autoridad de control establecer y publicar una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos y podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.

Será obligación del responsable del tratamiento consultar a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de datos muestre que el tratamiento implicaría un alto riesgo si el responsable no adopta medidas para mitigarlo (art. 36 RGPD).

3. Notificación de vulneración de la seguridad de los datos personales

Constituye una muestra especialmente significativa del cambio normativo en la protección de datos personales, la obligación legal que se configura, con carácter general, en el art. 33 del RGPD, y por la cual, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento lo notificará a la autoridad de control competente, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

Ciertamente esta obligación de notificar quiebras e incidencias en la seguridad de los datos personales no constituye una novedad en materia de protección de datos, habida cuenta que ya la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, con carácter sectorial[24], en su art. 4 establece la obligación de que "en caso de

[24] 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

violación de los datos personales, el proveedor de los servicios de comunicaciones electrónicas disponibles al público notificará, sin dilaciones indebidas, dicha violación a la autoridad nacional competente". Asimismo, "cuando la violación de los datos personales pueda afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el proveedor notificará también la violación al abonado o al particular sin dilaciones indebidas".

En el Derecho español, la Ley 9/2014 contempla la obligación de notificación de incidencias en el marco de tratamientos de datos relativos a comunicaciones electrónicas[25]; y con carácter general, el Real Decreto 1720/2007, de 21 de diciembre[26], por el que se aprueba el Reglamento de desarrollo de la LOPD en su art. 90 dispone que en el documento de seguridad "Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas". Es lo cierto, sin embargo, que dicha exigencia en la práctica carece de efectividad, y son pocas las organizaciones que cumplen a día de hoy con esta exigencia, ante la ambigüedad de la norma, y la falta de delimitación legal[27].

Por tanto, el RGPD presenta entonces la virtud de hacer extensiva la obligación de notificar dichas incidencias a la autoridad de control a todo tratamiento de la información, y no como hasta ahora, en relación exclusivamente con el tratamiento de datos personales relativos a comunicaciones electrónicas.

LA SEGURIDAD DE LOS DATOS PERSONALES. DE LAS EXPECTATIVAS PROFESIONALES A LAS OBLIGACIONES LEGALES

Expresa el Considerando 83 del RGPD que con el propósito de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

En concreto, el art. 32 del RGPD, prevé, que el responsable y el encargado, "teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

---

comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DOUE L 201 de 31 de julio de 2002.

[25] En ese mismo sentido se expresa el art. 41 de la Ley 9/2014 General de Telecomunicaciones, de 9 de mayo, BOE núm. 114, de 10 de mayo de 2014.

[26] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, BOE núm. 17, de 19 de enero de 2008.

[27] ABANLEX. Informe sobre la obligación legal de notificar o denunciar brechas de seguridad que afecten a datos personales (2015). Véase documento en https://www.abanlex.com/wp-content/Arbor/Informe_sobre_obligaciones_de_notificar_y_denunciar.pdf (última consulta: 20/05/2016)

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Como novedad, dispone el apartado segundo del citado precepto, que la adhesión a un código de conducta aprobado a tenor del artículo 40 RGPD o a un mecanismo de certificación aprobado a tenor del artículo 42 RGPD podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en materia de seguridad y respecto de las obligaciones con los encargado el tratamiento (véase arts. 28 y 32 del RGPD). No deja de sorprender la ambigüedad con la que se expresa el legislador, y son muchos los interrogantes que a este respecto se pueden plantear. En primer lugar, si nos atenemos a la literalidad de precepto, el código de conducta o la certificación constituyen elementos de prueba del cumplimiento de los requisitos en materia de seguridad; en segundo lugar, dicha previsión responde al giro legislativo que este Reglamento pretende introducir en las normas de protección de datos personales. Desde el fortalecimiento de la autorregulación, el autocontrol, y la implantación de medidas y garantías preventivas en el tratamiento de la información personal. Siendo esto así, mucho debe cambiar la perspectiva jurídica que a día de hoy impera en nuestro país a propósito del derecho de protección de datos personales, cuya normativa está indiscutiblemente fundamentada en el carácter represivo y sancionador de la norma nacional actualmente en vigor. Corresponde, a nuestro juicio, a partir de la aplicación del RGPD, a las Administraciones públicas realizar el esfuerzo necesario para promover una cultura preventiva en el tratamiento de los datos de carácter personal, que favorezca la consolidación de un marco de confianza en las relaciones entre el responsable del tratamiento de datos perdónales y el interesado.

1. El Delegado de Protección de Datos

Los antecedentes normativos de la figura del delegado de protección de datos o *Data Protección Officer* se encuentran en la propia Directiva 95/46/CE, de Protección de Datos, en sus artículos 18 y 20, con relación a las obligaciones de notificación a las autoridades de control, y en los llamados controles previos, si bien se establecía la existencia de un representante del responsable de tratamiento para finalidades puntuales y concretas; y en los artículos 24, 25, y 26 del Reglamento 45/2001, de 18 de diciembre, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Pero si bien puede afirmarse que esta figura en nuestro derecho constituye una novedad, no lo es para otros derechos como el alemán, que ya incluían al delegado de protección de datos en la Ley Federal de Protección de Datos de 27 de enero 1977.

Llegando al tiempo presente, y a tenor del silencio del art. 4 del RGPD, pudiera interpretarse que el legislador europeo en un descuido, ha soslayado la definición del delegado; pero es posible, también que la omisión de dicha definición obedezca a una decisión consciente y deliberada, y por la cual se pretende impedir que desde el RGPD se limite jurídicamente qué profesionales puedan ser designados delegados de protección de datos[28].

En el derecho español, si se compara esta figura con la del responsable de seguridad que regulan los artículos 95 y 109 del Real Decreto 1720/2007, de 21 de diciembre, se

[28] Así las cosas, debe subrayarse que la Comisión Europea, cuando presentó en 2012 su propuesta de Reglamento (COM (2012) 11 final, de 25 de enero), no incluyó la definición de delegado en la misma, pero sí lo hizo en el Documento de Trabajo de los servicios de la Comisión relativo a la evaluación de impacto de su propuesta (SEC (2012) 72 final, de 25 de enero). Y en dicho documento se define al delegado de protección de datos como una persona responsable del tratamiento para supervisar y monitorear de manera independiente la aplicación interna y el cumplimiento de las normas de protección de datos.

evidencia que el responsable de seguridad tiene actualmente asignadas menos funciones, menos capacidad de decisión y menos independencia dentro de la organización del responsable o encargado del tratamiento que la que ha sido reconocida al delegado de protección de datos en el RGPD.

A pesar de la incertidumbre y controvesia de los primeros textos y propuestas de Reglamento[29], finalmente el art. 37 ha delimitado los concretos supuestos en que deberá designarse un delegado de protección de datos por las organizaciones, estableciendo a tal efecto, que el responsable o encargado del tratamiento deberá nombrar un delegado siempre que: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

Se delimitan igualmente en el RGPD los principios que deben regir la actuación del delegado, y así, se señalan: el principio de independencia, de confidencialidad, de rendición de cuentas, y de no exclusividad en sus funciones. Por otra parte, su identidad debe ser comunicada a la autoridad de control y al público en general, puesto que los interesados deben tener la posibilidad de ponerse en contacto directo con el delegado, en caso de que quieran consultar cualquier asunto relativo al tratamiento de sus datos personales o ejercer cualquier derecho que les ampare. De esta forma, el delegado actuará como enlace entre el responsable del fichero o encargado del tratamiento y la autoridad de control.

A propósito del perfil profesional y del régimen jurídico a que quedará sometida su actuación, dispone el art. 37 RGPD que el delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones encomendadas por el Reglamento. Repárese en que no hay mención alguna a la necesidad de acreditación, ni certificación para el ejercicio de estas funciones; por el contrario, dicha acreditación, sin embargo, sí se exige para otras figuras reguladas en el propio RGPD. Por ello, no parece oportuno, ante el silencio normativo, exigir una certificación oficial para su ejercicio, especialmente además, cuando se trata de un ámbito tan especializado, y que requiere unas exigencias profesionales y periciales diferentes en cada sector, por lo que sin duda, a todas luces, parece mejor opción la autorregulación profesional y que la realidad profesional sitúe a cada experto en el ámbito que le corresponda.

Asimismo, el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Por todo lo anterior, la incorporación obligatoria de esta figura a determinadas organizaciones, en el marco de la aplicación del Reglamento general, ha sido considerada por los expertos en nuestro país como una fuente indudable de oportunidades profesionales para los juristas. Claro que conviene subrayar por un lado, que se trata de profesionales cuya actuación presenta carácter transversal, por lo que será precisa la combinación de conocimientos jurídicos y tecnológicos; y por otro lado, esta oportunidad profesional no está exenta de dificultades, porque requerirá de los abogados un importante esfuerzo de

[29] Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO 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 protección de datos), COM (2012) 11 final.

formación y puesta al día en las previsiones del RGPD y una incuestionable colaboración con los expertos del sector tecnológico[30].

2. Nuevas oportunidades profesionales. Los códigos de conducta y la certificación

Define el art. 40 del RGPD los códigos de conducta como aquellas normas "destinadas a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas".

Y así, conforme indica el art. 41 RGPD, sin perjuicio de las funciones y los poderes de la autoridad de control competente, podrá igualmente supervisar el cumplimiento de un código de conducta un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

Por su parte, contempla la normativa española la posibilidad de elaborar códigos tipo[31], cuya regulación establece a efectos de la necesidad de su inscripción en el actual RGPD, que se lleva en la AEPD. En efecto, dispone el art. 32 de la LOPD que "Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas…". En este sentido, a tenor de las previsiones normativas del RGPD, es sensato interpretar que dicha obligación legal de depósito persistirá en nuestro derecho, habida cuenta que conforme al art. 40 del RGPD, si el proyecto de código o la modificación o ampliación del código de conducta de que se trate no se refiere a actividades de tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

Sujeta además el RGPD a un permanente seguimiento a dichos códigos de conducta, estableciendo a tal efecto una vigilancia por la propia autoridad de control, o en su caso, por un organismo debidamente acreditado[32]. No obstante, se desprende del texto del RGPD, un régimen jurídico diferenciado entre los códigos de conducta de organismos y autoridades públicas, y los del sector particular, siendo estos últimos los únicos que pueden quedar sometidos a supervisión por organismos distintos de la autoridad de control, en los términos previstos en el Reglamento. Puede decirse entonces que el Reglamento cuando reconoce la posibilidad de que organismos acreditados puedan actuar como supervisores de códigos de conducta, abre una oportunidad profesional hasta ahora desconocida en nuestro derecho, puesto que dicha labor se encomendaba, tal y como hemos señalado, con carácter exclusivo a la AEPD[33].

De forma complementaria, el Reglamento contempla la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se trata de certificaciones voluntarias, que en ningún caso limitan la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del Reglamento. La certificación será expedida bien por los organismos de certificación acreditados (art. 43 RGPD), bien por la autoridad de

---

[30] C. FERNÁNDEZ HERNÁNDEZ, "El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales", *Diario La Ley*, núm. 8762, Sección Práctica Forense, 16 de Mayo de 2016, p.5.

[31] Para profundizar en el concepto, véase D. LÓPEZ JIMENEZ, "Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el Derecho español", *Estudios Constitucionales*, Año 11, núm. 2, 2013, pp. 575 – 614.

[32] Dispone a tal efecto el art. 41 del citado RGPD que ha de tratarse de un "organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente".

[33] C. FERNÁNDEZ HERNÁNDEZ, "El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales", *Diario La Ley*, núm. 8762, Sección Práctica Forense, 16 de Mayo de 2016.

control competente. Se prevé a tal efecto, la posibilidad de crear una certificación común, o Sello Europeo de Protección de Datos, cuando los criterios sean aprobados por el Comité. En cualquier caso, la certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes; la certificación podrá será retirada, cuando proceda porque no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

Como ya se apuntaba en líneas anteriores, la acreditación de estos organismos de certificación significará en nuestro país la creación de nuevas oportunidades profesionales en materia de protección de datos personales, que se unen a las que ofrece la creación de organismos supervisores de códigos de conducta, y a la designación del delegado de protección de datos personales.

CONSIDERACIONES FINALES

Es opinión extendida entre los expertos que el Reglamento General de Protección de Datos nace en cierto modo como una norma jurídica obsoleta, que esquiva los más recientes conflictos y cuestiones que la protección de datos personales plantea en la sociedad actual. Sirva como muestra que ilustra de dicho olvido, la ausencia de referencias explícitas en su texto a Big Data, internet de las cosas o *cloud computing*.

En otro orden de consideraciones, coincido con quienes argumentan que su aplicación se verá dificultada por la diversidad de normas especiales en materia de protección de datos personales de la UE, no olvidemos que el RGPD se publica conjuntamente con una Directiva, y que son números los textos normativos en la Unión que regulan aspectos derivados de la circulación de datos personales. Tanto es así, que el propio RGPD consciente el legislador de la dispersión legislativa en la Unión Europea, ha tenido que salir al paso de esta dificultad, intentando armonizar su texto con algunas de esas normas, tal y como se ocupa de indicar el texto del RGPD expresamente en numerosas ocasiones.

A lo anterior, se suma la necesidad de adaptar nuevamente las legislaciones nacionales en materia de protección de datos, y acomodar sus normas a los nuevos principios y previsiones del RGPD. Por otra parte, la tan ansiada y proclamada uniformidad legislativa, como elemento destacado del Reglamento, sin embargo, a nuestro juicio queda en entredicho, habida cuenta de las numerosas oportunidades en las que se deja al criterio de los Estados la adaptación y garantía de la aplicación normativa del Reglamento; así, por ejemplo, en el art. 6.2 o el art. 9. 4 del RGPD.

Igualmente, creemos que la configuración jurídica del derecho a la protección de datos personales desde unos nuevos principios y obligaciones constituye una oportunidad profesional para los expertos en protección datos; en verdad, se abre en nuestro país para estos profesionales del Derecho un elenco de posibilidades profesionales en los más diversos sectores relacionados con la creación y reconocimiento de nuevas figuras garantes de la protección de datos personales, a saber; el delegado de protección de datos, el supervisor de códigos de conducta, o las organizaciones de certificación en materia de protección de datos personales.

En definitiva, puede concluirse que al margen de las críticas ya expuestas, es opinión común que compartimos que la aprobación del RGPD era necesaria para superar una normativa europea anclada en los principios tradicionales y originarios de la protección de datos personales, y que no parece capaz de hacer frente a la nueva realidad digital, en la que son precisas renovadas herramientas y garantías para: por un lado, controlar, y garantizar la circulación de los datos personales entre países, y por otro, asegurar la tutela de los derechos y libertades en lo que respecta al tratamiento de sus datos personales. Y en este sentido, debe reconocerse al RGPD el mérito de nacer con la pretensión y el ánimo de establecer un contexto normativo de confianza que permita desarrollarse al mundo digital, al tiempo que legalmente se garantiza la seguridad jurídica y transparencia para la protección de datos personales de las personas físicas.

Para concluir, solo cabe esperar que el legislador español, tome buena nota de la evolución del derecho a la protección de datos personales, y a tenor tanto de los últimos pronunciamientos jurisprudenciales, como de la aplicación inminente de la nueva normativa europea proceda a reconocer explícitamente el elenco de derechos de protección de datos personales, cuya configuración jurídica uniforme se articula legalmente en el RGPD por vez primera en Europa.

REFERENCIAS BIBLIOGRÁFICAS

M. ARIAS POU, "Las 10 claves del Reglamento general de protección de datos (Reglamento 2016/679, de 27 de abril. DOUE del 4 de mayo de 2016)", *Diario La Ley*, núm. 8756, 2016, pp.1-7.

D. LÓPEZ JIMÉNEZ, "Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el Derecho español", *Estudios Constitucionales*, Año 11, núm. 2, 2013, pp. 575- 614.

J.L. PIÑAR MAÑÁ, "Principales novedades del Reglamento". Jornada de ENATIC sobre el Reglamento General de Protección de Datos, Madrid, 29 de abril de 2016.

C. FERNÁNDEZ HERNÁNDEZ, "El nuevo Reglamento Europeo de protección de datos: un texto complejo que abre nuevas perspectivas profesionales", *Diario La Ley*, núm. 8762, Sección Práctica Forense, 16 de Mayo de 2016.

R. MIRALLES. "El derecho de la portabilidad de los datos personales". En http://www.abogacia.es/2012/11/15/el-derecho-de-la-portabilidad-de-los-datos-personales

S. GARCÍA ROMERO, "Nuevo marco jurídico europeo en protección de datos: novedades conocidas y otras no tan conocidas", *Diario La Ley*, núm. 8691, ección Documento on-line, 28 de Enero de 2016.