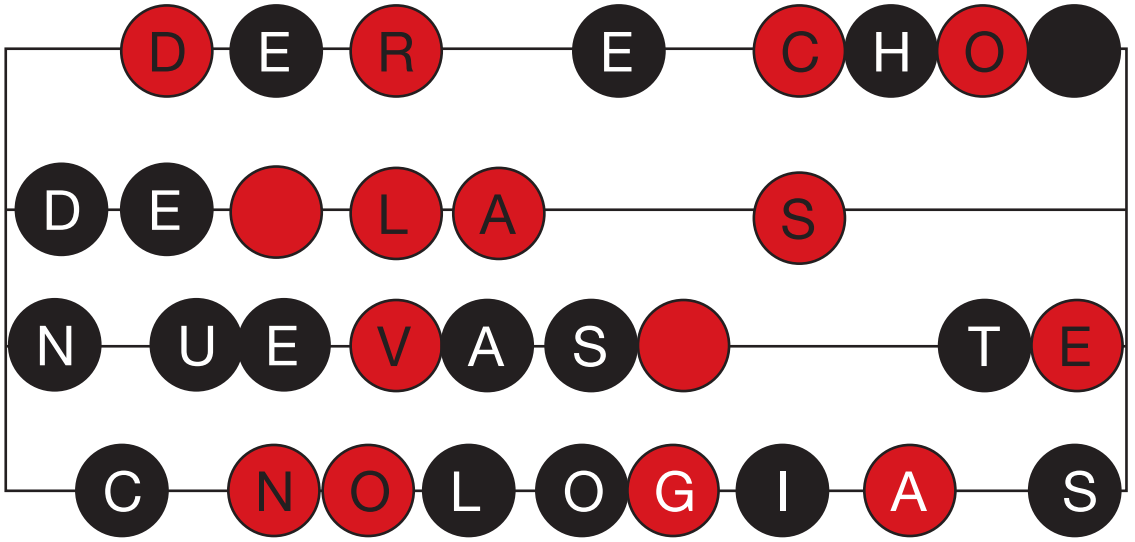

ESTUDIO JURÍDICO-CRÍTICO SOBRE LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

Análisis conjunto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de la Ley Orgánica 3/2018 de 5 de diciembre

Ana Isabel Berrocal Lanzarot
Profesora Contratada Doctora de Derecho Civil
Universidad Complutense de Madrid

REUS
EDITORIAL

COLECCIÓN DE DERECHO DE LAS NUEVAS TECNOLOGÍAS

TÍTULOS PUBLICADOS

Internet, privacidad y datos personales, *Víctor Drummond* (2004).
Contratos electrónicos y protección de los consumidores, *José Antonio Vega Vega* (2005).
Partes intervinientes, formación y prueba del contrato electrónico, *Sandra Camacho Clavijo* (2005).
Diccionario Jurídico de los Medios de Comunicación, *Renato Alberto Landeira Prado y Víctor R. Cortizo Rodríguez* (2006).
La firma electrónica, *Jesús Ignacio Fernández Domingo* (2006).
La interconexión de redes de telecomunicaciones, *Olga Lucía Alfonso Velásquez* (2006).
Sociedad de la información en Europa, *Luis M. González de la Garza* (2008).
Agricultura transgénica y medio ambiente. Perspectiva legal, *Ramón Herrera Campos y María José Cazorla (Coord.)* (2009).
***E-Learning* y Derecho,** *Pablo Gallego Rodríguez* (2010).
El contrato de servicio telefónico, *Olga Lucía Alfonso Velásquez* (2010).
La protección judicial de los derechos en Internet en la jurisprudencia europea, *David Ordóñez Solís* (2014).
Casos y cuestiones sobre Derecho Civil. Materiales para el estudio conforme al Plan Bolonia y ante las nuevas tecnologías, *Guillermo Cerdeira Bravo de Mansilla (Dir.) y Mª Carmen Fernández de Villavicencio Álvarez-Ossorio (Coord.)* (2014).
Casos y cuestiones sobre Derecho Internacional Privado, nacionalidad y extranjería. Materiales para el estudio conforme al Plan Bolonia y ante las nuevas tecnologías, *Fernando Moreno Mozo (Coord.), María Ascensión Martín Huertas y Ana Moreno Sánchez Moraleda* (2014).
El documento jurídico y su electronificación, *José Antonio Vega Vega* (2014).
Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital, *María Álvarez Caro* (2015).
Protección de datos personales e innovación: ¿(in)compatibles?, *Miguel Recio Gayo* (2016).
Contratación electrónica y protección de los consumidores –una visión panorámica–, *Leonardo B. Pérez Gallardo (Coord.)* (2017).
***Smart Contracts.* Análisis jurídico,** *Carlos Enrique Tur Faúndez* (2018).
Protección de datos, responsabilidad activa y técnicas de garantía. Curso de «Delegado de protección de datos», *Juan Pablo Murga Fernández, María de los Ángeles Fernández Scagliusi, Manuel Espejo Lerdo de Tejada (Dirs.), Sara Lorenzo Cabrera, Adrián Palma Ortigosa (Coords.)* (2018).
El Mercado Digital en la Unión Europea, *Paula Castaños Castro y José Antonio Castillo Parrilla (Dirs.)* (2019).
¿Cómo poner en práctica el Gobierno abierto?, *Fernando Galindo (Coord.)* (2019).
Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *Ana Isabel Berrocal Lanzarot* (2019).

COLECCIÓN DE DERECHO DE LAS NUEVAS TECNOLOGÍAS

Directores

GUILLERMO CERDEIRA BRAVO DE MANSILLA

Catedrático de Derecho civil de la Universidad de Sevilla

MIGUEL L. LACRUZ MANTECÓN

Profesor Titular de Derecho civil de la Universidad de Zaragoza

ESTUDIO JURÍDICO-CRÍTICO SOBRE LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

(Análisis conjunto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de la Ley Orgánica 3/2018 de 5 de diciembre)

Ana Isabel Berrocal Lanzarot

Profesora Contratada Doctora de Derecho Civil

Universidad Complutense de Madrid

REUS

EDITORIAL

Madrid, 2019

C/ Rafael Calvo, 18, 2º C – 28010 Madrid
Teléfonos: (34) 91 521 36 19 – (34) 91 522 30 54
Fax: (34) 91 445 11 26
reus@editorialreus.es
www.editorialreus.es

1.ª edición REUS, S.A. (2019)

ISBN: 978-84-290-2176-9
Depósito Legal: M-34391-2019
Diseño de portada: María Lapor
Impreso en España
Printed in Spain

Imprime: Ulzama Digital

A mis padres por su inestimable apoyo y dedicación;
y a mi sobrino Álvaro con todo mi cariño.

I. CONSIDERACIONES PREVIAS

Lo que constituye una realidad es que, el uso de Internet multiplica las oportunidades de recopilar datos, elaborar perfiles de los usuarios, personalizar la publicidad y promoción en la red y, asimismo, contribuye al riesgo de incumplimiento de los derechos y libertades de las personas, en especial el derecho a la vida privada. Ciertamente, en este ámbito digital resulta esencial respetar todos los derechos y libertades fundamentales y, en particular, el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de datos de carácter personal, la libertad de pensamiento, de conciencia, y de religión, la libertad de expresión e información, y, la libertad de empresa. Esto no impide que, se puedan vulnerar los derechos fundamentales como el derecho al honor, a la intimidad y la propia imagen; asimismo, se puede acceder por los usuarios a un listado de información de una persona de manera automatizada, instantánea, y continuada en el tiempo sin que tal información caiga en el olvido –memoria digital "eterna"- y, además compartirla en tiempo real; y, en fin, se puede llevar a cabo una utilización y cesión lícita –consentida- o ilícita de los datos. Asimismo, los motores de búsqueda ponen a disposición de los usuarios a través de operaciones de indexación, rastreo y almacenamiento una ingente cantidad de información que, puede tener un importante impacto en la privacidad y en la protección de datos.

Por otra parte, el Big Data –datos masivos o macrodatos-, cloud computing o computación en la nube, internet de las cosas (IoT), inteligencia artificial y blockchain o cadena de bloques como últimas tecnologías que, si bien pueden aportar beneficios a la sociedad, exigen, asimismo, que se garantice de forma adecuada la privacidad y la protección de datos de los interesados y usuarios de tales tecnologías.

Ahora bien, la inclusión del vigente artículo 18.4 puso de relieve que el constituyente era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona. Esto es, incorporando un instituto de garantía "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término

no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales", pero que también es "en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona no provenientes de un uso ilegítimo de tratamiento mecanizado de datos, lo que la Constitución llama "la informática"" (Sentencia del Tribunal Constitucional 254/1993, de 20 de julio, *Fundamento Jurídico sexto*). Con ello, el constituyente quiso garantizar mediante el citado artículo 18.4 de la Constitución Española no sólo un ámbito de protección específico sino también más idóneo que, el que podía ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del citado precepto. Pues, bien el Tribunal Constitucional en sentencia 94/1998, de 4 de mayo señala que, nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos (*habeas data*) y sobre su uso y destino para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos comprende la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que, justificó su obtención[1]; y, en sentencias 290/2000 y 292/2000, ambas de 30 de noviembre, configuran el derecho a la protección de datos como un derecho autónomo e independiente[2]. Asimismo, se ha considera el derecho a

[1] RTC 1998/94. *Fundamento de Derecho cuarto.*

[2] La sentencia 290/2000, de 30 de noviembre (RTC 2000/290) en su *Fundamento de Derecho 7* ha declarado que resulta procedente recordar que el artículo 1 de la LORTAD contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, en sí mismo "un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama "la informática (…). En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos". Y añade en su *Fundamento de Derecho 11* que "la LORTAD ha sido dictada en cumplimiento del mandato contenido en el artículo 18.4 CE de limitar el uso de la informática para garantizar ciertos derechos fundamentales y el pleno ejercicio de los derechos de los ciudadanos, de manera que si se considera la actividad aquí examinada como meramente instrumental o accesoria de otras materias competenciales, es claro que con este planteamiento se está desvirtuando cual es el bien jurídico constitucionalmente relevante, que no es otro que la protección de los datos de carácter personal frente a un tratamiento informático que puede lesionar ciertos derechos fundamentales de los ciudadanos o afectar al pleno ejercicio de sus derechos, como claramente se desprende del tenor de dicho precepto constitucional". Por su parte, la sentencia 292/2000, de 30 de noviembre (RTC 2000/292) señala, asimismo, al respecto que "el artículo 18.4 CE contiene, en los términos de la STC 254/1993, un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo "un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática", lo que se ha dado en llamar "libertad informática" (F. 6, reiterado luego en las

la protección de datos como una manifestación del derecho a la dignidad de la persona y al libre desarrollo de la personalidad contenidos en el artículo 10.1 de la Constitución[3].

SSTC 143/1994, F. 7, 11/1998, F. 4, 94/1998, F. 6, 202/1999, F. 2). La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (artículo 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático ("habeas data") y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, F. 5, 94/1998, F. 4)". Estamos ante un derecho a la protección de datos personales, libertad informática, autodeterminación informativa o *habeas data*, de creación jurisprudencial y no ante un derecho fundamental en sentido propio. Interesa destacar que el Tribunal Constitucional viene a considerar este derecho como "derecho de control sobre los datos relativos a la propia persona" y "a diferencia del derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (artículo 81.1 CE), bien regulando su ejercicio (artículo 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran" (FJ 5). De lo dicho resulta que "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que, le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele (FJ 7). Vid., asimismo, la sentencia del Tribunal Supremo, Sala de lo Civil, de 6 de octubre de 2014 (RJ 2014/5778).

[3] El voto particular a la STC 290/2000 formulado por el Magistrado D. Manuel Jiménez de Parga y Cabrera, al que presta su adhesión el Magistrado D. Rafael de Mendizábal Allende dispone que, nuestro Tribunal reconoce y protege ahora un derecho fundamental, el derecho de libertad informática, que no figura en la Tabla del texto de 1978. Y este derecho a la libertad informática debe tener como eje vertebrador el artículo 10 de la CE, ya que es un derecho inherente a la persona. Tal vinculación a la dig-

En este contexto, la regulación relativa a la protección de los datos personales se contiene en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal (LOPD) que traspuso a nuestro ordenamiento lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal (conocida como LORTAD)[4]. Esta Ley nació con una amplia vocación de generalidad, y así preveía en su artículo 1 que "tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal". Por lo que, comprendía tanto el tratamiento automatizado como el no automatizado de los datos de carácter personal. Se componía de un total de 49 artículos, seis disposiciones adicionales, tres disposiciones transitorias, una única disposición derogatoria y tres disposiciones finales. Después de concretar en su Título primero el objeto, ámbito de aplicación y definiciones; el Título II lo dedica a los principios de protección de datos (artículos 4 a 12); el Título III a los derechos de las personas (artículos 13 a 19); el Título IV a ciertas disposiciones sectoriales (artículos 20 a 32); el Título V a los movimientos internacionales de datos (artículos 33 y 34); el Titulo VI a la Agencia de Protección de Datos (artículos 35 a 42); y el Título VII a las infracciones y sanciones (artículos 43 a 49). Esta Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar (artículo 1). En cuando a su ámbito de aplicación material y territorial, se indicaba respecto del primer ámbito que, esta Ley Orgánica era de aplicación a los datos de carácter

nidad de la persona proporciona a la libertad informática la debida consistencia constitucional. También son preceptos que facilitan la configuración a la libertad informática los contenidos en el artículo 18.1 (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y 20.1 (libertad de expresión y de información) entre otros, así como los Tratados y Acuerdos Internacionales en cuanto son guías de interpretación constitucional (artículo 10.2 CE) (punto 3).

[4] Tenía como finalidad hacer frente a los riesgos que para los derechos de la personalidad podían suponer el tratamiento de datos por medios informáticos. Se regulaba el tratamiento automatizado de datos; se destacaba la importancia del consentimiento o autodeterminación del individuo que posibilitaba concretar el nivel de protección de datos a ella referente. Además de exigirse que el afectado antes de la recogida de datos debía ser informado del uso que se les podían dar a sus datos, con el objeto de consentir con cabal conocimiento. Se regulaban, asimismo, los derechos de acceso, rectificación y cancelación como piezas centrales del sistema cautelar o preventivo instaurado por la ley. Se hacía referencia a los datos sensibles y no sensibles, con unas exigencias mayores con relación a los primeros; y, se disponía un mecanismo de inscripción de los ficheros en el Registro General de Protección de Datos.

personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado (artículo 2.1)[5]; y en cuanto al segundo ámbito, esta Ley Orgánica se aplicaba: 1. Al tratamiento de datos de carácter personal sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento; 2. Respecto al responsable del tratamiento no establecido en territorio español, cuando le sea de aplicación la legislación española con relación a las normas de Derecho Internacional público; 3. Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en el territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito (artículo 2.1)[6]. En este contexto, se consideraba que, el régimen de protección de datos de carácter personal que se establece en esta Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas; c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos (artículo 2.2). En todo caso, se regirían por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los tratamientos de datos personales relativos: a) Los ficheros regulados por la legislación electoral; b) Los que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación estatal o autonómica sobre la función estadística pública; c) Los que tengan por objeto el almacenamiento de los datos contenido en los informes personales de calificación a que se refiere la legislación del régimen personal de las fuerzas Armadas; d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes; y e) Los procedentes de imágenes y sonidos

[5] Respecto a este ámbito material de aplicación y la referencia al tratamiento de datos de personas físicas de la derogada Ley Orgánica 15/1999, vid., la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, sección 1ª, de 9 de junio de 2011 (JUR 2011/214029) (*Fundamento de Derecho tercero*).

[6] La sentencia del Tribunal de Justicia de la Unión Europea, Sala Tercera, de 28 de julio de 2016 (TJCE 2016/296) en el asunto C-191/15 caso Verein für Konsumenteninformation contra Amazon EU Sarl en relación con la determinación de la legislación de protección de datos aplicable en relación con las empresas de comercio electrónico que, dirigen sus actividades a Estado en que no tienen establecimiento y la aplicación de la doctrina de la sentencia Google y Weltimmo estableció que, "el tratamiento de datos personales efectuado por una empresa de comercio electrónico, se rige por el Derecho del Estado miembro al que dicha empresa dirige sus actividades, si esa empresa efectúa el tratamiento de los datos en cuestión en el marco de las actividades de un establecimiento situado en un Estado miembro. Corresponde al órgano jurisdiccional nacional determinar si ese es el caso" (apartado 81).

obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia (artículo 2.3).

Ahora bien, con el fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos y pese a la derogación expresa de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal, el legislador español declaró subsistentes las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la citada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal (Disposición transitoria tercera), a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

En desarrollo de la Ley Orgánica 15/1999 se aprobó el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal (en adelante, RPD). Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que, en estos años de vigencia de la Ley se ha demostrado que, precisan de un mayor desarrollo normativo.

Por tanto, se aprobó este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema. Al respecto el título III se ocupaba de una cuestión tan esencial como los derechos de las personas en este ámbito[7]. Estos derechos de acceso, rectificación, cancelación y oposición al

[7] Además lleva a cabo un desarrollo de otras materias como la relativa al consentimiento para el tratamiento de datos y el deber de información (Capitulo II –artículo 12 a 19-); sobre los encargados del tratamiento de datos (Capítulo III –artículos 20 a 22-); los ficheros de información sobre solvencia patrimonial y crédito (Título IV Disposiciones aplicables de determinados ficheros de titularidad privada, Capítulo I –artículos 37 a 44-); los tratamientos para actividades de publicidad y prospección comercial

tratamiento, según ha afirmado el Tribunal Constitucional en la mencionada sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y "sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer".

En este contexto, hay que destacar en lo que representa la protección de datos en el ámbito internacional, el Convenio Europeo de Derechos Humanos y de las libertades fundamentales de 4 de noviembre de 1950 reconoce en su artículo 8 el derecho al respeto de la vida privada y familiar, aunque no incluye expresamente el derecho a la protección de datos personales. Así dispone que "toda persona tiene derecho al respecto de su vida privada y familiar, de su domicilio y de su correspondencia". Por lo que, incorpora el derecho a la privacidad, esto es, el respeto de la vida privada y familiar del hogar y de la correspondencia y prohíbe en el apartado 2 cualquier injerencia en el ejercicio del derecho a la privacidad, excepto si "está prevista por la ley" y "constituye una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás", esto es, con la finalidad de satisfacer determinados tipos de interés público específicamente enumerados y de carácter imperativo. El artículo 8 del Convenio se centra, pues, en la protección de la vida privada y exige una justificación de cualquier injerencia en la privacidad. Este enfoque se basa en una prohibición general de injerencia en el derecho a la privacidad que, no obstante permite excepciones, si bien solo en condiciones estrictamente definidas. En los casos en los que exista una "injerencia en la privacidad" se impone la exigencia de una base jurídica, así como la especificación de una finalidad legítima como condición precisa para evaluar y analizar la necesidad de la injerencia. Operar con este enfoque, explica que, en el Convenio no se proporcionen una lista de posibles fundamentos jurídicos, sino que se centre en la necesidad de un fundamento jurídico y en los criterios que, dicha base jurídica debe cumplir[8]. Ahora bien, en la medida en que la protección de los datos personales está estrechamente unido a la privacidad y puede desempeñar un

(Título IV Disposiciones aplicables de determinados ficheros de titularidad privada, Capítulo II –artículos 45 a 51-); las transferencias internacionales de datos (Título VI, Capítulos I y II –artículos 65 a 70-); las medidas de seguridad en el tratamiento de datos de carácter personal (Título VIII, Capítulos I, II, III y IV –artículos 79 a 114-); y el procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición (Título IX, Capítulo II –artículos 117 a 119-).

[8] Vid., el Dictamen del Grupo de Trabajo del Artículo 29 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento en virtud del artículo 7 de la Directiva 95/46/CE adoptado el 9 de abril de 2014 (WP 217), pp. 7 y 8.

papel sustancial en el ejercicio de otros derechos como la libertad de expresión o las libertades de religión y conciencia, el Consejo de Europa adoptó el 28 de enero de 1981, el Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, conocido habitualmente como Convenio número 108, en el que se señala que "es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respecto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamiento automatizado". Representa el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos y tiene como finalidad este Convenio "garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respecto de su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter persona correspondientes a dicha persona" (artículo 1). Tiene un total de siete capítulos, de los que el capítulo VI se refiere a las enmiendas (artículo 21) y el capítulo VII a las cláusulas finales como la entrada en vigor (artículo 22), la adhesión de los Estados no miembros (artículo 23) y la cláusula territorial que establece que "cualquier Estado podrá designar en cualquier momento de la firma o depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el territorio o los territorios a los cuales se aplicará el presente convenio" (artículo 24). A los efectos del presente Convenio, datos de carácter personal significa "cualquier información relativa a una persona física identificada o identificable"; por fichero automatizado "cualquier conjunto de informaciones que sean objeto de un tratamiento automatizado" y por tratamiento automatizado "las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de los procedimientos automatizados: registro de datos, aplicación de esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión". Se recogen un conjunto de principios y garantías en su Capítulo II bajo la rúbrica "Principios básicos para la protección de datos", así los principios de "calidad" (artículo 5), "seguridad" (artículo 7) e "información" (artículo 8) y los derechos de confirmación (artículo 8 b)); de comunicación (artículo 8 a)) y de rectificación y borrado (artículo 8 c)). Asimismo, establece en su artículo 18 un comité consultivo (T-PD) encargado entre otras tareas, de elaborar propuestas con el fin de facilitar o mejorar la aplicación del Convenio, presentar propuestas de enmienda del Convenio y pronunciarse sobre cuestiones relativas a su aplicación. La Agencia Española de Protección de Datos forma parte del comité que, a lo largo de treinta años de actividad ha elaborados numerosos informes y opiniones y estudios, así como la preparación de recomendaciones del Comité de Ministros del Consejo sobre cuestiones relativas a la protección de datos en redes

sociales, el perfilado o en el ámbito laboral. El Convenio fue ampliado a través de un protocolo en el año 2001. En 2010, el Comité de Ministros inició un proceso de revisión del Convenio número 108. El comité consultivo trabajó durante 2011 y 2012 en la preparación de un documento técnico de propuesta de reforma que remitió al Comité de Ministros a finales de 2012.

Ahora bien, los datos personales y el respeto a la vida privada son derechos fundamentales y necesitados de la adecuada protección. De ahí que, el Parlamento Europeo haya insistido siempre en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada; y, considere necesario una regulación europea de protección de datos destinada a fortalecer los derechos de los ciudadanos que, les brinde un mayor control de sus datos y que garantice la protección de su privacidad en la era digital. Antes de la entrada en vigor del Tratado de Lisboa, la legislación relativa a la protección de datos en el espacio de libertad, seguridad y justicia estaba repartida entre dos pilares, el primero relativo a la protección de datos con fines privados y comerciales, sometidos al método comunitario, y el segundo a la protección de datos con fines de aplicación de la ley, con toma de decisiones a escala intergubernamental. En consecuencia, el proceso decisorio se regía por dos normativas diferentes. La estructura de pilares desapareció con el Tratado de Lisboa que, aporta una base más sólida para desarrollar un sistema de protección de datos más claro y eficaz al tiempo que, prevé nuevas competencias para el Parlamento Europeo que, se convierte en colegislador y tanto al Parlamento como al Consejo les obliga a velar por la protección de datos en todos los ámbitos de la legislación europea. En otras palabras, otorga carta de naturaleza a un marco global en materia de protección de datos aplicable al sector privado y al sector público, tanto en el seno de los Estados miembros, como en el de las instituciones y organismos europeos[9]. Así el artículo 16 del Tratado Fundacional de la Unión Europea dispone, al respecto que, el Parlamento Europeo y el Consejo establecen las normas sobre protección de las personas físicas respecto al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión. En este contexto, como instrumentos normativos en materia de protección de datos, hay que señalar que, la Carta de los Derechos fundamentales de la Unión Europea que, fue proclamada por el Parlamento Europeo, el Consejo de la Unión Europea, y la Comisión europea el 7 de diciembre de 2000 en Niza, reconoce en sus artículos

[9] El programa de Estocolmo "Una Europa abierta y segura que sirva y proteja al ciudadano" DO C115, de 4 de abril de 2010 p. 1 en el punto 10 declara explícitamente que, la Unión Europea debe asegurar una estrategia global de protección de datos dentro de la Unión y en sus relaciones con otros países.

7 y 8 el respeto a la vida privada y la protección de los datos de carácter personal como derechos fundamentales estrechamente relacionados pero independientes. Al respecto establece el artículo 7 que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"; asimismo, el artículo 8 dispone que "1. Toda persona tiene derecho a la protección de datos de carácter personal que le conciernen; 2. Estos datos se tratan de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Todas persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación; 3. El respeto de estas normas quedará sujeta al control de una autoridad independiente"[10]; y, el artículo 52.1 señala que "cualquier limitación del ejercicio de los derechos y libertades públicas reconocidas por la presente Carta debe ser establecido por la ley y respetar el contenido esencial de dichos derechos y libertades", por lo que, dentro del principio de proporcionalidad "solo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás". Una revisión de la Carta tuvo lugar el 12 de diciembre de 2007 en Estrasburgo, antes de la firma del Tratado de Lisboa.

Esta Carta está integrada en el Tratado de Lisboa –cuya entrada en vigor tuvo lugar el 1 de diciembre de 2009-[11] y es jurídicamente vinculante para las instituciones y órganos de la Unión, así como para los Estados miembros cuando aplican el Derecho de la Unión con la entrada en vigor del citado Tratado en diciembre de 2009. Ahora tiene la misma validez jurídica que, los Tratados de la Unión Europea y ha creado una nueva base jurídica.

Ahora bien, como consecuencia de la antigua estructura de pilares, actualmente ya no están en vigor algunos de los instrumentos legislativos pertenecientes al primer pilar como, la citada Directiva 95/46/CE relativa a la protección de datos que, tenía dos objetivos, por un lado, garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales; y, por

[10] La sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 29 de enero de 2008 en el asunto C-275/06, Productores de Música de España (Promusicae) y Telefónica de España, S.A. señala en su apartado 64 que: "Con arreglo al segundo considerando de la Directiva 2008/58, ésta pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta. En especial, pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de ésta. Dicho artículo 7 reproduce, en esencia, el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950, que garantiza el respeto a la intimidad, y el artículo 8 de dicha Carta proclama expresamente el derecho a la protección de los datos personales".

[11] Véase el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE).

otro, que los Estados miembros no restringieran ni prohibieran la libre circulación de datos personales entre los Estados miembros (artículo 1)[12]. Se trataba de una directiva de máximos, puesto que pretendía una armonización completa de las legislaciones de los Estados miembros[13] y de carácter horizontal "en la medida en que resultaba de aplicación a los diferentes supuestos de tratamiento de datos personales, sin perjuicio de que para alguno de ellos pueda haber reglas específicas en otras normas"[14]; otros permanecen en vigor como la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de junio de 2002 relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónica (Directiva sobre la privacidad y las comunicaciones electrónicas), modificada por la Directiva 2009/136/CE[15]; la Directiva 2006/24/CE del Parlamento

[12] El artículo 94 del Reglamento General de Protección de Datos dispone al respecto que: "1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018. 2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento".

[13] Así lo ha declarado la sentencia del Tribunal de Justicia de 6 de noviembre de 2003 (asunto C-101/01) que tiene por objeto una petición dirigida al Tribunal de Justicia por Göta hovrätt (Suecia), destinada a obtener en el proceso penal seguido ante dicho órgano jurisdiccional contra Bodil Lindqvist (apartados 96 y 97). Al respecto dispone en su apartado 96 que: "Por tanto, la armonización de dichas legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una armonización completa. Desde este punto de vista, la Directiva 95/46 trata de asegurar la libre circulación de datos personales, garantizando al mismo tiempo un alto nivel de protección de los derechos e intereses de las personas titulares de dichos datos". Y, el apartado 97 añade que: "es cierto que la Directiva 95/46 reconoce a los Estados miembros un margen de apreciación en ciertos aspectos y que les permite mantener o establecer regímenes particulares para situaciones específicas, tal y como lo demuestra un gran número de sus disposiciones. No obstante, dichas posibilidades deben emplearse tal y como dispone la Directiva y de conformidad con su objetivo, que consiste en mantener un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad".

Por su parte, la sentencia del Tribunal de Justicia de la Unión Europea, de 20 de mayo de 2003 en los asuntos acumulados C-465/00, C-138/01 y C-139/01, Österreichischer Rundfunk dispone al respecto que, ciertas disposiciones de la Directiva 95/46/CE pueden ser invocadas directamente ante los órganos jurisdiccionales nacionales (apartados 95-101). En concreto el apartado 101 de la sentencia señala que: "Procede, por tanto, responder a la segunda cuestión que, los artículos 6 apartado 1 letra c) y 7 letras c) y e) de la Directiva 95/46 son directamente aplicables, en el sentido que un particular puede invocarlos ante los órganos jurisdiccionales nacionales para evitar la aplicación de normas de Derecho interno contrarias a dichas disposiciones".

[14] DE MIGUEL ASENSIO P.A., *Derecho Privado de Internet*, 5ª ed., Civitas Thomson Reuters, Navarra 2015, p. 301, asimismo, precisa que: "Especial alcance armonizador presenta la Directica 95/46/CE, que contiene un régimen elaborado, constitutivo de un verdadero derecho común europeo sobre protección de datos personales y que parece haber cumplido su principal objetivo: asegurar un alto nivel de protección de los datos personales de la UE (EEE) y garantizar la libre circulación de esos datos".

[15] Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios

Europeo y del Consejo, de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (declarada inválida por la sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 8 de abril de 2014 al constituir una injerencia de especial gravedad en la vida privada y la protección de datos)[16]; y el Reglamento (CE) número 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios; y, como instrumentos pertenecientes al antiguo segundo pilar como la Decisión Marco 2008/977/JAI, del Consejo de 27 de noviembre relativa a la protección de datos tratados en el marco de cooperación policial y judicial en materia penal. Se aplica a los datos policiales y judiciales intercambiados entre Estados miembros, autoridades y sistemas conexos de la Unión, sin que se incluyan los datos nacionales.

---

en relación con las redes y los servicios de comunicaciones electrónicas; la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de consumidores.

[16] La sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 8 de abril de 2014 en los asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland Ltd y Minister for Communications, Marine and Natural Resources argumenta al respecto que: "De ello se deduce que la obligación impuesta por los artículos 3 y 6 de la Directiva 2006/24/CE a los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar durante un determinado período datos relativos a la vida privada de una persona y a sus comunicaciones, como los que se indican en el artículo 5 de dicha Directiva, constituye en sí misma una injerencia en los derechos garantizados por el artículo 7 de la Carta" (apartado 34). Asimismo, ha de señalarse que, como indicó el Abogado General concretamente en los puntos 77 y 80 de sus Conclusiones "la injerencia que supone la Directiva 2006/24 en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta resulta de gran magnitud y debe considerarse especialmente grave. Además, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada, es objeto de una vigilancia constante, como afirmó el Abogado General en los puntos 52 y 72 de sus Conclusiones" (apartado 37). A esto se añade que "En lo que atañe al contenido esencial del derecho fundamental al respeto de la vida privada y de los otros derechos reconocidos en el artículo 7 de la Carta, debe señalarse que, aunque la conservación de datos que, la Directiva 2006/24 impone, constituye una injerencia especialmente grave en dichos derechos, no puede vulnerar dicho contenido puesto que, como se desprende de su artículo 1 apartado 2, la Directiva no permite conocer el contenido de las comunicaciones electrónicas como tal" (apartado 39); y, esta conservación de datos tampoco puede vulnerar el contenido esencial del derecho a la protección de datos de carácter personal reconocido en el artículo 8 de la Carta "ya que la Directiva 2006/24 establece, en su artículo 7, una regla relativa a la protección y a la seguridad de los datos según la cual, sin perjuicio de las disposiciones adoptadas con arreglo a las Directivas 95/46 y 2002/58, los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de telecomunicaciones deben respetar determinados principios de protección y de seguridad de los datos" (apartado 40).

Con la Directiva 95/46/CE se creó el llamado Grupo de Trabajo del Artículo 29 (GT29). Su denominación vino dada por el artículo 29 de la misma, y al que se atribuyó un carácter consultivo e independiente y sus funciones se encontraban recogidas en el artículo 30.1 de la citada Directiva. Entre las labores del Grupo ha estado la elaboración de dictámenes, entre los que podemos destacar los siguientes: Dictamen 4/2007, adoptado el 20 de junio sobre el concepto de datos personales (WP 136); el Dictamen 1/2008, emitido el 4 de abril de 2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda (WP 148); el Dictamen 8/2010 emitido el 16 de diciembre sobre el Derecho aplicable (WP 179); y el Dictamen 1/2010, adoptado el 16 de febrero sobre los conceptos de "responsable de tratamiento" y "encargado del tratamiento" (WP 169). Más recientemente, se publicaron las primeras guías sobre el Reglamento General de Protección de Datos con el objeto de fijar una serie de directrices prácticas que, ayudasen a los responsables y encargados del tratamiento de datos a adaptarse al nuevo marco normativo europeo. Así el 13 de diciembre de 2016 se publicaron las siguientes Guías: las Directrices sobre el derecho a la portabilidad de los datos (GT 242); las Directrices sobre los delegados de protección de datos (DPD) (GT 243); y, las Directrices para determinar la autoridad supervisora principal de un responsable o encargado del tratamiento (GT 244).

Ahora bien, ante la cuestión de si la legislación de la Unión Europea en materia de protección de datos es capaz de hacer frente plena y eficazmente a los nuevos retos en materia de protección de datos, la Comisión Europea inició un examen del marco jurídico europeo, con una conferencia de alto nivel en mayo de 2009, seguida de una consulta pública que duró hasta finales de 2009. Asimismo, se iniciaron varios estudios a tal fin[17]. Los resultados obtenidos conformaron que, los principios fundamentales de la Directiva 95/46/CE seguían siendo válidos, que, convenía preservar su neutralidad desde el punto de vista tecnológico; si bien, se identificaron varios problemas cuya resolución exigía retos específicos como: 1. Abordar el impacto de las nuevas tecnologías, aunque a ello había respondido parcialmente la Directiva 2002/58/CE, de 12 de julio relativa al tratamiento de los datos personales y a la protección de la intimidad n el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) –modificada por la Directiva 2009/13/CE-; 2. Reforzar la dimensión del mercado interior de la protección de datos, siendo insuficiente la armonización de las legislaciones de los Estados miembros en materia de protección de datos, a pesar de la existencia de un marco jurídico común de la UE; 3. Hacer frente a la globalización

[17] Véase, el *Study on the economic benefits of privacy enchancing technologies*, London Economics, julio de 2010; y, *Comparative study on different approaches to new privacy challenges in particular in the light of technological developments*, enero de 2010.

y mejorar las transferencias internacionales de datos; 4. Consolidar las disposiciones institucionales para la aplicación efectiva de las normas sobre protección de datos; y, 5. Mejorar la coherencia del marco jurídico que regula la protección de datos.

Por otra parte, los retos mencionados pusieron de manifiesto la necesidad que la Unión Europea elaborase un enfoque global y coherente que, garantizase el pleno respeto del derecho fundamental a la protección de los datos personales, tanto en la Unión Europea, como fuera de ésta. En este contexto, y atendiendo a los requerimientos y sugerencias de las diferentes instancias europeas, el 25 de enero de 2012 la Comisión publicó un amplio paquete legislativo destinado a reformar la legislación de la Unión en materia de protección de datos. La reforma persigue salvaguardar los datos personales en todo el territorio de la Unión, aumentando el control de los datos por parte de los usuarios y reduciendo los costes para las empresas. Los avances tecnológicos y la globalización han cambiado profundamente los métodos de recogida, acceso y uso de los datos. Además, los 28 Estados miembros han aplicado de manera distinta las normas de 1995. Se consideraba que, un único texto normativo eliminará la fragmentación actual y la onerosa carga administrativa que, el tratamiento de datos conlleva. Asimismo, contribuirá al aumento de la confianza de consumidores en los servicios en línea, lo que proporciona un impulso muy necesario para el crecimiento, el empleo y la innovación en Europa. El paquete incluye una Comunicación sobre los principales objetivos políticos de la reforma, una propuesta de Reglamento General para modernizar los principios consagrados en la Directiva sobre Protección de Datos de 1995 y una propuesta de Directiva específica sobre el tratamiento de los datos personales en el marco de la cooperación policial y judicial en materia penal. En diciembre de 2015, el Parlamento (en el ámbito de sus comisiones) y el Consejo (en el ámbito de los embajadores) alcanzaron un acuerdo sobre las nuevas normas en materia de protección de datos tras casi tres años de largas negociaciones. Las nuevas normas se publicaron el 27 de abril de 2016 y son de aplicación desde el 25 de mayo de 2018: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) –corrección de errores del Reglamento (UE) 2016/679 publicado en el Diario Oficial de la Unión Europea el 23 de mayo de 2018 en el que se modifican la redacción de algunos preceptos- (RGPD); y 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 o enjuiciamiento de

infracciones penales o de ejecución de sanciones penales y la libre circulación de dichos datos y, por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[18].

La adopción del Reglamento General de Protección de Datos responde a la rápida evolución tecnológica y la globalización que, han planteado nuevos retos para la protección de los datos personales que, la Directiva 95/46/CE no pudo tener en cuenta cuando se aprobó. Se constata una realidad como es que, las personas físicas difunden cada vez un mayor volumen de información personal a escala mundial. Además, la tecnología ha transformado tanto la economía como la vida social, y, asimismo, ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales. Con este Reglamento se pretende garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión; de ahí que, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros; y, en consecuencia, garantizarse en toda la Unión Europea que, la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. Este Reglamento General de Protección de Datos supone, pues, la revisión de las bases legales del modelo europeo de protección de datos, y no una mera actualización de la vigente normativa, en el que se pretende reforzar la seguridad jurídica y la transparencia en el tratamiento de los datos. Se incorpora, por ello, como novedad de gran relevancia el principio de responsabilidad proactiva ("*accountability*"), principio que inspira el modelo de cumplimiento previsto en el Reglamento. De ahí que, la reforma de la regulación de protección de datos constituya un cambio del modelo tradicional para afrontar las medidas que garantizan la protección de los datos hacia un modelo más dinámico, adaptado a la profunda transformación tecnológica que, se está produciendo en el ámbito del tratamiento de la información personal y, por ende, enfocado a la gestión continua de los riesgos potenciales asociados al tratamiento de los datos. Asimismo, este Reglamento General regula en términos

[18] Por su parte, la Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE en su considerando número 85 señala que "todo tratamiento de datos personales en el marco de la presente Directiva debe respetar los derechos fundamentales, incluidos el respeto a la vida privada y familiar y el derecho a la protección de datos de carácter personal establecidos en los artículos 7 y 8 respectivamente de la Carta y debe cumplir con la Directiva 2002/58/CE y el Reglamento (UE) 2016/679"; y, en su artículo 28 dispone en esta línea que "el tratamiento de datos personales efectuado en el marco de la presente Directiva se llevará a cabo de conformidad con el Directiva 2002/58/CE y el Reglamento (UE) 2016/679".

de igualdad las bases jurídicas que, legitiman el tratamiento, sin que primen ninguna de ellas sobre las otras, frente a la precisión de la derogada Directiva 95/46/CE que, dotaba de relevancia al consentimiento con respecto a las demás bases jurídicas que legitimaban el tratamiento de los datos. En fin, en la nueva normativa europea de protección de datos se opta por una doble estrategia de prevención y flexibilización, pues, no todas las organizaciones han de aplicar íntegramente las medidas contenidas en el Reglamento. Se trata de una norma muy extensa pues, consta de 173 considerandos previos –que es un desarrollo y explicación de la regulación normativa- y 99 artículos agrupados en once capítulos. Según dispone su artículo 99 este Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea" –por lo que ya está en vigor desde el 24 de mayo de 2016-; sin embargo, solo se ha considerado aplicable a partir del 25 de mayo de 2018, concediendo con ello un tiempo prudencial para que las empresas y los Estados se adapten a la nueva normativa de protección de datos. Como tal Reglamento de la Unión y según dispone el citado artículo 99 en su parte final "el presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro".

Ciertamente, este Reglamento General de Protección de Datos es una norma directamente aplicable, que no requiere normas internas de transposición, ni tampoco, en la mayoría de los casos, normas de desarrollo o de aplicación (artículo 288 del TFUE)[19]; no obstante, la existencia de normas genéricas de remisión al Derecho interno de cada Estado miembro y de un buen número de habilitaciones que, se contienen en el propio Reglamento para regular determinadas materias[20].

---

[19] El Reglamento como tal norma jurídica posee alcance general o *erga omnes* y es obligatorio en todos sus elementos y directamente aplicable.

[20] De todas formas, hay que tener presente que, el Reglamento General de Protección de Datos prevalece sobre las normas nacionales por el principio de prevalencia del derecho comunitario. Al respecto establece la sentencia del Tribunal Constitucional, Pleno, de 18 de diciembre de 2014 (RTC 2014/215) en su *Fundamento de Derecho tercero* apartados 8, 9 y 10 que: "(…) Así desde la incorporación de España a las Comunidades Europeas "se integró en el ordenamiento español un sistema normativo autónomo dotado de un régimen de aplicabilidad específico, basado en el principio de prevalencia de sus disposiciones propias frente a cualquiera del orden interno con las que pudieran entrar en contradicción" (STC 1/2004, de 13 de diciembre FJ 7º y en sentido parecido STC 26/2014, de 13 de febrero, FJ 3º). De acuerdo con lo anterior, la relación entre el Derecho de la Unión Europea y el Derecho nacional se rige por el principio de primacía (…) conforme al cual, las normas de la Unión Europea "tienen capacidad de desplazar a otras en virtud de su aplicación preferente o prevalente" (STC 1/2004, de 13 de diciembre, FJ 4º; y STC 145/2012, de 2 de julio (RTC 2012, 145) FJ 5º), pues no solo "forman parte del acervo comunitario incorporado a nuestro ordenamiento" sino que tienen "un efecto vinculante", de manera que opera "como técnica o principio normativo" destinado a asegurar su efectividad (STC 145/2012, de 2 de julio, FJ 5º y en sentido parecido SSTC 28/1991, de 14 de febrero, FJ 6º; y 64/1991, de 22 de marzo, FJ 4º a)). Ahora bien, aunque esa vinculación "instrumentada con fundamento del artículo 93 CE, en el Tratado de adhesión (STC 64/1991, de 22 de marzo, FJ 4º a) es "el fundamento último de nuestra incorporación al proceso de

A tal fin en su considerando número 8 dispone que, cuando sus normas deban ser especificadas o restringidas por el Derecho de los Estados miembros, éstos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar al derecho nacional previsiones contenidas específicamente en el Reglamento y añade el considerando número 10 que "(…) El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales ("datos sensibles"). En este sentido, este Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito". Por lo que el legislador nacional de cualquier Estado miembro puede completar la regulación contenida en el Reglamento General de Protección de Datos y hacerla más comprensible a los destinatarios, como asimismo, regular alguna situación concreta respetando, no obstante, las disposiciones y principios del mismo.

De todas formas, la eficacia directa de este Reglamento General de Protección de Datos no impide que, haya normas nacionales sobre la materia. A tal fin, se ha aprobado la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Consta de noventa

integración europea y de nuestra vinculación al derecho comunitario" (STC 1/2004, de 13 de diciembre, FJ 2º; y STC 100/2012, de 8 de mayo, FJ 7º), sin embargo, "no significa que por mor del artículo 93 se haya dotado a las normas del Derecho comunitario europeo de rango y fuerza constitucionales" (SSTC 28/1991, de 14 de febrero, FJ 4º; 64/1991, de 22 de marzo, FJ 4º a); y, 134/2011, de 20 de julio, FJ 6º), ni que el Derecho comunitario, originario o derivado, constituya canon de constitucionalidad de las normas de rango de ley (SSTC 235/2000, de 5 de octubre, FJ 11º; 12/2008, de 29 de enero, FJ 2º; y 136/2011, de 13 de septiembre, FJ 12º; y en sentido parecido, SSTC 49/1988, de 21 de marzo, FJ 14º; y 28/1991, de 14 de febrero, FJ 5º). Sí implica, por el contrario, con carácter general que los Estados miembros no solo adoptarán "todas las medidas generales o particulares apropiadas para asegurar el cumplimiento de las obligaciones derivadas de los tratados o resultantes de los actos de las institucionales de la Unión" (artículo 4.3 TUE), sino también "todas las medidas de Derecho interno necesarias para la ejecución de los actos jurídicamente vinculantes (artículo 291.1 TFUE) y a título particular que "los Estados miembros coordinarán sus políticas económicas en el seno de la Unión" (artículo 5.1 del TFUE)".

Vid., asimismo, PASCUAL HUERTA P., "Definición, funciones y estructura de los sistemas de información crediticia. El impacto del Reglamento General de Protección de Datos de la Unión Europea", *La Prevención del Sobreendeudamiento privado. Hacia un préstamo y consumo responsable, directora Matilde Cuena Casas*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017, pp. 222-223 precisa, al respecto que, el Reglamento no implica la derogación automática de la normativa española de protección de datos; por tanto "no sólo las normas estatuidas, que básicamente son la LOPD y el RLOPD, sino el conjunto del derecho español de protección de datos, esto es, también la interpretación de la AEPD y de los tribunales sobre dicha normativa, continúan en vigor después de la fecha en que el nuevo Reglamento será aplicable, pero sólo en la medida que no se oponga a las disposiciones de este último". Dichas normas a las que se refiere el autor hay que, señalar que, ya no están en vigor.

y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales[21].

El Título I, relativo a las disposiciones generales, regula el objeto de esta ley orgánica, destacando en primer lugar, que se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento General de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el citado Reglamento y en esta Ley Orgánica. Asimismo, se indica que, las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía –autoridad catalana de protección de datos, la Agencia Vasca de Protección de Datos y el Consejo de transparencia y protección de datos de Andalucía-. En segundo lugar, es también objeto de esta ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución. A tal fin, resulta importante destacar la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, "Principios de protección de datos", se establece la no imputabilidad al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la

[21] Antes de la aprobación de la Ley Orgánica 3/2018, se dictó 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 estructuraba en tres capítulos y catorce artículos. El primer capítulo bajo la rúbrica "Inspección en materia de protección de datos" (artículos 1-2); el capítulo II "Régimen sancionador en materia de protección de datos" (artículos 3-6); y el Capítulo III "Procedimiento en caso de posible vulneración de la normativa de protección de datos (artículos 7-14). Ha sido derogado por la Disposición Derogatoria única apartado 2 de la citada Ley Orgánica 3/2018.

portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se hace referencia expresamente al deber de confidencialidad, al tratamiento de datos amparado por la ley, a las categorías especiales de datos y el tratamiento de datos de naturaleza penal. Con relación al consentimiento se establece, que se ha de proceder a una declaración o acción afirmativa del afectado, excluyendo lo que se conoce como "consentimiento tácito", y además que, el consentimiento del afectado si se refiere a una pluralidad de finalidades, será preciso que conste de manera específica e inequívoca que se otorga para todas ellas. En fin, se fija en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Asimismo, se regulan las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal -por ejemplo, las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras-.

Por otra parte, se alude a la posibilidad de imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de "listas negras" de sindicalistas, si bien los datos

de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la citada norma europea.

Con relación con el tratamiento de categorías especiales de datos, el artículo 9.2 también consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento General de Protección de Datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, posibilitando incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en concreto, respecto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición Adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III se dedica a los derechos de las personas y se adapta al Derecho español el principio de transparencia en el tratamiento del Reglamento Europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento de sus datos. Asimismo, se recoge la denominada "información por capas" aceptada ya en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las "cookies"), facilitando con ello al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En este Título, también se hace uso de la habilitación permitida por el considerando número 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando con ello la adecuada estructura sistemática del texto y se regulan los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad con expresa remisión a la regulación contenida en el Reglamento e incorporando mediante normas más específicas o restringidas elementos del mismo, garantizando con ello una adecuada estructura sistemática del texto.

En el Título IV se recogen "Disposiciones aplicables a tratamientos concretos", tratamientos lícitos respecto de los que cabe señalar, en primer lugar, aquellos respecto de los que el legislador establece una presunción *"iuris tantum"* de prevalencia

del interés legítimo del responsable cuando los tratamientos de datos cumplan con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos, cuando, precisamente, no se cumplan estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del Reglamento, como los relacionados con la función estadística o con fines de archivo de interés general.

El Título V se refiere al responsable y al encargado del tratamiento. Sobre el principio de responsabilidad activa se exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas técnicas y organizativas que procedan. Se divide en cuatro capítulos dedicados, respectivamente, a las obligaciones generales del responsable y encargado del tratamiento, al bloqueo de dato, al régimen del encargado del tratamiento, a los mecanismos de autorregulación y certificación y, a la figura del delegado de protección de datos que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. En todo caso, la designación del mismo ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos puede posibilitar la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional.

En línea, con el esquema contenido en sus antecedentes normativos, se regula el régimen de la Agencia Española de Protección de Datos y se hace referencia a las autoridades autonómicas de protección de datos y la necesaria cooperación entre las diferentes autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el "Procedimientos en caso de posible vulneración de la normativa de protección de datos". El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, hacia un modelo de "ventanilla única" en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación contenida en esta Ley Orgánica se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX regula el régimen sancionador, sobre la base normativa del Reglamento (UE) 2016/679, se establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. A tal fin se procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento General de Protección de Datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. Asimismo, se regulan los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los

procedimientos establecidos en el Reglamento Europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento General de Protección de Datos.

De todas formas, el Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones por lo que esta Ley Orgánica aprovecha la cláusula residual contenida artículo 83.2 de la norma europea referida a los factores agravantes o atenuantes. Por ello se hace referencia a los elementos que habrán de tenerse en cuenta para tal determinación a tener en cuenta, que son conocidos por los operadores jurídicos, pues, ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999.

Finalmente, el Título X de esta Ley reconoce y garantiza un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras. Así respecto al cómputo de plazo, la Disposición Adicional tercera que dispone que, los plazos establecidos en el Reglamento (UE) 2016/679 o en esta Ley Orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas: a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos; b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento; c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes; d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente. Asimismo, de conformidad

ÍNDICE