# UN NUEVO ORDEN PARA PROTEGER LOS DATOS PERSONALES

## A new arrangement to protect the personal data

Por Alejandro Rodríguez Roca
Letrado de la Administración de Justicia
arguezroca@gmail.com

Artículo recibido: 14/11/18 | Artículo aceptado: 27/12/18

**RESUMEN**

La Unión Europea ha llevado a cabo un cambio significativo en el sistema de protección de datos personales. Antes del Reglamento General de Protección de Datos, cada Estado miembro tenía la posibilidad de regular la protección de la información personal, lo que significaba que las normas eran considerablemente diferentes entre ellos. Con el objetivo de contribuir a un sistema de protección reforzado la U.E. eligió la forma de reglamento comunitario para unificar los principios esenciales y los derechos de los ciudadanos europeos en esta materia. Este trabajo contiene un análisis de las novedades más importantes de la nueva normativa europea y sus consecuencias en el ordenamiento interno español.

**ABSTRACT**

The European Union has made a significant change in the personal data protection system. Until Regulation on the protection of natural persons with regard to the processing of personal data, each member state had the chance to regulate the protection of personal information what ment that the norms were significantly different among them. In order to contribute to a stronger system, the E.U. chose a Regulation to unify the basic principles and rights of European citizens in this matter. This paper conteains a review of the most significant improvements of the new European regulation and its consequences in the Spanish law system.

**PALABRAS CLAVE**

Sistema de protección de datos, reglamento comunitario, novedades, estudio académico.

**KEYWORDS**

Personal data system, European Regulation, Improvements, Academic research.

**Sumario**: 1. El RGPD, protagonista del cambio. 2. Marco jurídico anterior al RGPD. 3. Justificación de la necesidad del RGPD de la U.E. 4. Nuevo marco jurídico comunitario de protección de datos personales. Principales novedades del RGPD. 4.1. Normas comunitarias de interés. 4.2. Principales novedades del RGPD. 4.2.1. Los principios. 4.2.2. Derechos de los interesados. 4.2.3. Otras novedades destacables. 4.2.3.a. El delegado de protección de datos. 4.2.3.b. Evaluaciones de impacto. 5. Sistema actual de protección de datos en España. La nueva ley orgánica de protección de datos personales y garantía de derechos digitales. 6. Conclusiones. 7. Bibliografía.

## 1. El RGPD, protagonista del cambio

Veintiún años después de que se aprobase la Directiva 95/46/CE, de 24 de octubre de 1995, la Unión Europa aprobó el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (RGPD) 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 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 sobre protección de datos[77].

La Directiva de 1995 había quedado obsoleta a la luz de los nuevos retos que suponen los constantes cambios tecnológicos y que afectan muy especialmente a las garantías para la protección del derecho fundamental a la protección de datos personales. Este nuevo Reglamento, que entró en vigor el 25 de mayo de 2018, constituye una norma aplicable en todo el territorio de la Unión Europea, lo que implica un salto cualitativo importante en la legislación comunitaria sobre la protección de datos personales. Es la primera vez que esta materia no se regula mediante una directiva, sino en un reglamento comunitario, sin que su aplicabilidad dependa de la voluntad más o menos favorable de los gobiernos de los Estamos miembros a la transposición de su contenido. El RGPD se convierte, por lo tanto, en una nueva pieza fundamental del sistema de protección de datos[78]. Las posibilidades de que se desarrollen en normas internas determinados extremos del reglamento existen, pero no depende de ello su eficacia. El cambio de paradigma se produce porque a partir de ahora los responsables tienen como norma principal el RGPD y no las normas nacionales, como sucedía hasta su entrada en vigor. Sin embargo, la futura Ley de protección de datos que sustituirá a la actual Ley Orgánica de

[77] FERNÁNDEZ VILLAZÓN, L. A. El nuevo reglamento europeo de protección de datos. En: *Foro Nueva época*. Volumen 19, nº 1, 2016, p. 395.

[78] PLAZA PENADÉS, J. El nuevo marco normativo de la protección de datos. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

Protección de Datos (LOPD) sí podrá incluir algunas precisiones o desarrollos en materias en las que el RGPD lo permite[79].

El RGPD ha supuesto el cambio más importante de los últimos años en la legislación comunitaria sobre la protección de datos. Implica un cambio en la protección de este derecho fundamental[80]. Con esta nueva norma del legislador europeo se trata de dar una respuesta a los avances tecnológicos y las nuevas posibilidades económicas que suponen la globalización de la información y el tratamiento masivo de datos personales. Con el fin de adaptarse a las exigencias del Tratado de Lisboa, el RGPD constituye la pieza fundamental de un sistema europeo de protección de datos personales, cuyo eje es el derecho de los ciudadanos a ejercer un control efectivo sobre la información personal que les concierne[81].

**2. Marco jurídico anterior al RGPD**

Antes de la entrada en vigor del RGPD, en España regía la Ley Orgánica de Protección de Datos Personales (LOPD) y su reglamento de desarrollo[82] bajo el paraguas de la Directiva 95/46/CE. Este sistema establecía una regulación para la protección de los datos personales basada en cuatro pilares principales: unos principios de protección de datos; un elenco de derechos para los titulares de los datos; la exigencia de unas medidas de seguridad para el tratamiento de los datos personales y el establecimiento de unos requisitos formales como requisito de legalidad de ese tratamiento.

Respecto de los principios, se consagraron el de calidad, los principios de información y consentimiento, los principios de seguridad y secreto (artículos 4 a 10 LOPD). Sobre los derechos subjetivos, se reconocían los derechos de los ciudadanos en cuanto titulares de sus datos personales. Son los conocidos como derechos ARCO: Acceso, Rectificación, Cancelación y Oposición (13 a 19 LOPD). Por su parte, el Reglamento de desarrollo de la LOPD, determinaba en el Título III el procedimiento para el ejercicio de estos derechos.

Este sistema de protección establecía tres niveles de clasificación, paralelos a la sensibilidad o importancia de los datos personales que eran objeto

[79] PLAZA PENADÉS, J. El nuevo marco normativo de la protección de datos. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[80] ÁLVAREZ HERNANDO, J. El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades. En: *Aranzadi digital*. Cizur Menor: Ed. Aranzadi, nº 1, 2017.

[81] BLUME, P. Will it be a better world? The proposed EU Data Protection Regulation. En: International Data Privacy Law, nº 2, 2012, p. 130.

[82] España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

de tratamiento. De forma que, las medidas de seguridad exigidas debían ser correlativas a la clasificación del dato personal según las categorías previstas.

Como último pilar sobre el que se construye la protección de la información personal aparecía la exigencia de determinados formalismos que ampararan la legalidad de la recogida y tratamiento de la información personal. Diferenciándose entre ficheros de titularidad privada y pública. Los ficheros de titularidad privada, es decir, aquellos en los que el responsable de tratamiento es una empresa o un particular, debían inscribirse en el registro de la AEPD (artículo 25 LOPD). Mientras que los de titularidad pública requerían, además, su publicación en una orden general, de acuerdo con lo que establecía el artículo 20 LOPD (artículo 54 RDLOPD).

Es necesario mencionar que llegado el año 2000, el TC pondría fin a las dudas sobre la naturaleza del derecho a la protección de datos como derecho fundamental y autónomo del derecho a la intimidad, consolidando una línea jurisprudencial que venía consolidándose desde hacía años. Para el TC, el derecho a la protección de datos es un derecho fundamental que garantiza a la persona el control sobre sus datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o un uso lesivo para la dignidad y los derechos de los afectados; de este modo, este derecho se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención[83]. Un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a su titular para decidir cuáles de esos datos se pueden proporcionar a un tercero, sea el Estado o un particular, o cuáles puede ese tercero recabar, e igualmente permite al individuo saber quién posee tales datos y para qué, pudiendo oponerse a su posesión o uso[84, 85].

Desde entonces entendemos por derecho a la protección de datos el derecho de todo ciudadano a disponer de sus datos personales y conocer el tratamiento de los mismos que realicen otras personas. Se trata de garantizar y proteger el control de todo sujeto de derecho de sus datos personales.

Hasta la entrada en vigor del RGPD, se puede decir que el sistema español de protección de datos era bastante garantista. Sin embargo, el principal obstáculo con el que se encontró fue su propia burocratización y la falta de adaptación a la vertiginosa evolución del empleo de las nuevas tecnologías en todos los ámbitos de la vida pública y privada. En clave global nos encontrábamos además con una fragmentación normativa que hacía que en

[83] España. Tribunal Constitucional. Sentencia núm. 94/1998, de 4 de mayo.

[84] RUBIO TORRANO, E. Del Reglamento europeo a la nueva Ley Orgánica de Protección de Datos. En: *Revista Doctrinal Aranzadi Civil-Mercantil*. Cizur Menor: Ed. Aranzadi, nº 6, 2018.

[85] España. Tribunal Constitucional. Sentencia núm. 292/2000, de 30 de noviembre.

el propio territorio de la U.E. hubiera normas heterogéneas e incompatibles entre los diferentes Estados miembros.

**3. Justificación de la necesidad del RGPD de la U.E.**

El propio RGPD se pronunció sobre la necesidad de la nueva norma en su considerando sexto, según el cual "la rápida evolución tecnológica y la globalización han plasmado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial".

La heterogeneidad de normas para la protección de los datos personales se convirtió en un problema que requería una solución europea. El propio Tribunal de Justicia de la Unión Europea (en adelante TJUE), en la conocida como Sentencia Lindqvist[86], advirtió las diferencias entre los regímenes nacionales aplicables al tratamiento de datos personales afectaban gravemente al funcionamiento del mercado interior. Estas diferencias en las regulaciones de los Estados miembros dieron lugar a incongruencias que hicieron que la Comisión Europea se planteara la necesidad de una regulación unitaria y armonizada de protección de datos en todo el territorio de la Unión, reduciendo la capacidad de decisión de los legisladores nacionales[87].

Lo que el TJUE estaba advirtiendo, por lo tanto, era la necesidad alcanzar el objetivo común perseguido por la Directiva 95/46/CE para lograr un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad[88]. Sin embargo, esta Directiva no ha resultado ser un instrumento suficiente porque, a pesar de estar consagrado el derecho a la protección de datos personales en el artículo 8 de la Carta Europea de Derechos Fundamentales**,** no se ha conseguido un mismo nivel de protección en los ordenamientos internos de los Estados miembros[89]. En este sentido, no ha logrado evitar la fragmentación en la aplicación en la Unión del derecho

[86] Tribunal de Justicia de la Unión Europea. Caso Lindqvist. Sentencia de 6 de noviembre de 2003.

[87] SOLAR CALVO, P. Nueva regulación europea en protección de datos. Urgente necesidad de una normativa nacional. En: *Revista Aranzadi Unión Europea*. Cizur Menor: Ed. Aranzadi, nº 7. 2018.

[88] Tribunal Europeo de Derechos Humanos (Gran Sala). Sentencia de 6 de noviembre de 2003.

[89] DÍAZ DÍAZ, E. El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. En: *Revista Aranzadi Doctrinal.* Cizur Menor: Ed. Aranzadi, nº 6, 2016.

fundamental a la protección de datos de carácter personal, ni tampoco la inseguridad jurídica ni la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea[90].

El nuevo ámbito de la economía digital requiere un marco jurídico coherente y armonizado que consiga su adecuado desarrollo permitiéndole aprovechar todo su potencial, pero, a la vez, de manera respetuosa con las garantías que protegen derechos fundamentes como el derecho a la protección de datos personales en veintiocho. La integración económica y social que se ha producido gracias al crecimiento del mercado interior europeo ha dado lugar a un incremento de los flujos transfronterizos de información que tiene que reconocerse como potenciales peligros para el derecho que aquí nos ocupa. Los cambios tecnológicos demandaban una nueva regulación adaptada a los cambios producidos, adaptada a la nueva era tecnológica[91].

Estas circunstancias fueron cultivando la necesidad de actualizar este sistema de protección de datos personales a escala supranacional. Ello implicaba ir más allá de la propia Directiva 95/46/CE, que había quedado obsoleta a la luz de los nuevos retos que plantean los cambios tecnológicos, especialmente en lo relativo a la protección de los datos personales. Así es como llegamos a la aprobación del 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 (RGPD) y por el que se deroga la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 sobre protección de datos. Esta norma constituye la pieza principal de un sistema de protección de datos personales que es aplicable a toda la Unión Europea.

Se hacía necesario un nuevo cuerpo legislativo común en todos los Estados miembros, estableciendo una mayor seguridad jurídica y una igualdad de condiciones en un mercado único digital europeo. Por ello se entiende que la fórmula del Reglamento, y no de cualquier otro instrumento o acto jurídico, es la idónea para la consecución de dichos objetivos[92].

---

[90] DÍAZ DÍAZ, E. El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. En: *Revista Aranzadi Doctrinal.* Cizur Menor: Ed. Aranzadi, nº 6, 2016.

[91] PANIZA FULLANA, A. Una nueva era en la privacidad y las comunicaciones electrónicas: la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas. En: *Revista Doctrinal Aranzadi Civil-Mercantil*. Cizur Menor: Ed. Aranzadi Thomson Reuters, nº 7, 2017.

[92] GARCÍA ROMERO, S. Nuevo marco jurídico europeo en protección de datos: novedades conocidas y otras no tan conocidas. En: *Diario La Ley*. Madrid: Ed. La Ley, nº 8691, 2016.

Con este nuevo instrumento, el legislador europeo, quiere solucionar los problemas que el sistema anterior suponía para el mercado interior de la UE y el desarrollo de actividades económicas, tratando de que las autoridades de control de los diferentes países persigan los incumplimientos en materia de protección de datos como consecuencia de la heterogeneidad que se daba entre los diferentes ordenamientos[93].

Se perfila una nueva normativa cuya finalidad es promover el mercado único digital y atender sus necesidades. Por todo ello se puede concluir que todas las reformas pretenden alcanzar el objetivo de actualizar la normativa existente que había quedado obsoleta frente a nuevos desarrollos tecnológicos como el Big Data, el *cloud computing*, la creación de perfiles, las redes sociales o el desarrollo del mercado digital; y, por otro lado, el objetivo de adaptarse al fenómeno de la globalización de la información en los nuevos mercados. La aprobación del nuevo RGPD responde también a la necesidad de crear un marco jurídico que elimine la heterogeneidad de normas obligaciones y responsabilidades, de manera que se consiga una mayor seguridad jurídica, así como mayores garantías para los ciudadanos para la protección de su derecho fundamental a la protección de datos personales[94].

## 4. Nuevo marco jurídico comunitario de protección de datos personales. Principales novedades del RGPD

### 4.1. Normas comunitarias de interés

A nivel comunitario son dos las normas principales que componen el nuevo sistema de protección. En primer lugar, el Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que constituye la norma básica del sistema y que se estudiará a continuación, sin embargo no se pueden obviar una serie de directivas entre las que cabe destacar la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales; ejecución de sanciones penales, y a la libre circulación de dichos datos, por la

[93] ÁLVAREZ HERNANDO, J. El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades. En: *Aranzadi digital.* Cizur Menor: Ed. Aranzadi, nº 1, 2017.

[94] GARCÍA ROMERO, S. Nuevo marco jurídico europeo en protección de datos: novedades conocidas y otras no tan conocidas. En: *Diario La Ley*. Madrid: Ed. La Ley, nº 8691, 2016.

que se deroga la Decisión Marco 2008/977/JAI del Consejo[95]. Ésta es llamada doble vía para la protección de la información personal.

La directiva europea para la protección de los ficheros policiales, la ya mencionada Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, regula por primera vez los datos de las víctimas, testigos y sospechosos y demás sujetos que estén relacionados con la investigación criminal, juicio penal o ejecución de sentencia, en su caso. Pretende precisar los derechos de estos sujetos y establecer los límites de la transmisión de datos personales. La directiva contiene prevenciones para evitar riesgos para la seguridad pública y promueve una cooperación fluida entre las autoridades policiales y judiciales de los distintos Estados miembros[96].

Esta norma se estructura en diez capítulos: Provisiones Generales, Principios, Derechos del Titular de los Datos, Responsable de Tratamiento y Usuarios, Transferencia Internacional de Datos, Autoridad Nacional de Supervisión, Cooperación, Régimen de Sanciones, y los de Actos de Delegación e Implementación y Provisiones Finales. En el primero encontramos la definición del objeto y ámbito de aplicación de la directiva, circunscritos al tratamiento de datos en la investigación criminal, quedando fuera los relativos a la seguridad nacional y los tratamientos llevados a cabo por las propias instituciones europeas.

La doctrina destaca la distinción que hace la norma entre las diferentes categorías de datos y su diferente tratamiento según se trate de datos personales de sospechosos, condenados, víctimas, terceros u otros. Del contenido cabe destacar que los principios que establece son similares a los que reconocía nuestra LOPD. En la directiva se asume también el concepto de datos especialmente protegidos y en cuanto a los derechos del titular se concretan conceptos, como la cancelación y el bloqueo de datos y se determina el periodo previsto de conservación de los datos. Y en cuanto a los sujetos, los responsables, además de remitir a las obligaciones generales se concretan las medidas de seguridad que se deben implementar. Asimismo, se establece la necesidad de consultar a la autoridad de supervisión nacional con carácter previo al tratamiento de determinadas clases de datos personales. Adicionalmente, establece la obligación de notificar las brechas de seguridad a la autoridad de control y al sujeto o sujetos afectados; incorpora la figura del

[95] SOLAR CALVO, P. La doble vía europea en protección de datos. En: *Diario La Ley*. Sección Doctrina. Madrid: Ed. La Ley, nº 7832, 2012.

[96] SOLAR CALVO, P. Los datos personales en la investigación criminal. En: *Revista de la Guardia Civil*. Sección Formación. Madrid: Dirección General de la Guardia Civil, nº 817, 2012.

Oficial de Protección de Datos y simplifica los supuestos de transferencia internacional[97].

Tampoco podemos dejar de mencionar la Directiva 2016/681, de 27 de abril relativa a la utilización de datos del registro de nombre de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. El objeto de esta Directiva es regular la transferencia de los datos PNR de los pasajeros de vuelos internacionales, siendo obligatorio para las compañías aéreas que los faciliten a las autoridades de los Estados miembros, ya sean vuelos que entren o salgan de la Unión Europea. También permite, aunque no de manera obligatoria, que los Estados miembros puedan recabar datos PNR de vuelos internos en la Unión Europea. Además, los Estados miembros tendrán que crear una Unidad de Información sobre pasajeros que recibirá y registrará los datos PNR obtenidos de las compañías aéreas, que sólo podrán ser tratados para la finalidad de prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves[98].

### 4.2. Principales novedades del RGPD

Entre las principales novedades del RGPD cabe destacar el carácter ya mencionado anteriormente de norma de aplicación directa en todos los Estados Miembros sin necesidad de transposición, de acuerdo con el artículo 288 del Tratado de Funcionamiento de la Unión Europea. Constituye una única norma para todo el territorio de la Unión homogeneizando y simplificando el sistema de protección a nivel supranacional; incorpora además el sistema de ventanilla única, a través del cual se establece un único supervisor según el lugar donde radique el establecimiento principal; se incorpora el concepto de privacidad desde el diseño, en virtud del cual se incorpora la protección de datos personales desde los primeros pasos de desarrollo de productos y servicios. Se introduce la necesidad de notificar a los interesados las violaciones de seguridad que se hayan producido; la consulta previa a la autoridad de control en caso de identificarse riesgos en el tratamiento; la introducción de la figura del Delegado de protección de datos y del reconocimiento de nuevos derechos para los interesados como el derecho al olvido y a la portabilidad de datos[99].

---

[97] SOLAR CALVO, P. Nueva regulación europea en protección de datos. Urgente necesidad de una normativa nacional. En: *Revista Aranzadi Unión Europea.* Cizur Menor: Ed. Aranzadi, nº 7, 2018.

[98] BOTANA GARCÍA, G. A. Crónica anunciada de un Reglamento de Protección de Datos en la Unión Europea. En: *Actualidad Civil.* Madrid: Ed. Wolters Kluwer, nº 6,2016.

[99] RODRÍGUEZ BALLANO, S. Año nuevo, Reglamento de Protección de Datos nuevo. En: *Actualidad Jurídica Aranzadi.* Cizur Menor: Ed. Aranzadi, nº 915, 2016.

Se puede decir que el RGPD configura un nuevo sistema de protección de datos más moderno, menos burocratizado y más homogéneo, aunque la remisión a las normativas internas de los Estados para desarrollar determinados aspectos puede comprometer el tan ansiado objetivo de la unificación de criterios. Se trata de normas que basan el uso de datos de carácter personal en el consentimiento previo del usuario, salvo excepciones, previa información sobre el tratamiento. Pero ahora, ya se va un poco más allá, previendo fórmulas de salvaguarda de los derechos de los usuarios *ex ante* con la privacidad desde el diseño y las configuraciones de privacidad de los navegadores[100].

Los europeos tendrán un mayor control de sus datos personales mientras se promueve la circulación de la información y las posibilidades de crecimiento económico. Se refuerzan los derechos de los interesados, implicando a su vez un mayor nivel de responsabilidad y cuidado por parte de entidades públicas y privadas[101].

Sin embargo, la ambición del Reglamento no ha impedido que esté lleno de excepciones y conceptos jurídicos indeterminados que hacen que en ocasiones se complique la tarea de su interpretación. Por ello, se pone también en duda que pueda ser considerado un reglamento homogéneo para todos los países.

Entre los inconvenientes que se detectan al RGPD destaca la sensación de que la norma nace ya obsoleta. Se le atribuye una suerte de falta de previsión de la velocidad a la que la tecnología cambia las circunstancias por las que se puede comprometer el derecho fundamental a la protección de datos. Parece que se ha perdido una ocasión para adaptar completamente la norma al entorno digital para permitirla envejecer bien. Hay quien entiende que el reglamento deja en manos de los propios interesados la efectividad del sistema de protección a través de la reclamación de sus derechos cuando para ellos se requiere de un nivel de formación que aún no se le puede exigir al ciudadano medio. Asimismo, se critica al reglamento el hecho de estar redactado pensando más en la gran empresa y no al pequeño y mediano empresario, que, para el cumplimiento, a pesar de la eliminación de ciertas trabas burocráticas y la adaptación al riesgo específico que su actividad presente, estará obligado a solicitar y abonar asesoramiento técnico.

---

[100] PANIZA FULLANA. A. Una nueva era en la privacidad y las comunicaciones electrónicas: la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas. En: *Revista Doctrinal Aranzadi Civil-Mercantil.* Cizur Menor: Ed. Aranzadi Thomson Reuters, nº 7. 2017.

[101] PADÍN, A. Reglamento General de Protección de Datos de la UE: una visión desde el período de adaptación. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 925,2016.

Si analizamos la estructura del RGPD, nos encontramos con que se trata de una norma extensa. Está compuesta por 173 considerandos previos y 99 artículos, estructurados en 11 capítulos: Capitulo I. Disposiciones generales; Capitulo II. Principios; Capítulo III. Derechos del interesado; Capítulo IV. Responsable del tratamiento y encargado del tratamiento; Capítulo V. Transferencias de datos personales a terceros países u organizaciones internacionales; Capítulo VI. Autoridades de control independientes; Capítulo VII. Cooperación y coherencia; Capítulo VIII. Recursos, responsabilidad y sanciones; Capítulo IX. Disposiciones relativas a situaciones específicas de tratamiento; Capítulo X. Actos delegados y actos de ejecución; Capítulo XI. Disposiciones finales[102].

De acuerdo con su artículo segundo, el RGPD se aplica 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[103]. Quedan fuera de su ámbito de aplicación las actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión, la actividad de las autoridades con fines de prevención o investigación de delitos o de protección de la seguridad pública y el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas[104].

El sistema para determinar su aplicación territorialmente es, según su artículo 3, la regla del establecimiento. Es decir, que el reglamento se circunscribe al tratamiento de datos personales llevados a cabo en el contexto de las actividades del establecimiento del responsable o del encargado dentro de la U.E., sin perjuicio de que el tratamiento pueda llevarse a cabo dentro o fuera de la Unión. O incluso cuando el tratamiento de los datos se realice por parte de un responsable o encargado no establecido en la Unión y afecte a residentes en ella, siempre que estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a éstos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. El RGPD se aplica también, por lo tanto, al tratamiento de datos que se realice fuera de las fronteras de la U.E.

---

[102] DAVARA RODRÍGUEZ, M. A. Una primera aproximación al Reglamento europeo de protección de Datos y su incidencia en el tratamiento de datos de carácter personal de las Administraciones Publicas. En: *Actualidad Administrativa*. Madrid: Ed. Wolters Kluwer, nº 4, marzo, 2108.

[103] RODRÍGUEZ ESCANCIANO, S. *El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679*. Ed. Aranzadi. 2017.

[104] ÁLVAREZ HERNANDO, J. El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades. En: *Aranzadi digital*. Cizur Menor: Ed. Aranzadi, nº 1, 2017.

En cuanto a las definiciones se refiere, al igual que haría la LOPD de 1999, en el RGPD también se establecen las definiciones de los conceptos elementales del sistema de protección de datos, aunque a salvo de alguna modificación de estilo o accesoria, no varían las definiciones tradicionales de fichero, responsable de tratamiento, encargado del tratamiento o la de tercero. No obstante, el RGPD amplía la definición de dato personal, al considerar expresamente los datos de localización, un identificador en línea o un nombre de identificación, como datos susceptibles de identificar o hacer identificable a una persona[105].

De acuerdo con el artículo 4 del RGPD establece que se considera tratamiento de datos personales aquel que se lleve a cabo con datos relativos a una persona física identificada o que pueda ser identificable. No obstante, "a la luz de lo que se indica en el Considerando 15 del RGPD y de que su artículo 2.1 replica el artículo 3.1 de la Directiva 95/46/CE el mero hecho de que un dato personal figure en una base de datos no significa que se esté llevando a cabo un tratamiento de ese dato. Podríamos distinguir en este punto, quizá, entre lo que podríamos denominar tratamiento activo o dinámico de datos personales y tratamiento pasivo o estático de datos personales, quedando referido, en principio, el tratamiento al que se refiere el RGPD, al primero de ellos únicamente[106].

#### 4.2.1. Los principios

En materia de principios, los cambios introducidos por el reglamento son notables. Viene a consolidar principios esenciales de la protección de datos que ya eran conocidos, pero añade a la lista principios nuevos. Anteriormente, la Directiva 95/46/CE en sus artículos 6 y 7 distinguía entre los principios relativos a la calidad de los datos y los relativos a la legitimación. Sin embargo, el reglamento los regula como principios relativos al tratamiento, donde incluye el tradicional principio de calidad y otros nuevos como el de minimización, el de limitación del plazo de conservación y el principio de responsabilidad proactiva. También destaca el nuevo principio de integridad y confidencialidad[107]. Veamos un poco más detenidamente los aspectos más destacables.

***1. Licitud, lealtad y transparencia.*** En virtud de este principio, los datos personales deberán ser "tratados de manera lícita, leal y transparente en

[105] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad Civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[106] MARTÍN, B. Sobre el ámbito de aplicación material del reglamento general de protección de datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 943, 2018.

[107] RODRÍGUEZ ESCANCIANO, S. *El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679*. Ed. Aranzadi. 2017.

relación con el interesado". De esta manera el reglamento vincula el principio de licitud al principio de transparencia, que queda, a su vez, vinculado al derecho del titular de los datos a estar informado de manera clara e inequívoca sobre dicho tratamiento. El interesado debe poder conocer en todo momento quién, cómo y para qué están tratando su información personal, así como cuáles son los datos que están siendo tratados y si ha habido incidencias que afecten a sus derechos como titular de los mismos.

Con el RGPD se refuerza, por tanto, el derecho a la información, tanto en el supuesto de que los datos se recaben directamente del interesado como si los datos se obtienen de otra fuente ya que, además de la información obligatoria ya establecida en la normativa española actualmente vigente, se tiene que facilitar la información respecto otros elementos (base jurídica del tratamiento, la intención de realizar transferencias internacionales, el plazo de conservación de los datos, el derecho a la portabilidad de los datos…). Este principio de transparencia conlleva un aumento de la información que el responsable del fichero debe facilitar al titular de los datos previamente a su obtención o tratamiento si se van a emplear para una finalidad distinta de aquella que motivó su recogida[108,109].

De acuerdo con el considerando 39 "toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento". De esto se deriva que los avisos legales y las políticas de privacidad deban proporcionarse de manera más completa que antes, a la vez que de forma más simple e inteligibles para facilitar su comprensión.

Por ello, se entiende que para que el tratamiento sea leal, lícito y transparente, debe proporcionarse la información de forma comprensible y accesible.

---

[108] MAYOR GÓMEZ, R. *Contenido y novedades del reglamento general de protección de datos de la U.E. (reglamento UE 2016/679, de 27 de abril de 2016)*. En: *Revista digital Gabilex.* Toledo: Ed. Vicepresidencia Primera Junta Comunidades Castilla la Mancha, nº 6, 2016, p 11.

[109] BIURRUN ABAD, F. Novedades del nuevo Reglamento de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 916, 2016.

El RGPD exige, además, que todos los tratamientos de datos personales sean leales, lo que significa que se proscriben los tratamientos que no sean legítimos, de forma que los datos personales deben ser tratados sólo si existe un fin legítimo para el tratamiento de los datos personales.

***2. Limitación de la finalidad.*** Este principio pretende que los objetivos perseguidos sean determinados, explícitos y legítimos. Según el artículo 5.1.b. del RGPD los datos personales, consecuentemente, no podrán ser tratados ulteriormente de manera incompatible con dichos fines. De acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales. No se trata por lo tanto de limitar finalidades distintas, sino finalidades incompatibles. Así especifica el considerando 39, los datos personales deben de ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Por este motivo el RGPD aclara que se pueden realizar tratamientos de datos con finalidades distintas de las recogidas siempre y cuando se dé una serie de presupuestos. Así en su artículo 6.4 se establece que el responsable de tratamiento, para determinar si la nueva finalidad es compatible con la originaria, deberá tener en cuenta circunstancias tales como la relación que pueda haber entre las distintas finalidades de tratamiento; el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento; la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de acuerdo con el artículo 10; las posibles consecuencias para los interesados del tratamiento ulterior previsto; así como la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

El reglamento crea nuevas categorías especiales de datos personales entre las que se incluyen algunas ya conocidas (como el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, datos relativos a la salud o a la sexualidad, y las infracciones o condenas) y se añaden los datos genéticos y los datos biométricos, cuyo tratamiento se prohíbe con carácter general siempre que se lleve a cabo con el fin de identificar de forma única una persona»[110].

***3. Minimización de datos***: este principio implica que los datos tratados deben ser en todo caso "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". Es el principio análogo al

[110] BIURRUN ABAD, F. Novedades del nuevo Reglamento de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 916, 2016.

tradicional de proporcionalidad que recogía la LOPD, en virtud del cual se establecía que los datos debían ser adecuados pertinentes y no excesivos en relación con la finalidad y el ámbito para la que fueron recabados. No obstante, existe una diferencia relevante y es que el RGPD no limita el tratamiento por el exceso sino por su necesidad. Este criterio de la necesidad ya fue establecido por la jurisprudencia del TC de tal manera que, si el objetivo podría alcanzarse sin realizar un tratamiento de datos, éstos no deberían ser tratados. Este principio trata de limitar el uso de datos que no sean considerados como adecuados. Como también, pertinentes y limitados en relación con las finalidades para las cuales sean tratadas. Esta limitación del tratamiento según el criterio de la necesidad debe ser ponderado teniendo en cuenta tanto el criterio cuantitativo sobre el volumen de datos almacenados, como el cualitativo sobre qué categoría de datos son objeto de tratamiento. En este sentido el considerando 39 establece que "los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios".

***4. Exactitud.*** Los datos deberán ser exactos y, si fuera necesario, actualizados. Deberán adoptarse las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. En este sentido establece también el considerando 39 que "deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos". Se corresponde con el principio tradicional de calidad de los datos. El responsable de tratamiento deberá actuar con la diligencia necesaria para que los datos sean correctos, completos y actuales.

***5. Limitación en el plazo de conservación.*** De acuerdo con este principio, los datos deben ser "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales". La LOPD establecía que los datos deberán ser cancelados cuando dejen de ser útiles para la finalidad en la que fueron recabados, sin embargo, el RGPD además de limitar el plazo de conservación impone al responsable la obligación de incluir plazos para la supresión o revisión periódica. Así el considerando 39 indica que "para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica."

Este principio pretende reforzar el control del titular de los datos sobre la conservación de los mismos a través de la limitación del uso de datos personales temporalmente, obligando a cesar en su tratamiento cuando estos dejan de ser necesarios para la finalidad perseguida. Esta necesidad surgió como consecuencia del frecuente desconocimiento de los diferentes plazos de conservación.

***6. Principio de responsabilidad proactiva (accountability).*** Este principio constituye una de las principales novedades del RGPD. Impone al responsable, y al encargado del tratamiento, estar en condiciones de demostrar que cumple con las previsiones normativas en materia de protección de datos de carácter personal. Recae, por lo tanto, sobre el cumplimiento de las obligaciones que establece el reglamento. De manera que la responsabilidad no se salva sólo con no incumplir las normas sobre protección de datos, sino que hay que demostrar que se están cumpliendo[111].

De acuerdo con el artículo 24.1 RGPD, "el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".

Por lo tanto, se hace obligatorio implementar mecanismos que permitan acreditar que se han adoptado todas las medidas necesarias para tratar los datos personales como exige la norma mediante el establecimiento de políticas internas de protección de datos, procedimientos de seguridad, controles periódicos que aseguren el cumplimiento. En este sentido, el RGPD establece una serie de normas que impone obligaciones que tienden al cumplimiento preventivo de sus prescripciones. Entre ellas el principio que se estudia a continuación, el de privacidad desde el diseño o por defecto. Pero además nos encontramos con que el artículo 32 RGPD establece que "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, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (...)".

Desde la entrada en vigor del RGPD, todo al que le sea aplicable, debe acreditar que ha evaluado, y en caso necesario, rediseñado adecuadamente su sistema de tratamiento; que las medidas de seguridad implementadas son adecuadas y eficaces; y que se está aplicando una política interna de protección de datos que establece obligaciones claras, acciones concretas, y con designación de responsables de su cumplimiento[112].

La evolución del modelo de protección de datos que se ha producido responde a un cambio en el que se pasa de un modelo basado fundamentalmente en el control de cumplimiento a un nuevo modelo que

[111] BIURRUN ABAD, F. Novedades del nuevo Reglamento de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 916, 2016.

[112] BIURRUN ABAD, F. Accountability o responsabilidad activa en el Reglamento General de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 927, 2017.

descansa en el principio de responsabilidad activa. El RGPD exige al responsable o al encargado de tratamiento una previa valoración del riesgo que pudiera generar el tratamiento de los datos personales que sirva para determinar qué medidas se han de adoptar para prevenir el perjuicio o la lesión del derecho[113]. En el cambio de sistema de *accountability* que impone el Reglamento conlleva importantes multas pecuniarias en caso de incumplimiento de sus prescripciones, sin perjuicio de la responsabilidad civil por el daño que pueda ocasionarse al titular de los datos[114].

***7. Principio de protección de datos por defecto y desde el diseño.*** Entre los aspectos más novedosos del reglamento se encuentra este concepto de *privacy by design* (privacidad en el diseño) y *privacy by default* (privacidad por defecto). Este concepto está configurado como un principio de carácter preventivo. La privacidad desde el diseño conlleva la necesidad de prevenir y de anticipar cualquier invasión de la privacidad en el momento de la concepción de un producto o servicio. De acuerdo con este principio se deberán adoptar medidas que garanticen el cumplimiento de la norma desde los comienzos de cualquier proyecto, empresa, producto, servicio o actividad que implique tratamiento de datos personales, como regla y desde el origen[115].

En efecto, se deberán tener en cuenta *ab initio* cuestiones tales como el deber de información, la prestación del consentimiento al tratamiento de datos de carácter personal o las preceptivas medidas de seguridad. Por otra parte, la privacidad por defecto obliga a proteger de manera predeterminada los datos de carácter personal de los interesados sin que estos tengan que realizar ninguna acción para que su privacidad se vea protegida.

Se considera que constituye la clave de bóveda del sistema de protección de datos porque establece que teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de

[113] RUBIO TORRANO, E. Del Reglamento europeo a la nueva Ley Orgánica de Protección de Datos. En: *Revista Doctrinal Aranzadi Civil-Mercantil*. Cizur Menor: Ed. Aranzadi, nº 6, 2018.

[114] PLAZA PENADÉS, J. Implementando el nuevo Reglamento General Europeo de Protección de Datos. En: *Revista Aranzadi de Derecho y Nuevas Tecnologías*. Cizur Menor: Ed. Aranzadi, nº 43, 2017.

[115] RODRÍGUEZ BALLANO, S. Año nuevo, Reglamento de Protección de Datos nuevo. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 915, 2016.

datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados[116].

Éstos son los principios que prevé el nuevo RGPD los cuales son una versión mejorada de los ya regulados en la LOPD. Y por supuesto se convierten en obligaciones para el responsable del tratamiento. Podríamos decir que el más significativo de los principios es el de transparencia. El RGPD establece la transparencia como una de sus banderas, puesto que es el camino hacia la excelencia en la protección de los derechos de los interesados.

Cuanto más transparente sea el responsable del tratamiento con el titular de los datos, mejor se estará implementando la nueva normativa y más control tendrá éste sobre sus datos personales.

#### 4.2.2. Derechos de los interesados

En cuando a los derechos de los titulares, nos encontramos con que el RGPD da un paso más y supera la ya clásica construcción de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). El reglamento, en desarrollo de los principios anteriores, enumera y amplía los derechos que hasta ahora se les reconocían a los titulares de los datos[117]. Así nos encontramos ahora con los derechos de Transparencia (artículo 12); Información (artículos 13 y 14); Acceso (artículo 15); Rectificación (artículo 16); Supresión o derecho al olvido (artículo 17); Limitación del tratamiento (artículo 18); Portabilidad de datos (artículo 20) y Oposición (artículo 21).

Para proteger de manera efectiva el derecho fundamental a la protección de datos personales era necesario reforzar algunos derechos, como el derecho a la información, y crear nuevos derechos[118]. Podemos resumir las principales novedades a este respecto en tres cuestiones principales. La reformulación del requisito consentimiento del interesado, el reconocimiento del derecho a la portabilidad de los datos y, en tercer lugar, en estrecha relación con la disponibilidad efectiva sobre los datos personales protegidos, se incorpora el denominado derecho al olvido[119].

---

[116] CAMPOS ACUÑA, M. C. La política de seguridad en el RGPD. Análisis de riesgos y Evaluación de Impacto. La aplicación del Esquema Nacional de Seguridad. Esta doctrina forma parte del libro "Administraciones Públicas y Protección de Datos: adaptación al RGPD. En: *Actualidad Civil*. Madrid: Ed. Wolters Kluwer. 2018.

[117] FERNÁNDEZ VILLAZÓN, L. A. El nuevo reglamento europeo de protección de datos. En: *Foro Revista de Ciencias Jurídicas y Sociales*. Madrid: Universidad Complutense de Madrid, Facultad de Derecho, volumen 19, nº 1,2016, p. 398.

[118] RECIO GAYO, M. Los nuevos y los renovados Derechos en Protección de Datos en el RGPD, así como sus limitaciones. En: *Actualidad Civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[119] ALEJANDRO PADÍN. Reglamento General de Protección de Datos de la UE: una visión desde el período de adaptación. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 925, 2016.

La nueva norma pretende ampliar el control que los titulares tengan de sus propios datos y para eso el RGPD utiliza el requisito del consentimiento como instrumento principal. El consentimiento se convierte por tanto en "la llave de todo tratamiento de datos personales. Salvo las excepciones legalmente previstas, el consentimiento da acceso al tratamiento de nuestros datos personales, lo legitima, y permite hablar de un mayor o menor control de los mismos, esto es, haber sido conscientes o no de que nuestros datos están siendo tratados"[120]. Actúa pues como un mecanismo de legitimación para el lícito tratamiento de datos personales[121].

A partir de mayo de 2018, el consentimiento que presta el titular se fortalece a través de mayores garantías puesto que ahora deberá ser libre, específico, informado e inequívoco. Aunque tal y como se ha advertido, no en todos los supuestos se requiere el consentimiento puesto que se contemplan cuatro excepciones, entre las que se encuentra el caso de que los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias[122]. Pero en el caso de aquellos supuestos en que sí se requiera del consentimiento del interesado, éste ha de obtenerse explícitamente, descartándose fórmulas hasta ahora permitidas que diluían la capacidad de disposición del interesado sobre sus propios datos.

El responsable del tratamiento de los datos deberá "poder probar que el titular consintió el tratamiento de sus datos y además, "la obligación de información aparece estrechamente unida al aspecto clave del consentimiento del afectado, no sólo porque el consentimiento ha de ser informado, sino también porque en ocasiones la mera información, unida a la posibilidad de que el usuario manifieste su negativa, puede ser determinante de que concurra el consentimiento (cuando no haya manifestado el usuario su voluntad en contra)"[123].

El segundo de los instrumentos para el fortalecimiento de los derechos de los particulares es el derecho a la portabilidad de los datos. A través de él se pretende que los ciudadanos puedan acceder de manera más fácil a sus propios datos a través del reconocimiento de la facultad de transferir sus datos

[120] ARENAS RAMIRO, M. *Reforzando el ejercicio del derecho a la protección de datos personales, Hacia un nuevo derecho europeo de protección de datos.* Valencia: Ed. Tirant lo Blanch, 2015. p. 329.

[121] HECKH, N., y otros. *Memento experto Protección de Datos*. Madrid: Ed. Francis Lefebvre, 2012. p. 47.

[122] PLAZA PENADÉS, J. Aspectos básicos de los derechos fundamentales y la protección de datos de carácter personal en internet. En: PLAZA PENADÉS, J., VÁZQUEZ DE CASTRO, E., GUILLÉN CATALÁN, R., CARBAJO CASCÓN, F. *Derecho y nuevas tecnologías de la información y la comunicación*. Cizur Menor: Ed. Aranzadi, 2013.

[123] DE MIGUEL ASENCIO, P. A. *Principios de protección de datos. Derecho Privado de Internet*. Navarra: Ed. Aranzadi, 2011. p. 260.

personales de un proveedor de servicios a otro con mayor facilidad. El interesado tiene derecho a recibir sus datos personales que haya proporcionado a un responsable, en un formato legible estructurado y de uso común y a que esos datos se transmitan directamente a otro responsable cuando ello sea técnicamente posible.

Para determinar qué información personal será objeto de portabilidad, es necesario estudiar los límites del propio derecho[124]. En primer lugar, incluye el derecho a recibir datos personales, es decir a recibir datos personales procesados por un responsable de tratamiento, para almacenarlo para uso personal adicional en un dispositivo privado, sin transmitirlo necesariamente a otro responsable de tratamiento. En segundo lugar, además, implica el derecho a transmitir datos personales de un responsable de tratamiento de datos a otro sin obstáculos, proporcionando a los titulares la posibilidad de obtener, reutilizar, y transmitir los datos que han proporcionado a otro proveedor de servicios.

En el ámbito técnico, el RGPD establece que los responsables del tratamiento de datos deben ofrecer diferentes mecanismos para garantizar la portabilidad de datos. Hay que tener en cuenta que quien recibe los datos como consecuencia del ejercicio de este derecho se convierte en nuevo responsable del tratamiento de los datos personales y deberá respetar los principios del artículo 5 de la norma comunitaria, teniendo que informar sobre la finalidad del nuevo tratamiento.

Cuando el interesado ejerce alguno de los derechos recogidos en el RGPD, lo hace sin perjuicio de cualquier otro. Por ello si el interesado desea ejercer su derecho a la supresión de los datos, los efectos de una portabilidad de datos no pueden ser utilizados por el responsable como forma de obstaculizar o impedir la supresión[125].

Por otra parte, encontramos el conocido como el derecho al olvido que ha sido una de las cuestiones que más interés ha suscitado desde la STJUE de 13 de mayo de 2014 del caso Google contra España. A pesar de que no sea éste el momento de entrar en profundad en él, no parece tampoco admisible tratar el tema de las novedades que ha supuesto el RGPD sin hacer una mínima referencia al derecho al olvido dada la trascendencia que ha experimentado.

Este derecho permite a los usuarios eliminar sus datos personales cuando no existan razones legítimas para que sigan siendo conservados una vez cumplida su finalidad.

---

[124] BIURRUN ABAD, F. Novedades del nuevo Reglamento de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 916, 2016.

[125] VALDECANTOS FLORES, M. El derecho a la portabilidad de los datos en el Reglamento General de Protección de datos. En: *Diario La Ley*. Madrid: Ed. Wolters Kluwer, nº 2, 2017.

"El llamado derecho al olvido es el derecho a que nuestro pasado sea enterrado, que no sea reabierto y que hechos que sucedieron en el pasado, y que habían sido olvidados, se vuelvan a divulgar"[126]. El titular de un dato tiene derecho, por tanto, a que éste sea borrado o bloqueado, y, en particular, que no sea accesible a través de Internet, cuando se produzcan determinadas circunstancias que establece el propio reglamento comunitario: a) que los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados; b) que el interesado retira el consentimiento en que se basa el tratamiento o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos; o c) el interesado se opone al tratamiento de sus datos personales ejerciendo su derecho de oposición[127].

Asimismo, se prevé para el caso en que un responsable de tratamiento haya hecho públicos los datos personales, que éste deberá adoptar todas las medidas razonables para realizar el derecho del titular, informando a terceros que estén tratando dichos datos de que un interesado ha requerido su supresión.

La mencionada STJUE, de 13 sobre el caso Google Spain contra la AEPD, declaró la aplicación de la legislación de protección de datos a los motores de búsqueda porque entendió que su actividad de almacenamiento e indexación de la información para ponerla a disposición del público general, corresponde con una actividad de tratamiento de datos personales y consecuentemente, los conocidos como buscadores de Internet tienen la consideración reglamentaria de responsable de tratamiento. "En caso que una determinada indexación realizada por los buscadores lesione la dignidad de la persona o limite el libre desarrollo de la misma, esto es, el bien jurídico protegido por el derecho al olvido, los órganos competentes podrán adoptar medidas encaminadas a retirar los datos que permiten tal lesión"[128].

Se refuerza, por tanto, la protección del derecho al olvido, de acuerdo con la tesis mantenida inicialmente tanto por la AEPD como de la AN y por la STJUE de 13 de mayo de 2014[129]. No obstante, el artículo 17 RGPD establece un elenco de exclusiones al derecho de supresión o derecho al olvido, que no se aplicará: a) cuando el tratamiento de los datos sea necesario para ejercer el

[126] COBAS COBIELLA, M. E. Derecho al olvido: de la STJUE de 2014 al Reglamento europeo de Protección de Datos. En: *Actualidad Civil*. Madrid: Ed. Wolters Kluwer, nº 1, 2017.

[127] DAVARA RODRÍGUEZ, M. A. El Derecho al olvido en Internet. El Consultor de los Ayuntamientos. En: *Diario La Ley*. Madrid: Ed. Wolters Kluwer, nº 13, 2014.

[128] SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital*. Valencia: Ed. Tirant lo Blanch, 2011. p. 173.

[129] BUISÁN GARCÍA, N. El derecho de supresión en el nuevo reglamento europeo de protección de datos personales. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 7, 2018.

derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones.

Hay otro derecho que procede destacar que es el derecho de los titulares a no ser objeto de decisiones basadas en automatismos ni perfiles. El RGPD consagra así un derecho estratégico para la efectiva protección de los datos personales.

El Considerando 71 y el artículo 22 del RGPD regulan las decisiones individuales automatizadas, incluida la elaboración de perfiles, estableciendo que todo interesado tendrá derecho "a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar".

Los datos personales revelan información sobre multitud de aspectos de la vida privada de los titulares, tales como sus hábitos, comportamientos, su situación patrimonial… datos que convenientemente analizados, pueden utilizarse para predecir su comportamiento futuro y en base a esta predicción ser objeto de decisiones que le afecten en su esfera jurídico individual y que sean tomadas de manera automática por los programas informáticos.

El Reglamento define la elaboración de perfiles como la actividad que "consiste en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar" (de acuerdo con el Considerando 71 y el artículo 4 RGPD)[130].

[130] RECIO GAYO, M. Los nuevos y los renovados Derechos en Protección de Datos en el RGPD, así como sus limitaciones. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

El apartado segundo del artículo 22 RGPD establece sin embargo excepciones a la regla general establecida en el apartado precedente, por cuanto que no será aplicable a los siguientes casos:

a) Cuando sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) Cuando esté autorizada por el Derecho de la Unión o de los Estados Miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) Cuando se base en el consentimiento explícito del interesado.

Sobre la prestación del consentimiento hay que destacar que no se trata de una prestación general del consentimiento para el tratamiento de los datos del titular, sino que se requiere el consentimiento expreso a que la decisión se tome automáticamente sobre la base del tratamiento de los datos almacenados[131].

#### 4.2.3. Otras novedades destacables

##### 4.2.3.a. El delegado de protección de datos

El reglamento europeo sobre protección de datos crea la figura del Delegado de Protección de Datos, conocido comúnmente por sus siglas en inglés DPO (*Data Protection Officer*). El legislador europeo entiende que existe la necesidad de que exista un profesional que ayude al responsable o encargado del tratamiento a supervisar la observancia interna del propio reglamento. El DPO será la persona encargada de informar a la entidad o responsable del fichero sobre sus obligaciones legales en materia de protección de datos de carácter personal, así como velar para se cumplan las normas (internas y externas) al respecto y de cooperar con la autoridad de control y actuar como punto de contacto entre ésta y la entidad responsable del tratamiento de datos[132].

La figura del delegado de protección de datos no es en sí novedosa, aunque sí lo es para España[133]. Tiene su origen en Alemania que la incluyó en su Ley Federal de Protección de Datos de 1977. Países como Francia, Suecia,

[131] MÁS BADIA, M. D. Los sistemas de información crediticia y la protección de datos personales: un Reglamento europeo y una Ley Orgánica concebida y no nacida. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[132] BIURRUN ABAD, F. Novedades del nuevo Reglamento de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, núm. 916, 2016.

[133] RECIO GAYO, M. *La independencia del delegado de protección de datos (DPD): obligación y garantía*. Diario La Ley, Sección Ciberderecho. Madrid: Ed. Wolters Kluwer, número 19, 2018.

Luxemburgo, los Países Bajos o las propias instituciones de la Unión Europea también cuentan con esta figura[134].

En el ámbito de las instituciones de la Unión Europea esta figura se ha regulado por el Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, 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. Su artículo 24 señala que cada organismo comunitario nombrará al menos a una persona para que actúe como responsable de la protección de datos, encargado, entre otras cosas, de garantizar que los responsables del tratamiento y los interesados sean informados de sus derechos y obligaciones de conformidad con el presente reglamento y velar porque el tratamiento no tenga efectos adversos sobre los derechos y las libertades de los interesados[135].

El RGPD contempla tres supuestos en los que es obligatorio el nombramiento de un Delegado de Protección de Datos: en primer lugar los tratamientos de datos llevados a cabo por Autoridades u Organismos Públicos, aunque se excluye expresamente el tratamiento de datos llevado a cabo por los Juzgados y Tribunales en el ejercicio de su función; en segundo lugar, los tratamientos a gran escala que por su alcance precisen de vigilancia sistemática; y, finalmente, los tratamientos a gran escala de categorías especiales de datos[136].

Tal y como puede comprobarse, la definición de los supuestos es poco precisa. Por esta razón el GT29 recomienda que se realice un análisis interno con el objeto de determinar primeramente si la persona o entidad tiene o no la obligación de nombrar a un delegado de protección de datos. De esta manera, se permite que se recoja documentalmente las razones suficientes por las que se concluye no estar subsumidos en el artículo 37 del RGPD.

Se advierte que este artículo afecta profundamente al sector público puesto que uno de los supuestos en los que es obligatoria la designación del DPO es cuando el tratamiento lo lleve a cabo una autoridad u organismo

134 BOTANA GARCÍA, G. A. La formación del Delegado de Protección de Datos (DPO).En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

135 DAVARA RODRÍGUEZ, M. A. El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 1, 2017.

136 NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

público como regla general[137]. En el caso de los Juzgados y Tribunales que actúen en ejercicio de su función judicial no será necesario[138].

El GT29 también se ha pronunciado a este respecto sobre el caso en que una autoridad u organismo público es la que tiene la obligación de designar un DPO y considera que, a falta de una definición más precisa del RGPD, tendrá que ser el ordenamiento interno de cada Estado miembro el que concrete los supuestos en los que se exija tal designación. El GT29 ha llegado a sugerir que existirá la obligación de designar a un DPO en los casos en los que una organización se rija por derecho público en la prestación o gestión de servicios[139]. Lo cual, tampoco ayuda a delimitar más precisamente su ámbito de aplicación.

Los interesados y titulares de datos personales podrán acudir al delegado de protección de datos en relación a todas las cuestiones relativas al tratamiento de su información personal y al ejercicio de sus derechos.

El artículo 37, apartado quinto RGPD, exige que el delegado de protección de datos sea 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 propias de su cargo que se prevén el artículo 39 del Reglamento, entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte del responsable o encargado. Esta es la primera vez que se hace referencia a la necesidad de especialización cualitativa del delegado de protección de datos, cuestión sobre la que hace hincapié 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 que se le asignan[140].

No obstante, lo anterior, conviene precisar dos cuestiones, porque si bien el DPO deberá contar con conocimientos especializados del Derecho, y obviamente en protección de datos, el RGPD no exige que tenga que ser un jurista, aunque sí debe tener el conocimiento en Derecho en los términos

[137] PLAZA PENADÉS, J. Implementando el nuevo Reglamento General Europeo de Protección de Datos. En: *Revista Aranzadi de Derecho y Nuevas Tecnologías*. Cizur Menor: Ed. Aranzadi, nº 43, 2017

[138] ÁLVAREZ HERNANDO, J. El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades. En: *Aranzadi digital*. Cizur Menor: Ed. Aranzadi nº 1, 2017.

[139] RECIO GAYO, M. (Directrices del GT29 sobre el delegado de protección de datos: figura clave para la responsabilidad («accountability»). En: *Diario La Ley*. Sección Legal Management. En Madrid: Ed. Wolters Kluwer, nº 2, 2017.

[140] DAVARA RODRÍGUEZ, M. A. El Delegado de Protección de Datos. En: *El Consultor de los Ayuntamientos*. Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 24, 2017, p. 3091.

expuestos[141]. Asimismo, encontramos que tampoco es obligatoria una titulación específica ni que dispongan de ninguna certificación específica.

Cuando el responsable o el encargado del tratamiento es una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, dependiendo de su tamaño y estructura organizativa. No se exige formalmente que se trate de una figura con dedicación exclusiva puesto que el propio RGPD establece que podrá desempeñar otras funciones y cometidos, sin embargo, en la práctica ocurrirá así frecuentemente puesto que también establece el reglamento que el responsable o encargado del tratamiento garantizarán que dichas funciones y cometidos no den lugar a conflicto de intereses. Asimismo, se establece la obligación del delegado de protección de datos de mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones[142].

Sin perjuicio de lo anterior, conviene destacar dos cuestiones principales sobre el delegado de protección de datos. La primera es que éste debe desarrollar sus funciones con independencia y para ello ha de proporcionarse las condiciones necesarias que lo permitan. En segundo lugar, se advierte que el delegado no tiene que ser necesariamente un empleado o funcionario dependiente del responsable del tratamiento y por lo tanto este cargo puede cubrirlo tanto una persona que forme parte de la plantilla del responsable o del encargado del tratamiento o si no, una persona que desempeñe sus funciones en el marco de un contrato de servicios, aunque se debe garantizar en ambos casos que el DPO no reciba ninguna instrucción para desempeño de sus funciones[143].

Tanto el responsable como el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en el proceso de toma de decisiones relativas a la protección de datos personales y deberán respaldar al delegado de protección de datos en el desempeño de sus funciones, facilitándole los recursos necesarios para el desempeño de las mismas, el acceso a los datos personales y a las operaciones de tratamiento, así como proporcionarle el personal, los locales, los equipamientos y cualesquiera otros recursos necesarios para el desempeño de

[141] BOTANA GARCÍA, G. A. La formación del Delegado de Protección de Datos (DPO). En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[142] DAVARA RODRÍGUEZ, M. A. Posición y funciones del delegado de protección de datos. En: Actualidad Administrativa, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 1, 2018.

[143] DAVARA RODRÍGUEZ, M. A. El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 1, 2017.

sus funciones así como las condiciones necesarias que le permitan el mantenimiento de sus conocimientos especializados.

El responsable o el encargado del tratamiento velarán para que desempeñe sus funciones y tareas con independencia y no reciba ninguna instrucción en lo que respecta al ejercicio de sus funciones. De igual forma, el responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de sus tareas y facilitarán el personal, los locales, los equipamientos y cualesquiera otros recursos necesarios para el desempeño de sus funciones y tareas.

El RGPD establece que las tareas del delegado de protección de datos son, como mínimo y entre otras, las siguientes:

a) La de informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben.

b) Supervisar el cumplimiento de la normativa vigente en protección de datos y, en particular, de lo previsto en el propio Reglamento, así como de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que trata datos de carácter personal y las auditorías correspondientes.

c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

d) Cooperar con la autoridad de control

e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento[144].

Asimismo, se establece que el delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

#### 4.2.3. b. Evaluaciones de impacto

Las evaluaciones de impacto relativas a la protección de datos o también conocidas por sus siglas en inglés, *PIA* (*privacy impact assessment*), son otra de las figuras estrella del RGPD"[145]. No obstante, el Reglamento no define su concepto, pero en 2014, antes de la aprobación si quiera del Reglamento, la AEPD publicó un documento llamado "Guía para una evaluación de impacto

[144] DAVARA RODRÍGUEZ, M. A. Posición y funciones del delegado de protección de datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 1, 2018.

[145] RODRÍGUEZ BALLANO, S. Habemus nuevo Reglamento General de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 919, 2016.

en la protección de datos personales". En ella se aportaba la siguiente definición: una metodología para evaluar el impacto en la privacidad de un proyecto, política, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales y, tras haber consultado con todas las partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos[146]. Una evaluación de impacto en la privacidad es un proceso que debería comenzar en las etapas más iniciales posibles, cuando todavía hay oportunidades de influir en el resultado del proyecto[147]. La AEPD a través de este documento hacía recomendaciones para realizar análisis de seguridad análogos a los previstos por el legislador europeo y de esta manera España se adelantaba y sentaba las bases de esta figura que con el RGPD se vuelve de obligado cumplimiento.

La evaluación de impacto es una herramienta que debe implementar el responsable del tratamiento, con carácter previo al propio tratamiento de los datos personales. De esta manera se deben identificar, evaluar y gestionar los riesgos a los que están sometidas las actividades de tratamiento con la finalidad de garantizar los derechos y libertades de las personas físicas. A este respecto, el responsable del tratamiento podrá estar asesorado, en su caso, por el Delegado de Protección de Datos. De esta manera se pretende establecer una actividad preventiva de seguridad que permite establecer las medidas técnicas y organizativas adecuadas al tratamiento que se traducen en la implantación de procedimientos y mecanismos para analizar los riesgos derivados del tratamiento.

De acuerdo con el RGPD, se tendrá que llevar a cabo un PIA cuando se inicien tratamientos de datos mediante nuevas tecnologías que supongan un alto riesgo para los interesados tales como el uso de drones, geolocalización, tratamiento a gran escala de datos de salud, elaboración de perfiles, etc. Así como cuando los citados tratamientos sufran algún tipo de modificación y en los proyectos en los que se utilicen técnicas o tecnologías *Big Data*, o en tratamientos a gran escala de categorías especiales de datos (datos étnicos, políticos, religiosos, sindicales, genéticos, biométricos, sexuales, médicos, etc.) o en la elaboración de perfiles.

El responsable del tratamiento es el obligado a realizar las evaluaciones de impacto. Para ello, puede apoyarse, pedir asesoramiento o encargarlo al

---

146 DAVARA RODRÍGUEZ, M. A. Evaluación del Impacto en la Protección de Datos de Carácter Personal (EIPD). En: *El Consultor de los Ayuntamientos*. Sección Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 9, tomo 1, 2014, p. 1041.

147 GARCÍA, D. Las evaluaciones o análisis de riesgos de las operaciones de tratamiento de protección de datos en el ámbito de las AAPP. La guía de la APDCAT sobre orientaciones prácticas para una EIPD. En: *El Consultor de los Ayuntamientos*. Madrid: Ed. Wolters Kluwer, nº 24, 2018, p. 3037.

Delegado de Protección de Datos, pero se establece como una obligación para el responsable del tratamiento.

Es conveniente destacar que la evaluación de impacto ha de ejecutarse de manera previa al tratamiento. No se extiende esta obligación a los tratamientos que ya se estén llevando a cabo. Se trata de una medida preventiva y, por lo tanto, antes de iniciar un tratamiento que pueda ser susceptible de entrañar riesgos, habría que realizar un *PIA*, que proporcione la información sobre si es seguro llevar a cabo dicho tratamiento, en cuyo caso habrá que desistir de hacerlo o bien aplicar medidas correctoras que permitan superar los riesgos potenciales que pretenden salvarse. En cualquier caso, ha de considerarse que esta herramienta preventiva va a permitir, por un lado, reducir los costes de la implementación de la normativa de protección de datos, y, por otro, prevenir posibles problemas que puedan dañar la reputación de las entidades afectadas[148].

Una correcta evaluación de impacto de protección de datos personales debe incluir aspectos tales como la descripción de la actividad de tratamiento prevista, una adecuada evaluación de los riesgos del tratamiento, una ponderación de la necesidad y proporcionalidad del tratamiento, así como las medidas de seguridad y mecanismos que garanticen la protección de los datos personales[149].

La autoridad de control publicará una lista de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos. Estas listas se comunicarán al Comité Europeo de Protección de Datos por la AEPD de acuerdo con el artículo 68 RGPD. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos, para mayor seguridad jurídica de los responsables, en cuyo caso también se comunicarán al Comité.

Sin perjuicio de lo anterior, antes de adoptar las listas del párrafo anterior, la AEPD aplicará el mecanismo de coherencia contemplado en el artículo 63 RGPD si esas listas incluyen actividades de tratamiento sobre datos de oferta de bienes o servicios a interesados o sobre el comportamiento de éstos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

De acuerdo con la normativa europea un *PIA*, deberá incluir como mínimo, una descripción sistemática de las operaciones de tratamiento

[148] DAVARA FERNÁNDEZ DE MARCOS, E. La evaluación de impacto en protección de datos: aspectos de interés. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº4, 2018.

[149] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

previstas y de los fines del tratamiento, incluyendo, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento. Así como una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad. Se deberá realizar una evaluación de los riesgos para los derechos y libertades de los interesados y una selección de las medidas previstas para afrontar los riesgos, incluyendo garantías, medidas de seguridad y mecanismos para garantizar la protección de datos personales. A través del *PIA*, se podrá demostrar que las actividades se han realizado de conformidad con el nuevo sistema de protección de datos personales[150].

**5. Sistema actual de protección de datos en España. La nueva ley orgánica de protección de datos personales y garantía de derechos digitales**

La entrada en vigor del RGPD impuso también un cambio en el marco jurídico del derecho a la protección de datos en el ordenamiento interno de los Estados miembros[151]. En este apartado se pretende dilucidar cómo queda el sistema de protección después de la llegada del reglamento puesto que éste deroga la normativa europea anterior pero también cuestiona la vigencia de la normativa interna que fuera incompatible con aquél[152].

Es innegable que el RGPD es plenamente aplicable en España, como en el resto de países miembros de la U.E., y por lo tanto ha pasado a ser la norma principal en materia de protección de datos personales. A nivel de ordenamiento interno tenemos que plantearnos la cuestión de la vigencia de la LOPD de 1999 y su reglamento de desarrollo.

Aún después de la entrada en vigor del reglamento comunitario de protección de datos, el ordenamiento interno español no se había adaptado al nuevo marco jurídico. El Gobierno de España aprobó el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. Se trataba de una previsión transitoria, solo en materia sancionadora, hasta que se publicara definitivamente lo que podemos llamar la nueva LOPD. Actualmente nos encontramos con que el Senado aprobó el 21 de noviembre de 2018 el Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de Derechos

150 CAMPOS ACUÑA, M. C. La política de seguridad en el RGPD. Análisis de riesgos y Evaluación de Impacto. La aplicación del Esquema Nacional de Seguridad. Esta doctrina forma parte del libro "Administraciones Públicas y Protección de Datos: adaptación al RGPD". En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

151 TRONCOSO REIGADA, A Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. En: *Revista de los Estudios de Derecho y Ciencia de la UOC*. Barcelona: Ed. Universitat Oberta de Catalunya, nº 15, 2012.

152 SOLAR CALVO, P. Nueva regulación europea en protección de datos. Urgente necesidad de una normativa nacional. En: *Revista Aranzadi Unión Europea*. Cizur Menor: Ed. Aranzadi, nº 7, 2018.

Digitales (en adelante LOPDGDD), que a la fecha de presentación de este trabajo se encontraba aún pendiente de publicación en el Boletín Oficial del Estado.

Esta norma, deroga expresamente la LOPD de 1999 y Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea, así como cualquier otra disposición que contradiga, se oponga o resulte incompatible con lo dispuesto en el RGPD o la LOPDGDD. No hay un pronunciamiento expreso sobre el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD de 1999, así que cabría plantearse su vigencia respecto de aquello que no se entienda derogado tácitamente por la nueva norma española[153].

La entrada en vigor del RGPD prácticamente imponía la necesidad de sustituir la LOPD por una nueva. "El Considerando 17 del Reglamento de 2016 deja vigente el Reglamento 45/2001, si bien matiza que junto con otras normas "deben adaptarse a los principios y normas establecidas 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. De manera que deben introducirse las adaptaciones necesarias"[154]. Aunque **la nueva ley** debería tener **un alcance** limitado puesto que, aunque el RGPD permite un cierto margen de maniobra a los Estados miembros, éste se restringe por razones de coherencia y esclarecimiento de su contenido. La LOPDGDD no debería hacer reiteraciones de las disposiciones del RGPD sino clarificar sus disposiciones "dentro de los márgenes que éste establece y teniendo en cuenta la propia tradición jurídica nacional"[155], especificar y a ampliar determinados aspectos del RGPD[156].

La Ley está compuesta por 97 artículos, dispuestos en 10 Títulos, 22 Disposiciones Adicionales, 6 Disposiciones Transitorias, 1 Disposición Derogatoria y 16 Disposiciones Finales.

En primer lugar, destacamos la cuestión de la denominación de la norma, puesto que se trata de la Ley Orgánica de Protección de datos y Garantía de Derechos Digitales. Como se puede comprobar se añade la cuestión de los

[153] ROJO FERNÁNEZ-MATINOT, I. El Delegado de Protección de Datos. En: Diario La Ley, Sección Temas de hoy. Madrid: Ed. Wolters Kluwer, nº 9189, 2018.

[154] REBOLLO DELGADO, L. *Manual de protección de datos*. 2ª edición. Madrid: Ed. Dykinson, 2017. Página 53.

[155] RALLO LOMBARTE, A. España en la vanguardia de la protección de datos: nuevos retos del reglamento europeo, En LÓPEZ CALVO, J. *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* Madrid: Ed. Bosch. Wolters Kluwer, 2018. Página 79.

[156] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

derechos digitales a la rúbrica de la norma. Esto es consecuencia de la especial preocupación que rodea a la cuestión de la protección de la información personal ante los retos que suponen los avances tecnológicos. Se advierte un salto cualitativo en esta cuestión respecto del anterior texto de 1999. "El Derecho debe ir por delante de las novedades y de los problemas sociales (y tecnológicos), pero lo cierto es que en este terreno dicha actuación se reputa, si no imposible, sí realmente complicada. En todo caso, la regulación jurídica de las nuevas tecnologías en todos sus aspectos, y más en concreto, con relación a la intimidad de las personas, debe evitar la tendencia deshumanizadora provocada por las nuevas tecnologías y debe tener como fundamento y fin a la misma persona humana"[157].

Por todo ello, era predecible la evolución normativa que se aprobaba el 23 de noviembre en el Senado. "El reconocimiento constitucional o europeo, legal o constitucional, del derecho fundamental a la protección de datos no agota la necesidad de establecer un nuevo marco de protección de los ciudadanos en la era digital"[158]. Por eso se antojaba imprescindible la incorporación de los nuevos derechos digitales al texto de la nueva LOPD como garantía de los derechos de los individuos en Internet y ante la Tecnología. Se trata de una nueva generación de derechos digitales, de carácter sustantivo o prestacional.

Así, se incorpora al texto de la ley un título, el décimo, en el que se reconoce el elenco de derechos digitales tales como el derecho a la neutralidad de Internet, el acceso universal a la Red, el derecho a la seguridad digital, el derecho a la educación digital y la protección de los menores en Internet, el derecho de rectificación en Internet y el de actualización de informaciones en medios de comunicación digital, el derecho al olvido en búsquedas de Internet y en servicios de redes sociales o servicios equivalentes, el derecho a la portabilidad en servicios de redes sociales y equivalentes y el derecho al testamento digital.

Del nuevo texto español procede hacer las siguientes apreciaciones. Respecto del ámbito de aplicación, el artículo 2 de la LODP de 1999 en sus apartados segundo y tercero, excluía de su ámbito el tratamiento de datos referidos a personas jurídicas, personas físicas que presten servicio en personas jurídicas o empresarios individuales en ejercicio de su actividad, cuando consistan únicamente en datos identificativos o de contacto. Sin embargo, el

[157] JIMÉNEZ RIUS, P. Antecedentes legislativos de la nueva Ley Orgánica de Protección de Datos Personales. En: *Actualidad Administrativa*. Madrid: Ed. La Ley, tomo 2, 2001, página 965.

[158] RALLO LOMBARTE, A. De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018). En: Revista de Derecho Político. Madrid: UNED, nº 100, 2017. p. 665.

RGPD no establece tal exclusión y, por lo tanto, podría haber producido una incompatibilidad con el nuevo régimen comunitario, pero la nueva ley de protección de datos incorpora en su artículo 19.1 una previsión permitiendo el tratamiento de los datos de contacto de personas jurídicas y empresarios individuales, sin necesidad del consentimiento del interesado, en base al interés legítimo. Esto ha sido considerado un acierto por cuanto que se trata de supuestos en los que la aplicación de técnicas como las de *Big Data* pueden generar riesgos potenciales para la protección de los datos que de otra manera podrían quedar sin la protección del nuevo sistema de normas[159].

Aspecto destacable es la cuestión del consentimiento. Se trata de uno de los pilares principales sobre los que se construye el nuevo modelo de protección de datos y la Ley española no podía hacer otra cosa más que seguir la línea marcada por el reglamento[160]. Aquélla exige en su artículo 7 que el consentimiento sea específico y verificable, prestado a través de una clara acción afirmativa. De esta manera marca una diferencia importante respecto al sistema anterior que, en determinados casos, permitía el consentimiento tácito.

La utilización del requisito del consentimiento como eje vertebrador del sistema de protección de datos ha sido criticado por parte de la doctrina, puesto que se cuestiona la capacidad de decisión real del interesado, planteándose si la no aceptación del tratamiento de los datos puede dar lugar a que una parte de la población quede al margen del desarrollo tecnológico. Este desarrollo trae consigo una serie de posibilidades de crecimiento a las que tendrían que renunciar aquellos que no estuvieran dispuestos a consentir el tratamiento de los datos de la manera que se impone por parte de quien presta los servicios. Servicios sin los cuales parecería muy difícil desenvolverse en la sociedad actual. Me refiero a servicios financieros, de contratación electrónica, plataformas de comunicación digital, etc. que suponen un escenario en el que no se puede elegir participar o no sin resultar perjudicado en cuanto a las posibilidades de desarrollo personal o profesional. En este sentido hay una previsión en la nueva LOPDGDD en el artículo 6.3 que establece que "no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual". Este precepto viene a reforzar la aplicación del principio de finalidad en el sentido de proteger al titular de los datos respecto de tratamientos abusivos que deban

[159] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[160] VALDECANTOS, M. El consentimiento como base legitimadora del tratamiento en el Reglamento europeo de protección de datos. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

consentirse, so pena de quedar excluido de la obtención de determinados servicios o incluso ventajas que ofrece el mercado o la sociedad del s. XXI.

El RGPD establece la edad mínima de los menores para prestar el consentimiento en los 16 años, pero dejaba en manos de los Estados miembros la determinación concreta de la edad mínima siempre que ésta no fuera nunca inferior a 13 años. En nuestro caso, el nuevo texto fija el límite de edad para prestar el consentimiento en los 13 años, siguiendo en este caso la línea marcada por otros países de nuestro entorno[161].

En el artículo 73 a) se tipifica como sanción grave el tratamiento de datos personales de un menor de edad sin recabar su consentimiento cuando tenga capacidad para ello o bien el del titular de la patria potestad o tutela[162]. Por su parte, en el apartado letra b) del mismo artículo se prevé también como infracción grave el no acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de trece años o por el titular de su patria potestad o tutela.

A partir de ahora, con la nueva LOPDGDD se permite que los herederos o representantes legales de personas fallecidas puedan tener acceso a los datos del difunto en Internet. Esto significa que podrán dirigirse a los prestadores de servicios de la sociedad de la información para decidir sobre el destino o la supresión de dichos datos del fallecido[163].

En cuanto a los derechos de los titulares de los datos, se reflejan también en la norma española los mismos derechos comunitarios de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición. Se incorpora, además, la llamada obligación de bloqueo[164]. A través de ella se garantiza que los datos queden a disposición de un Tribunal, el Ministerio Fiscal u otras autoridades competentes (como la Agencia Española de Protección de Datos) cuando se presenten reclamaciones de posibles responsabilidades derivadas del tratamiento dado a los datos, impidiendo así la destrucción de material y pruebas que puedan encubrir el incumplimiento[165].

---

[161] DAVARA RODRÍGUEZ, M. A. Hacia una nueva Ley de Protección de Datos. En: *El Consultor de los Ayuntamientos*. Sección Zona Local / Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 15, 2017, p. 1983.

[162] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[163] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[164] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[165] DAVARA RODRÍGUEZ, M. A. Hacia una nueva Ley de Protección de Datos. En: *El Consultor de los Ayuntamientos*. Sección Zona Local / Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 15, 2017, p. 1983.

Mediante la LOPDGDD se quiere aplicar la garantía de la rectificación al derecho a la libertad de expresión *online.* Este es uno de los extremos que más suspicacias está generando desde que se conoce la aprobación de la norma en el Senado. Tradicionalmente esta rectificación estaba ideada como una garantía de la libertad de información que permitiera reforzar la comunicación de hechos veraces, objetivos y relevantes para la opinión pública, pero para emplearse respecto de opiniones e ideas subjetivas. Esto llevaría a un control de las expresiones que se usen a través de plataformas o medios ajenos que podrían desembocar en una suerte de censura de opinión que quedaría en manos de los titulares de los medios a través de los cuales se realizan[166].

Por su parte, esta nueva Ley Orgánica de Protección de Datos contempla el deber de información al usuario en el caso de obtención de datos a través de redes de comunicaciones electrónicas o en el marco de la prestación de un servicio de la sociedad de la información. En cualquier caso, se debe indicar al usuario la identidad del responsable del tratamiento, la finalidad para la que se recaban los datos, y el modo en que puede ejercer los derechos de acceso, rectificación, supresión, limitación y portabilidad[167].

La nueva ley ha tratado de solucionar un problema respecto de los denominados SIC (Sistema de Información Crediticia). En España, para el caso de prestatarios personas físicas, se venía distinguiendo entre datos positivos y negativos sobre solvencia, y se prescindía del consentimiento del afectado sólo para el caso de los datos negativos, salvo que procedieran de fuentes de acceso público. Esto dio lugar a que los ficheros privados de solvencia patrimonial se configuraran, en general, como ficheros negativos (conocidos como registros de morosos o de impagados) limitándose el tratamiento de los datos al de las deudas concretas incumplidas a diferencia de lo que se ha hecho en otros países de nuestro entorno. La LOPDGDD introduce cambios significativos en el modelo descrito. Dedica a la regulación de los Sistemas de Información Crediticia el art. 20, además de la Disposición Adicional 8. Y es que el artículo 20 no contiene referencia expresa alguna a los datos de solvencia positivos y establece que prevalece el interés legítimo del responsable del tratamiento de los datos en cumplimiento de determinados requisitos, como en el caso de los sistemas de información crediticia. Igualmente, regula situaciones en las que se aprecia la existencia de interés público, como los relacionados con la videovigilancia y sistemas de exclusión publicitaria ("listas Robinson"), la función estadística pública y las denuncias internas en el sector privado.

[166] TEJERINA, O. Libertad de información: responsabilidad y delegación de poderes en la nueva LOPD. En: *Diario La Ley*. Sección Ciberderecho. Madrid: Ed. Wolters Kluwer, nº 22, 2018.

[167] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

El legislador "ha considerado que en el caso del tratamiento de datos sobre deudas incumplidas debe, no tanto considerarse directamente, sino presumirse, salvo prueba en contrario, que lo son el interés del acreedor y el interés general en que puedan tratarse los datos sin necesidad de que el deudor lo consienta siempre que se den unos requisitos que se enuncian en el precepto. En cambio, no se ha establecido la misma presunción en relación con los datos positivos sobre solvencia"[168].

Se fomentarán mecanismos de autorregulación tanto en el sector público, como en el privado, con el objetivo de mejorar los procedimientos de tratamiento de datos.

Con respecto al Delegado de Protección de Datos, el artículo 34 LOPDGDD determina los supuestos en los que es obligatoria su designación, sin perjuicio de lo dispuesto en el RGPD. Entre ellos, encontramos el caso de los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio; de las compañías de marketing conductual; operadores de apuestas en Internet, entidades de crédito, entidades aseguradoras o entidades de inversión. Además, se prevé en el artículo 37 la posibilidad de que un afectado, antes de interponer una reclamación ante AEPD, se dirija frente al Delegado de Protección de Datos de la entidad correspondiente[169].

Sobre las evaluaciones de impacto, la ley española ha dejado pasar la posibilidad de determinar en su articulado los supuestos en los que se deberían llevar a cabo. La consecuencia lógica que se vaticina entre la doctrina especializada es que será la propia AEPD la que tenga que suplir esta falta para otorgar una mayor seguridad jurídica que ya se venía solicitando desde la publicación del propio RGPD[170].

En cuanto al régimen sancionador procede hacer las siguientes aclaraciones. En primer lugar, encontramos que, sobre los sujetos potencialmente sancionables, artículo 70, a diferencia de lo que hacía la Ley de 1999 que únicamente atribuía responsabilidad a los responsables del fichero y encargados del tratamiento, añade, además, a los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea, así como a las entidades de certificación y a las entidades

[168] MÁS BADIA, M. D. Los ficheros de solvencia patrimonial en la proyectada nueva Ley Orgánica de Protección de Datos de carácter personal. ¿Un avance o una oportunidad perdida? En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 11, 2017.

[169] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

[170] CUESTA GARCÍA, V. Acerca del Proyecto de Ley Orgánica de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº7, 2018.

acreditadas de supervisión de los códigos de conducta. Sin embargo, en su aparado segundo excluye al delegado de protección de datos.

Respecto de las infracciones, vemos como se mantiene la distinción de la LOPD de 1999 de infracciones muy graves, graves y leves, así como los plazos de prescripción de las mismas en tres, dos y un año respectivamente. En cuanto a las sanciones, el texto remite al artículo 83 del RGPD aunque incorpora en el apartado segundo del mismo artículo unos criterios de graduación de la sanción, que deberán aplicarse teniendo en cuenta: el carácter continuado de la infracción; la vinculación de la actividad del infractor con la realización de tratamientos de datos personales; los beneficios obtenidos como consecuencia de la comisión de la infracción; la posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción; la existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente; la afectación a los derechos de los menores; disponer, cuando no fuere obligatorio, de un delegado de protección de datos; así como el sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado[171].

En el ámbito de las Administraciones Públicas (órganos constitucionales, órganos jurisdiccionales, Administración Central, Autonómica o Local… de acuerdo con el artículo 77.1) LOPDGDD, el régimen sancionador se ventila con un apercibimiento al ente y con una posible exigencia de responsabilidad disciplinaria del funcionario o persona que cometa la infracción en cuestión. En concreto, el artículo 77.2 de la nueva norma (LOPDGDD) establece que cuando los responsables o encargados de tratamiento enumerados en el apartado 1 cometiesen alguna de las infracciones previstas en la ley, la autoridad de protección de datos competente según los casos, dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido. Sin perjuicio de la iniciación de actuaciones disciplinarias[172].

En este caso la aplicación del régimen de responsabilidades resulta muy laxo con las Administraciones Públicas, que generalmente son las que tienen que decidir qué medios se destinan a la protección efectiva de los datos que

[171] DAVARA FERNÁNDEZ DE MARCOS, L. Una primera aproximación al Anteproyecto de Ley Orgánica de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 1, 2018.

[172] CUESTA GARCÍA, V. Acerca del Proyecto de Ley Orgánica de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 7, 2018.

obren en su poder, y sin embargo son los funcionarios o el personal que en ellas trabajen los que deban sufrir las consecuencias de unas infracciones en las que, en muchos casos, no ha tenido capacidad de decisión ni intervención para evitar la comisión de la infracción.

Otro de los aspectos destacables de la norma española es la regulación del conocido como *whistleblowing*. Su interés proviene de ser la primera vez que se regula el sistema de información de denuncias internas en el sector privado (también prevé la posibilidad de que puedan crearse en las administraciones públicas). En concreto, el artículo 24 del nuevo texto declara lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

En su caso, los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información y el acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a los que desarrollen las funciones de control, o a los encargados del tratamiento que se designen a tal efecto. Sin perjuicio de lo anterior, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan. Deberán adoptarse las medidas necesarias para preservar el anonimato del *whistleblower.*

"De otro lado, en lo referente al tratamiento de los datos, se adopta el principio de transparencia, se regulan los sistemas de información crediticia, la video vigilancia, los sistemas de exclusión publicitaria («listas Robinson»), la función estadística pública y las denuncias internas en el sector privado"[173].

La nueva ley establece que será lícito el tratamiento de datos de carácter personal que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas. Esto se refiere esencialmente a la conocida como "Lista Robinson"[174].

Sobre la cuestión de la videovigilancia es conveniente aclarar que, antes de la LOPDGDD, sólo venía regulada por la Instrucción 1/2006 de la AEPD dado que la LOPD de 1999 no preveía regulación sobre la utilización de estos sistemas de seguridad. Con el nuevo texto, aparece regulada en el artículo 22. El supuesto es el de la utilización de una instalación de cámaras. Una persona

[173] DAVARA RODRÍGUEZ, M. A. Hacia una nueva Ley de Protección de Datos. En: *El Consultor de los Ayuntamientos*. Sección Zona Local / Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 15, 2017, p. 1983.

[174] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

física o jurídica instala cámaras o videocámaras con el fin de preservar la seguridad tanto de sus instalaciones como de los recursos, humanos y materiales, que en ella se encuentran.

Sólo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad de preservar la seguridad, matizando que dicho límite no es aplicable cuando el objeto de la grabación sea garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte. Mantiene el criterio que la AEPD había establecido en la mencionada instrucción puesto que establece obligación de suprimir los datos de las cámaras y videocámaras en el plazo máximo de un mes desde su captación (salvo que se requiera su conservación para acreditar la comisión de actos delictivos) así como el deber de informar de la grabación mediante la colocación de un distintivo que cumpla con el deber de información del tratamiento de datos y de la posibilidad del ejercicio de derechos. De esta manera se limitan algunas técnicas de tratamiento tales como las conocidas como *deep learning* o videovigilancia inteligente, es decir, el reconocimiento de patrones a través del tratamiento de grandes cantidades de imágenes[175].

Para finalizar este apartado en el que se ha tratado de concentrar los aspectos más destacables de la nueva ley española de protección de datos (en la medida de las posibilidades de un trabajo de esta naturaleza), hay una cuestión más que resulta de especial interés. Se trata de la disposición final cuarta LOPDGDD. En ella se establece una modificación de la LOPJ, en concreto del artículo 58, para establecer el ámbito competencial de la Sala de lo Contencioso-Administrativo del Tribunal Supremo para el caso de suspensiones de procedimientos en supuestos de transferencia internacional de datos, cuando el órgano de control competente sea el CGPJ. Lo que se quiere destacar es lo que se deja de decir a través de esta reforma, puesto que falta mucho por desarrollar para hacer compatible el cumplimiento de la función jurisdiccional, a través de nuestra Administración de Justicia, con el sistema de protección de datos personales y hacerlo, además, con garantías para los justiciables y para los profesionales que desarrollan su función en ella. A través de la reforma operada por la L.O. 7/2015, se introdujo en la LOPJ un intento de adaptar este sistema de protección al funcionamiento de los Juzgados y Tribunales, aunque de manera manifiestamente insuficiente. No obstante, lo anterior, nos encontramos ahora con un reglamento comunitario de 2016 que conlleva cambios significativos que se antojan incompatibles con la regulación actual de la LOPJ, manteniéndose aplicable el Reglamento 1/2005 de Aspectos Accesorios a las Actuaciones Judiciales, norma que contiene prescripciones sobre la protección de datos en la

[175] NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

Administración de Justicia que tienen difícil encaje en el nuevo paradigma europeo. La LOPDGDD ha perdido la ocasión de contribuir al esclarecimiento del régimen de protección de datos en un ámbito tan sensible como es el de la Administración de Justicia.

## 6. Conclusiones

El RGPD supone un cambio de paradigma para el sistema de protección de datos personales, que queda reforzado a través de esta norma comunitaria puesto que permite una aplicación directa en todo el territorio de la Unión y evita que el salto cualitativo que pretende darse quede en manos de la actitud más o menos favorable de los Gobiernos de los Estados miembros. Se consolida un sistema de protección en el que se asumen instituciones ya consideradas tradicionales aunque con un reforzamiento del derecho a la protección de datos que, en unos casos, se realiza de manera explícita a través de la formulación del alcance y límites de estos propios derechos subjetivos o bien a través del establecimiento de principios esenciales de un marco jurídico que a pesar de ser ambicioso, resulta lento para adaptarse al medio tecnológico en el que se producen los peligros para los derechos de los ciudadanos europeos.

Por su parte, la nueva LOPDGDD, a pesar de su reciente aprobación, ya ha suscitado las primeras críticas. Se está extendiendo la idea de que se ha perdido la oportunidad de ofrecer seguridad jurídica aportando más claridad por ejemplo en el trascendental sistema de sanciones, en la concreción de los supuestos en los que es obligatoria las evaluaciones de impacto y especialmente en el encaje del sistema de protección de datos en ámbitos especialmente sensibles para la autodeterminación informativa como pueda ser la Administración Pública.

## 7. Bibliografía

ALEJANDRO PADÍN. Reglamento General de Protección de Datos de la UE: una visión desde el período de adaptación. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 925, 2016.

ÁLVAREZ HERNANDO, J. El Reglamento Europeo y la futura Ley General de Protección de Datos: sus principales novedades. En: *Aranzadi digital*. Cizur Menor: Ed. Aranzadi, nº 1, 2017.

ARENAS RAMIRO, M. *Reforzando el ejercicio del derecho a la protección de datos personales, Hacia un nuevo derecho europeo de protección de datos.* Valencia: Ed. Tirant lo Blanch, 2015.

BIURRUN ABAD, F. Accountability o responsabilidad activa en el Reglamento General de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 927, 2017.

BIURRUN ABAD, F. Novedades del nuevo Reglamento de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor. Ed. Aranzadi, nº 916, 2016.

BLUME, P. Will it be a better world? The proposed EU Data Protection Regulation. En: International Data Privacy Law, nº 2, 2012.

BOTANA GARCÍA, G. A. La formación del Delegado de Protección de Datos (DPO).En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

BUISÁN GARCÍA, N. El derecho de supresión en el nuevo reglamento europeo de protección de datos personales. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 7, 2018.

CAMPOS ACUÑA, M. C. La política de seguridad en el RGPD. Análisis de riesgos y Evaluación de Impacto. La aplicación del Esquema Nacional de Seguridad. Esta doctrina forma parte del libro "Administraciones Públicas y Protección de Datos: adaptación al RGPD". En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

COBAS COBIELLA, M. E. Derecho al olvido: de la STJUE de 2014 al Reglamento europeo de Protección de Datos. En: *Actualidad Civil*. Madrid: Ed. Wolters Kluwer, nº 1, 2017.

CUESTA GARCÍA, V. Acerca del Proyecto de Ley Orgánica de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, número 7, 2018.

DAVARA FERNÁNDEZ DE MARCOS, E. La evaluación de impacto en protección de datos: aspectos de interés. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, número 4, 2018.

DAVARA FERNÁNDEZ DE MARCOS, L. Una primera aproximación al Anteproyecto de Ley Orgánica de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 1, 2018.

DAVARA RODRÍGUEZ, M. A. El Delegado de Protección de Datos en los ficheros y/o tratamientos de la Administración en consonancia con el Reglamento Europeo de Protección de Datos. En: *Actualidad Administrativa*, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, nº 1, 2017.

DAVARA RODRÍGUEZ, M. A. El Delegado de Protección de Datos. En: *El Consultor de los Ayuntamientos*. Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 24, 2017.

DAVARA RODRÍGUEZ, M. A. El Derecho al olvido en Internet. El Consultor de los Ayuntamientos. En: *Diario La Ley*. Madrid: Ed. Wolters Kluwer, nº 13, 2014.

DAVARA RODRÍGUEZ, M. A. Evaluación del Impacto en la Protección de Datos de Carácter Personal (EIPD). En: *El Consultor de los Ayuntamientos*. Sección Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 9, tomo 1, 2014.

DAVARA RODRÍGUEZ, M. A. Hacia una nueva Ley de Protección de Datos. En: *El Consultor de los Ayuntamientos*. Sección Zona Local / Nuevas tecnologías. Madrid: Ed. Wolters Kluwer, nº 15, 2017.

DAVARA RODRÍGUEZ, M. A. Posición y funciones del delegado de protección de datos. En: Actualidad Administrativa, Sección Administración del siglo XXI. Madrid: Ed. Wolters Kluwer, número 1, 2018

DAVARA RODRÍGUEZ, M. A. Una primera aproximación al Reglamento europeo de protección de Datos y su incidencia en el tratamiento de datos de carácter personal de las Administraciones Publicas. En: *Actualidad Administrativa*. Madrid: Ed. Wolters Kluwer, número 4, marzo, 2108.

DE MIGUEL ASENCIO, P. A. *Principios de protección de datos. Derecho Privado de Internet*. Navarra: Ed. Aranzadi, 2011.

DÍAZ DÍAZ, E. El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. En: *Revista Aranzadi Doctrinal.* Cizur Menor: Ed. Aranzadi, nº 6, 2016.

FERNÁNDEZ VILLAZÓN, L. A. El nuevo reglamento europeo de protección de datos. En: *Foro Nueva época*. Volumen 19, nº 1, 2016.

GARCÍA ROMERO, S. Nuevo marco jurídico europeo en protección de datos: novedades conocidas y otras no tan conocidas. En: *Diario La Ley*. Madrid: Ed. La Ley, nº 8691, 2016.

GARCÍA, D. Las evaluaciones o análisis de riesgos de las operaciones de tratamiento de protección de datos en el ámbito de las AAPP. La guía de la APDCAT sobre orientaciones prácticas para una EIPD. En: *El Consultor de los Ayuntamientos*. Madrid: Ed. Wolters Kluwer, nº 24, 2018.

HECKH, N., y otros. *Memento experto Protección de Datos*. Madrid: Ed. Francis Lefebvre, 2012.

JIMÉNEZ RIUS, P. Antecedentes legislativos de la nueva Ley Orgánica de Protección de Datos Personales. En: *Actualidad Administrativa*. Madrid: Ed. La Ley, tomo 2, 2001.

MARTÍN, B. Sobre el ámbito de aplicación material del reglamento general de protección de datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 943, 2018.

MÁS BADIA, M. D. Los ficheros de solvencia patrimonial en la proyectada nueva Ley Orgánica de Protección de Datos de carácter personal. ¿Un avance o una oportunidad perdida? En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 11, 2017.

MÁS BADIA, M. D. Los sistemas de información crediticia y la protección de datos personales: un Reglamento europeo y una Ley Orgánica concebida y no nacida. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

MAYOR GÓMEZ, R. *Contenido y novedades del reglamento general de protección de datos de la U.E. (reglamento UE 2016/679, de 27 de abril de 2016)*. En: *Revista digital Gabilex.* Toledo: Ed. Vicepresidencia 1ª Junta Comunidades Castilla la Mancha, nº 6, 2016.

NOGUEIRA BLANCO, J. Reglamento General de Protección de Datos (RGPD) y BIG DATA. En: *Actualidad Civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

OTANA GARCÍA, G. A. Crónica anunciada de un Reglamento de Protección de Datos en la Unión Europea. En: *Actualidad Civil.* Madrid: Ed. Wolters Kluwer, nº 6, 2016.

PADÍN, A. Reglamento General de Protección de Datos de la UE: una visión desde el período de adaptación. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 925, 2016.

PANIZA FULLANA, A. Una nueva era en la privacidad y las comunicaciones electrónicas: la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas. En: *Revista Doctrinal Aranzadi Civil-Mercantil*. Cizur Menor: Ed. Aranzadi Thomson Reuters, nº 7, 2017.

PLAZA PENADÉS, J. Aspectos básicos de los derechos fundamentales y la protección de datos de carácter personal en internet. En: PLAZA PENADÉS, J., VÁZQUEZ DE CASTRO, E., GUILLÉN CATALÁN, R., CARBAJO CASCÓN, F. *Derecho y nuevas tecnologías de la información y la comunicación*. Cizur Menor: Ed. Aranzadi, 2013.

PLAZA PENADÉS, J. El nuevo marco normativo de la protección de datos. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

PLAZA PENADÉS, J. Implementando el nuevo Reglamento General Europeo de Protección de Datos. En: *Revista Aranzadi de Derecho y Nuevas Tecnologías*. Cizur Menor: Ed. Aranzadi, nº 43, 2017.

RALLO LOMBARTE, A. De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018). En: *Revista de Derecho Político*. Madrid: UNED, nº 100, 2017.

RALLO LOMBARTE, A. España en la vanguardia de la protección de datos: nuevos retos del reglamento europeo, En LÓPEZ CALVO, J. *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos.* Madrid: Ed. Bosch. Wolters Kluwer, 2018.

REBOLLO DELGADO, L. *Manual de protección de datos*. 2ª edición. Madrid: Ed. Dykinson, 2017.

RECIO GAYO, M. (Directrices del GT29 sobre el delegado de protección de datos: figura clave para la responsabilidad («accountability»). En: *Diario La Ley*. Sección Legal Management. En Madrid: Ed. Wolters Kluwer, nº 2, 2017.

RECIO GAYO, M. La independencia del delegado de protección de datos (DPD): obligación y garantía. En: *Diario La Ley*. Sección Ciberderecho. Madrid: Ed. Wolters Kluwer, nº 19, 2018.

RECIO GAYO, M. Los nuevos y los renovados Derechos en Protección de Datos en el RGPD, así como sus limitaciones. En: *Actualidad Civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

RODRÍGUEZ BALLANO, S. Año nuevo, Reglamento de Protección de Datos nuevo. En: *Actualidad Jurídica Aranzadi.* Cizur Menor: Ed. Aranzadi, nº 915, 2016.

RODRÍGUEZ BALLANO, S. Habemus nuevo Reglamento General de Protección de Datos. En: *Actualidad Jurídica Aranzadi*. Cizur Menor: Ed. Aranzadi, nº 919, 2016.

RODRÍGUEZ ESCANCIANO, S. *El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679*. Ed. Aranzadi. 2017.

ROJO FERNÁNEZ-MATINOT, I. El Delegado de Protección de Datos. En: Diario La Ley, Sección Temas de hoy. Madrid: Ed. Wolters Kluwer, nº 9189, 2018.

RUBIO TORRANO, E. Del Reglamento europeo a la nueva Ley Orgánica de Protección de Datos. En: *Revista Doctrinal Aranzadi Civil-Mercantil*. Cizur Menor: Ed. Aranzadi, nº 6, 2018.

SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital*. Valencia: Ed. Tirant lo Blanch, 2011.

SOLAR CALVO, P. La doble vía europea en protección de datos. En: *Diario La Ley*. Sección Doctrina. Madrid: Ed. La Ley, nº 7832, 2012.

SOLAR CALVO, P. Los datos personales en la investigación criminal. En: *Revista de la Guardia Civil.* Sección Formación. Madrid: Dirección General de la Guardia Civil, nº 817, 2012.

SOLAR CALVO, P. Nueva regulación europea en protección de datos. Urgente necesidad de una normativa nacional. En: *Revista Aranzadi Unión Europea*. Cizur Menor: Ed. Aranzadi, nº 7. 2018.

TEJERINA, O. Libertad de información: responsabilidad y delegación de poderes en la nueva LOPD. En: *Diario La Ley*. Sección Ciberderecho. Madrid: Ed. Wolters Kluwer, nº 22, 2018.

TRONCOSO REIGADA, A Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. En: *Revista de los Estudios de Derecho y Ciencia de la UOC*. Barcelona: Ed. Universitat Oberta de Catalunya, nº 15, 2012.

VALDECANTOS FLORES, M. El derecho a la portabilidad de los datos en el Reglamento General de Protección de datos. En: *Diario La Ley*. Madrid: Ed. Wolters Kluwer, nº 2, 2017.

VALDECANTOS, M. El consentimiento como base legitimadora del tratamiento en el Reglamento europeo de protección de datos. En: *Actualidad civil*. Madrid: Ed. Wolters Kluwer, nº 5, 2018.

España. Tribunal Constitucional. Sentencia núm. 292/2000, de 30 de noviembre.

España. Tribunal Constitucional. Sentencia núm. 94/1998, de 4 de mayo.

Tribunal de Justicia de la Unión Europea. Caso Lindqvist. Sentencia de 6 de noviembre de 2003.

Tribunal Europeo de Derechos Humanos (Gran Sala). Sentencia de 6 de noviembre de 2003.

**Conflicto de intereses**

El autor declara no tener ningún conflicto de intereses.

**Financiación**

El documento ha sido elaborado sin financiación.