El derecho a la intimidad, la administración electrónica y la transparencia. La nueva protección europea de datos de las personas físicas

José Enrique Candela Talavero

Funcionario con habilitación de carácter nacional
Doctorando en Derecho

Extracto

Existe un equilibrio de necesario respeto en nuestro ordenamiento jurídico formado por el derecho a la intimidad, dentro del que se encuentra el tratamiento y la protección de datos y la buena administración, la transparencia y el derecho de acceso a la información, como guía del quehacer de los poderes públicos.

Se trata de materias respaldadas por la regulación europea y que encuentran reflejo hoy en leyes españolas. Se abordan los aspectos destacados de la nueva regulación comunitaria a través del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Reglamento general de protección de datos que regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la Unión Europea, y que provocó la derogación de la Directiva 95/46/CE así como de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, apoyándose en las posturas jurisprudenciales en ambos ámbitos de regulación y protección.

Palabras clave: derecho a la intimidad; administración electrónica; protección europea de datos personales.

Fecha de entrada: 16-12-2018 / Fecha de aceptación: 17-01-2019

Cómo citar: Candela Talavero, J. E. (2019). El derecho a la intimidad, la administración electrónica y la transparencia. La nueva protección europea de datos de las personas físicas. *Revista CEFLegal*, *220*, 109-136.

The right to privacy, electronic administration and transparency. The new European protection of data from physical persons

José Enrique Candela Talavero

Abstract

There is a balance of necessary respect in our legal system consisting of the right to privacy, within which is the treatment and data protection and good administration, transparency and concrete the right of access to information, as a guide to the task of the public authorities.

These are subjects supported by European regulation and which is reflected today in Spanish laws. Addressing the highlights of the new Community regulation through Regulation (EU) 2016/679 of the European Parliament and of the Council, general Regulations on data protection regulating the treatment of persons, companies or organizations of personal data relating to persons in the European Union, and which caused the repeal of Directive 95/46/EC as well as the new Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of rights, supported in the jurisprudence positions in both regulation and protection.

Keywords: right to privacy; public electronic administration; European protection of personal data.

Citation: Candela Talavero, J. E. (2019). El derecho a la intimidad, la administración electrónica y la transparencia. La nueva protección europea de datos de las personas físicas. *Revista CEFLegal*, *220*, 109-136.

Sumario

1. Introducción
2. Regulación normativa
3. La protección de datos y la jurisprudencia
4. Principios generales
5. Derechos y requisitos en el ejercicio de la protección de datos
6. Las medidas de seguridad
7. Conclusiones

Referencias bibliográficas

1. Introducción

Desde las instancias de la Unión Europea para la protección de las personas físicas en la dimensión del tratamiento de sus datos personales y para garantizar su libre circulación, a partir del 25 de mayo del 2018 entró en vigor un nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Reglamento general de protección de datos (RGPD) que regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la Unión Europea, y que provocó la derogación de la Directiva 95/46/CE. No obstante advertir de que:

> Rasgo muy destacado es el cambio de instrumento normativo, pues frente al marco legislativo previo de mera armonización se ha optado por la unificación mediante un Reglamento llamado a sustituir a las legislaciones nacionales, salvo en aspectos en los que el RGPD prevé que sus normas pueden ser especificadas o restringidas por los Estados miembros, como contempla su artículo 8 sobre la edad aplicable al consentimiento de los niños. En todo caso, la aplicación de determinados aspectos del RGPD, como en materia de supervisión, requerirá la adaptación de las legislaciones nacionales (De Miguel Asensio 2017, p. 77)[1].

Conviene así enmarcar el análisis de los derechos que entran en juego, como es la intimidad, en su forma de protección de los datos personales, con la transparencia y acceso a la información que engloban el principio de buena administración, en la doctrina de nuestro Tribunal Constitucional (STC 292/2000, de 30 de noviembre, FD 7.º), por el capital equilibrio que se exige entre el derecho al honor y a la protección de datos reconocido en el artículo 18 de la Constitución (CE), al reconocer que:

> 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

[1] «El TJUE puso de relieve que la armonización llevada a cabo por la Directiva 95/46/CE era completa o de máximos, pero destacó que la flexibilidad de sus normas dejaba en muchos casos en manos de los Estados la regulación de los detalles y la posibilidad de elegir entre varias opciones, SSTJUE de 6 de noviembre de 2003, Lindqvist, C-101/01, ECLI:EU:C:2003:596, apartados 83 y 95-96; y 7 de noviembre de 2013, C-473/12, IPI, ECLI:EU:C:2013:715, apartado 31».

> 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.

A lo que uniremos el reconocimiento de derechos fundamentales en nuestra carta magna de estos derechos, con incidencia inmediata en la privacidad de los ciudadanos y la libertad de información con los principios que vertebran, o deberían,la actuación de los poderes públicos. De manera que si en el artículo 53.1 de la CE se estipula que:

> Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Solo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161.1 a).

y en el artículo18.4 de la CE el derecho fundamental a la protección de datos personales, resultará que «le es aplicable la necesidad de una ley para limitar el mismo».

A este respecto hay además que señalar que el Tribunal Constitucional ha interpretado los requisitos y circunstancias de la cesión de datos entre Administraciones públicas, bajo la vigencia de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD),en diversas sentencias, entre las que cabe destacar ahora la STC 17/2013, de 31 de enero (FJ 4.º), y la STC 292/2000, de 30 de noviembre (Informe del Gabinete Jurídico de Agencia Española de la Protección de Datos (AEPD), ampliación del informe emitido en los expedientes 108/2018 (ref. 181577/2018) y 155/2018 (ref. 200012/2018).

2. Regulación normativa

Desde el prisma nacional actualmente en España debemos citar la regulación que ofrecía la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personaly su desarrollo mediante el Real Decreto 1720/2007, de 21 de diciembre, así como que

desde el 7 de diciembre de 2018 se encuentra en vigor la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Negro y Esteban, 23 de noviembre de 2018), cuyo régimen derogatorio previsto en su disposición derogatoria única derogación normativa señala que:

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
2. Queda derogado 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.
3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Ley 3/2018, en la que:

> Se especifican las condiciones de diseño de algunos aspectos nucleares del RGPD. Hay que prestar mucha atención a la llamada transparencia por capas, a la modulación del consentimiento y a la operatividad de las excepciones de ciertas bases de legitimación legal para el tratamiento, como por ejemplo las relativas a la administración electrónica, los datos personales de empresarios individuales y personas de contacto o la investigación biomédica (Martínez, 2018), [sin que estemos ante una norma que sustituya al RGPD, sino que] adapta nuestro ordenamiento jurídico al RGPD, complementando y clarificando algunas cuestiones de gran relevancia. La nueva LOPD valida y da cierto confort a la hora de realizar determinados tratamientos de datos (Monclús Cuatrecasas, 5 de diciembre de 2018).

Entre cuyas directrices, saber que los poderes públicos deberán, según la nueva norma, promover políticas de impulso de los derechos digitales (art. 97) en forma de:

> Previsión de que el Gobierno de la Nación, en colaboración con las comunidades autónomas, deberá elaborar dos documentos:
>
> - Un "Plan de Acceso a Internet" orientado a superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos, y
> - Un "Plan de Actuación" dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la

> finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales (Fernández, 6 de diciembre de 2018).

Existen además diversidad de regulaciones que se deben tomar en consideración al abordar el asunto de la protección de datos personales, fundamentalmente por cuanto es una materia donde la privacidad del individuo se encuentra en el centro de la toma de decisiones administrativas. En este sentido citar la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno (Guichot Reina, 2017a), de la que resulta capital saber que:

> El derecho de acceso a la información pública debe ser considerado como un derecho fundamental. El derecho de acceso no solo es imprescindible para la construcción de una sociedad democrática y participativa (en este sentido son esenciales las sentencias dictadas por el Tribunal de Justicia en el asunto Access Info Europe, a las que luego me referiré), sino que es imprescindible para el libre desarrollo de la personalidad frente a los poderes públicos.
>
> El ser humano tiene derecho a conocer la actuación de los poderes, incluidas las motivaciones de las decisiones adoptadas, y el uso que se hace de los fondos públicos.

Si bien añadiendo que el llamado Grupo de Trabajo de Autoridades de Protección de Datos, Grupo del Artículo 29,35, y el Tribunal de Justicia de la Unión Europea se han ocupado en reiteradas ocasiones del tema. Grupo de Trabajo del Artículo 29, que en su dictamen 3/99, relativo a información del sector público y protección de datos personales (WP 20), aprobado el 3 de mayo de 2003 señala que:

> El legislador, cuando desea que un dato se vuelva accesible al público, no considera, sin embargo, que haya de convertirse en *res nullius*. Tal es la filosofía del conjunto de nuestras legislaciones.
>
> Que el carácter público de un dato de carácter personal resulte de una normativa o de la voluntad de la propia persona a la que alude el dato, no priva ipso facto y para siempre, a dicha persona, de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana (Piñar Mañas, 2014, pp. 7, 8 y 14).

Actuación administrativa transparente (Ghichot Reina, 2014a y 2017b) que hace real el principio de la buena administración, así como «una Administración donde imperen los principios éticos que contribuirá decisivamente a la moralización de la vida social, en no menor medida en que la moralización de la vida social redundará en beneficio de la ética en la Administración» (García Mexía, 1996, p. 332).

Tener presente igualmente la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documen-

tación clínica (Sangüesa Cabezudo, 1 de diciembre de 2012); el Real Decreto 1690/1986, de 11 de julio, por el que se aprueba el Reglamento de Población y Demarcación Territorial de las Entidades Locales (en materia de empadronamiento) (Beato Espejo, 2014, p. 1.212): la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, sobre el censo electoral; la Ley General Tributaria 58/2003, de 17 de diciembre (art. 112); la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico; la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados (art. 24.3, párrafo 2.º); la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (art. 28.2); la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local (arts. 4.1.a, 22.1.d y 123.d) o el Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales (art. 50).

De estas, citar tres. Por un lado, saber que en la Ley 39/2015 destacan previsiones como los artículos 9 a 12, 13, 14, 16, su disposición final segunda sobre la modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica, al incluir un nuevo apartado 11 en el artículo 3 con la siguiente redacción: «11. Todos los sistemas de identificación y firma electrónica previstos en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley de Régimen Jurídico del Sector Público tendrán plenos efectos jurídicos», y por lo que hace a velar por la protección de datos y la dinámica del procedimiento administrativo (Campos Acuña, 2016) en el artículo 41 de la Ley 39/2015, que como regla general reconozca para la práctica de las notificaciones, que «las notificaciones se practicarán preferentemente por medios electrónicos y, en todo caso, cuando el interesado resulte obligado a recibirlas por esta vía. No obstante lo anterior, las Administraciones podrán practicar las notificaciones por medios no electrónicos en los siguientes supuestos […]».

Por otro, que la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dedica su capítulo V del título preliminar (arts. 38 a 46) al funcionamiento electrónico del sector público, y finalmente mencionar la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, que prevé la Administración electrónica en su aplicación y desarrollo así como la protección de datos de licitadores y contratistas (arts. 52, 54, en el recurso especial, el art. 63 sobre el perfil del contratante o el art. 133.1 para asegurar la confidencialidad) (Razquin Lizarraga, 2018), de manera que disponga que:

> Los órganos de contratación no podrán divulgar la información facilitada por los empresarios que estos hayan designado como confidencial en el momento de presentar su oferta. El carácter de confidencial afecta, entre otros, a los secretos técnicos o comerciales, a los aspectos confidenciales de las ofertas y a cualesquiera otras informaciones cuyo contenido pueda ser utilizado para falsear la competencia, ya sea en ese procedimiento de licitación o en otros posteriores. El deber de confidencialidad del órgano de contratación, así como de sus servicios

> dependientes no podrá extenderse a todo el contenido de la oferta del adjudicatario ni a todo el contenido de los informes y documentación que, en su caso, genere directa o indirectamente el órgano de contratación en el curso del procedimiento de licitación. Únicamente podrá extenderse a documentos que tengan una difusión restringida, y en ningún caso a documentos que sean públicamente accesibles. El deber de confidencialidad tampoco podrá impedir la divulgación pública de partes no confidenciales de los contratos celebrados, tales como, en su caso, la liquidación, los plazos finales de ejecución de la obra, las empresas con las que se ha contratadoy subcontratado, y, en todo caso, las partes esenciales de la oferta y las modificaciones posteriores del contrato, respetando en todo caso lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

De esta suerte, vistala normativa nacional, saber de la regulación internacional sobre la protección de datos, por lo que:

> Se ha formado, de este modo, una suerte de ius commune de la protección de datos, tanto en general, como en concreto respecto a los datos personales en poder de la Administración, en el que observamos un triple escalón, una «normación en cascada»: un Derecho de mínimos del Consejo de Europa (integrado en este caso por el Convenio de 1981 y por la jurisprudencia en torno al art. 8 del Convenio Europeo de Derechos Humanos); un Derecho comunitario más detallado (Directiva 95/46/CE); y un Derecho pormenorizado (Reglamento 45/2001/CE, respecto a las Instituciones; las respectivas Leyes nacionales, en relación con los Estados) (Ghichot Reina, 2005, p.84).

Además, que el

> Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, más conocido como la Convención Europea de Derechos Humanos, se inspira expresamente en la Declaración Universal de los Derechos Humanos, adoptada por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948 en París; donde se recogen en sus treinta artículos los derechos humanos considerados básicos, a partir de la Carta de San Francisco, de 26 de junio de 1945.
>
> Asimismo, es de innegable interés citar el Convenio 205 del Consejo de Europa sobre el acceso a los documentos públicos, de fecha 18 de junio del 2009, debido a que su artículo 3.1 otorga la prerrogativa a los Estados para que puedan limitar el derecho de acceso a los documentos públicos, con la salvedad que los límites deberán estar previstos por una ley, ser necesarios en una sociedad democrática y tener como objetivo la protección, entre otros, de «(…) f. La intimidad y otros intereses privados legítimos» (Garrós Font, 2018).

En definitiva, se trata de una materia, la de la protección de datos, de amplio reconocimiento internacional y:

> Firmemente reconocida en el derecho de la Unión Europea. Cabe recordar que, el 28 de enero de 1981, en el seno del Consejo de Europa, se firmó el Convenio 108, para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal. En este, se fijaron los principales elementos del actual régimen jurídico del tratamiento de datos.
>
> A partir de entonces, los Estados europeos comenzaron a reconocer jurisprudencialmente este derecho –como lo haría el Tribunal Constitucional de Alemania, en 1984– y a aprobar sus leyes de protección de datos personales. El Tribunal Europeo de Derechos Humanos (TEDH) en caso Leander, de 26 de marzo de 1987, incluyó este derecho fundamental en el ámbito protegido por el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH). Este garantiza el derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. A partir de entonces, otras sentencias TEDH han ido perfilando este derecho, [resultando clave saber que] la protección de datos protege toda información sobre una persona física identificada o identificable, pero no la relativa a una empresa o persona jurídica (Cotino Hueso, 2018, pp. 314 y 319).

Particularmente sobre la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica a la luz del derecho de acceso, en relación con la historia clínica, de su artículo 18, se dictó Resolución n.º 01727/2018, por la AEPD que en su FD 5.º resolviera que:

> La solicitud de acceso que se formule obliga al responsable del tratamiento a dar una respuesta expresa, incluso en aquellos supuestos en los que no reuniera los requisitos previstos, en cuyo caso el destinatario de esta viene igualmente obligado a requerir la subsanación de las deficiencias observadas o, en caso contrario, motivar la negativa a atender la misma.

Sin perder de vista la STC 139/2016, de 21 julio 2016, para la que:

> c) En la cesión concurre una finalidad legítima que consiste en la obtención de la información y los datos necesarios para hacer posible la materialización efectiva del modelo universal de salud pública que prevé la contribución progresiva de los ciudadanos asegurados o de sus beneficiarios del Sistema Nacional de Salud […]. En consecuencia, la comunicación de datos limitada a la mera indicación del tramo de entre los tres previstos en que se halla el usuario se encuentra amparada por el artículo. 11.2 a) LOPD, en conexión con el artículo 94 ter de la Ley 29/2006 (art. 103 del Real Decreto Legislativo 1/2015) (igualmente la STC 17/2013, de 31 de enero de 2013, FJ 7.º y 8.º).

Intimidad como derecho junto a la realidad electrónica en la actuación de la Administración, para conocer que su implantación:

> Supone, como sabemos, no ya la posibilidad, sino el derecho de todos a relacionarse con la Administración a través de medios informáticos o telemáticos. Pero también implica que las Administraciones públicas van a poder obtener y manejar (someter a tratamiento, en suma) un volumen de información como nunca antes había sido posible.

Por ello, insisto una vez más, el respeto al derecho a la protección de datos de carácter personal adquiere una trascendencia incuestionable. Ya desde la exposición de motivos de la Ley 11/2007 se llama la atención sobre ello (Piñar Mañas, 2011, pp. 161-162). Sin perder de vista que:

> La revolución tecnológica no puede dejar de condicionar los modos en que se ejerce el poder, del mismo modo que ha venido a transformar el funcionamiento de los sectores productivos. El surgimiento de las Intranets administrativas; el reconocimiento de la firma digital; las múltiples utilidades de la llamada Administración electrónica, interactiva o no (Mexía García, 2003, p. 112).

Aunque en sede de protección de datos no debemos olvidar la STJUE de 19 de octubre de 2016, C-582/14, Breyer, apartados 53 y 60 –dictada en interpretación del concepto de interés legítimo del art. 7.1 f) de la Directiva 95/46, y por tanto anterior al RGPD–, que admitió «que una autoridad pública puede tener un interés legítimo como base jurídica en sus tratamientos de datos».

Libertad de expresión en las redes sociales y protección de datos personales que nos sitúa en el equilibrio señalado:

> En la medida en que muchas de las situaciones conflictivas que vamos a estudiar tienen que ver con peligros derivados de esa capacidad de maximización de la expresión, así como de su difusión, que tienen las redes sociales, es esencial contemplar siempre que estos no son sino el inevitable envés de la gran capacidad para fomentar ese mismo pluralismo que esas herramientas poseen. De manera que no puede desatenderse nunca que la cercenación o imposición de excesivos controles y restricciones afecta indefectiblemente a ambas caras de la moneda.
>
> El recuerdo de la importancia del pluralismo como elemento democrático esencial y la convicción de que las posibilidades que las comunicaciones electrónicas, Internet y las redes sociales aportan a la consecución del mismo son cuando menos tan grandes como sus supuestos riesgos nos van a llevar por sistema a ser prudentes a la hora de analizar el papel que han de desarrollar los poderes públicos en esta materia, especialmente en una vertiente activa y limitadora. Esta tesis, por

> lo demás, es perfectamente coherente con los criterios interpretativos más clásicos en materia de derechos fundamentales y libertades públicas, que como es sabido preconizan una visión de los mismos favorecedora de su extensión y obligan a restringir posibles límites a los mismos cuando estos no tengan una base constitucional suficiente (Boix Palop, 2016, pp. 61-62).

Teniendo siempre presente el servicio como norte de la actuación de la Administración pública y su implicación por una ética pública (Mexía García, 2001, p. 135), que ya reconociera nuestro Tribunal Constitucional en su STC n.º 292/2000, de 30 de noviembre, FD 7.º, 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.

3. La protección de datos y la jurisprudencia

El nuevo Reglamento comunitario presenta notas particulares que debemos tener presente desde la relación del ciudadano con la Administración. Así, para una primera aproximación saber que se aplicará:

> 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 […] quedando fuera del mismo, eltratamiento de datos personales en cuatro supuestos determinados, a saber:
>
> a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
>
> b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
>
> c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como podrá resultar cuando un sujeto realiza una invitación a conocidos empleando su correo electrónico no estando relacionado con ninguna actividad profesional o comercial, actividades socioculturales o financieras.

En este sentido son fundamentos los distintos pronunciamientos jurisprudenciales sobre la materia (Nogueira Guastavino, 2016), caso de la STS de 3 de octubre de 2014, que en

su FD 4.º estimó que las direcciones IP son datos personales, en el sentido del artículo 3 de la LOPD, ya que contienen información concerniente a personas físicas «identificadas o identificables» y

> d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Datos que, para tener la consideración de ser personales, según manifestara la Audiencia Nacional (Sentencia de 8 de marzo de 2002), no era imprescindible que coincidiese el dato y la persona concreta, siendo bastante que la identificación «pueda efectuarse sin esfuerzos desproporcionados».

Al respecto saber que la STJUE de 13 de mayo de 2014, resolviendo una cuestión prejudicial sobre la actividad de tratamiento, reconoció el tratamiento de datos personales como:

> Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción, [que] al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsqueda.

Resultando así que el derecho a obtener información por tener interés legítimo habrá de ser ejercitado de forma proporcionada, es decir, poniéndolo en relación con la necesidad de la información que se trata de obtener y con los inconvenientes que pueda producir en la actividad del órgano de la Administración (SSTS de 24 de marzo de 2004 y 4 de diciembre de 1990), pues si:

> De un lado, el acceso a la información integra la libertad de expresión e información, reconocida como fundamental en España, que tanto en el ámbito de Naciones Unidas cuanto la STEHD de 8 de noviembre de 2016 –caso Magyar Helsinki Bizottság contra Hungría–, del otro lado la fundamentalidad del acceso a la información pública en España se deriva del reconocimiento del derecho de acceso a los documentos en el artículo 42 de la Carta de los Derechos Fundamentales de la Unión Europea.

Además, desde el prisma del titular del derecho y la protección iusfundamental más intensa en razón del ejercicio por sujetos cualificados:

> Las «normas de la ONU» del 2000 hacen referencia a que el derecho de acceso a la información pública es un derecho de «todo miembro del público», sin mayor concreción.
>
> Sin embargo, en el ámbito de la ONU el derecho de acceso a la información se reconoce en el marco de la libertad de buscar información, reconocida inicialmente a los periodistas. Como consecuencia, la Observación general n.º 34 del CDH de 2011 afirma que el acceso a la información pública es de los medios de comunicación para que faciliten al público los resultados de su actividad. No obstante, se extiende el derecho a otros sujetos que tienen especial vinculación con el control y vigilancia del poder público, como los autores en internet o asociaciones defensoras de derechos humanos, como en el Dictamen CDN del caso Nurbek Toktakunov vs. Kirguistán (Cotino Hueso, 2017, pp. 280 y 296).

4. Principios generales

Fue criterio de la AEPD, en su informe jurídico 0443/2008 (FD 3.º) que:

> En los supuestos en que el tratamiento del dato de la persona de contacto es meramente accidental en relación con la finalidad del tratamiento, referida realmente a las personas jurídicas en las que el sujeto presta sus servicios, no resulta de aplicación lo dispuesto en la Ley Orgánica 15/1999, viniendo el Reglamento a plasmar este principio.
>
> No obstante, es necesario que el tratamiento del dato de la persona de contacto sea accesorio en relación con la finalidad perseguida (Díaz, Meseguer y Romero de Ávila, 14 de julio de 2017).

Dato personal delimitado en el ámbito comunitario por la Sentencia de 6 de noviembre de 2003, Lindqvist, como «toda información sobre una persona física identificada o identificable»; concepto que incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones (Piñar Mañas, 2003, pp. 74 y 76)[2].

[2] La Sra. Lindqvist sostuvo que «un particular que, en el ejercicio de su libertad de expresión, crea diversas páginas web en el marco de una actividad sin ánimo de lucro o en su tiempo de ocio, no realiza una actividad económica y, por tanto, su conducta no está sujeta al Derecho comunitario. Si el Tribunal de Justicia declarara lo contrario, se plantearía la cuestión de la validez de la Directiva 95/46, puesto que al

Para no perder de vista la dimensión social en la aplicación de la nueva norma europea, como debe por otra parte ser directriz en cualquier aplicación normativa, en el nuevo reglamento europeo se estipulan (art. 5) una serie de principios como piedras angulares de su ejecución, y cuyo desconocimiento o ignorancia dará lugar a la oportuna responsabilidad exigible al responsable de su tratamiento (arts. 24 y 82).

Así, en ese tratamiento de los datos se respetará la licitud, lealtad y la transparencia; se respetará la limitación de la finalidad y su uso y utilización para fines adecuados, pertinentes y limitados a lo necesario, es decir, siguiendo el criterio de la minimización de datos; además deberán ser siempre datos exactos y, para ello, se permite adoptarse por las autoridades medidas para suprimir o rectificar datos personales inexactos con respecto a los fines para los que se tratan. Apuntar de manera específica el principio novedoso en nuestro ordenamiento jurídico o no señalado de manera tan expresa, como es la responsabilidad proactiva, para el que se acuña el término *accountability* para exigir «al responsable del tratamiento no solo el cumplimiento de estos principios, sino que además deberá ser capaz de demostrarlo» (Pérez Cambero, 2016).

Finalmente citar como principios capitales la integridad y confidencialidad, que implican que los datos personales sean tratados para resultar garantizados con una seguridad adecuada, y así,básicamente, «la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas», no aplicándose para tratar datos personales de personas jurídicas o fallecidas. Reconoció al hilo de lo expuesto la STS 574/2016 de 14 de marzo de 2016 (FD 9.º) que:

> Aun en los supuestos en los que existe corresponsabilidad en el tratamiento de datos, no es de apreciar solidaridad en el cumplimiento de las obligaciones, de manera que cada responsable lo es de aquellas que se derivan de su actividad, lo que tiene una doble consecuencia: primera, la necesidad de precisar el alcance de la participación en el tratamiento de cada corresponsable, para identificar el alcance de sus obligaciones; y segunda, que la exigencia de su cumplimiento ha de efectuarse por el interesado a quien resulte responsable en cada caso, lo que significa que el procedimiento no puede seguirse indistintamente frente a cualquiera de ellos, sino que necesariamente ha de identificarse el responsable en cada caso, siendo este el legitimado al efecto (STJUE de 13 de mayo de 2014, FD 40.º).

adoptarla el legislador comunitario se habría excedido en las competencias que le confiere el artículo 100 A del Tratado CE (actualmente artículo 95 CE, tras su modificación). En efecto, la aproximación de las legislaciones, que tiene por objeto el establecimiento y el funcionamiento del mercado interior, no puede servir de base legal para adoptar medidas comunitarias que regulen el Derecho de los particulares a la libertad de expresión en Internet» (véase apartado 30 de la sentencia).

Resultará pues, en cualquier caso, «imprescindible reivindicar el derecho a la protección de datos, manifestación de la dignidad de la persona» (en mi opinión, y pese a que se ha planteado ya desde hace años la posibilidad de reconocer el derecho a la privacidad de los grupos, y teniendo en cuenta que privacidad y protección de datos no son del todo coincidentes, la protección de datos ha de reconocerse solo a las personas físicas) (Piñar Mañas, 2017, p. 70).

Principios que se acompañan con las previsiones del artículo 40, configuradores de unos códigos de conducta, siendo destinatarios los Estados miembros, las autoridades de control, el Comité y la Comisión, que deberá también instar la creación de mecanismos de certificación en esta materia de protección de datos y de sellos y marcas de protección de datos para el cumplimiento de las nuevas previsiones en las operaciones de tratamiento de los responsables y los encargados (art. 42), asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento, que deberán promover su elaboración para contribuir a la correcta aplicación del reglamento, según parámetros como las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Delimitándose los parámetros de estos códigos en:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

5. Derechos y requisitos en el ejercicio de la protección de datos

Esta protección al individuo pretendida por la nueva regulación se muestra en la prohibición, como regla y con sus excepciones (art. 9.2), del uso de los datos personales, de su tratamiento, cuando de los mismos se descubra o manifiesten referencias privadas del sujeto, como su origen étnico o racial, sus opiniones políticas, convicciones religiosas o filosóficas, o su afiliación sindical, se trate de datos genéticos, biométricos, relativos a su salud, o datos relativos a la vida u orientación sexual. Así como en el reconocimiento de derechos a este interesado, como la transparencia de la información, comunicación y modalidades de ejercicio de sus derechos, la información que deberá facilitarse (arts. 13 y 14), así como su derecho al acceso,a la rectificación, supresión y oposición (arts. 15, 16, 17 y 21), en particular acceso a los datos, como los fines del tratamiento, las categorías de datos personales, los destinatarios, el plazo previsto de conservación, la existencia del derecho de rectificación o supresión o de presentar reclamaciones.

No perder de vista interpretaciones claves para el tratamiento de estos datos reservados, como es la presencia o no del interés legítimo que busca el responsable del tratamiento de los datos, y es que la STJUE de 24 de noviembre de 2011 recordó:

> Esa satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección.

Será requisito para su uso que el interesado otorgue su consentimiento para ese tratamiento de sus datos con un fin concreto, caso de un contrato en el que aquel fuera parte. Consentimiento expreso que supondrá quedar derogado el contenido del artículo 28 de la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, en lo relativo a la obtención del consentimiento tácito,pues ya el consentimiento no podrá adoptar la forma tácita, como admitió la AEPD (Informe n.º 645/2009).

Además el Tribunal de Justicia de la Unión Europea, en Sentencia de 24 de noviembre de 2011 (asuntos acumulados C-468/10 y C-469/10, caso ASNEF), recordó los:

> Dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado (apartado 38).

De lo que se sigue que el indicado artículo 7 f) de la Directiva 95/46 «se opone a toda normativa nacional que, en el caso de que no exista consentimiento del interesado, imponga exigencias adicionales que se sumen a los dos requisitos acumulativos mencionados en el apartado anterior» (apartado 39).

Así que recordemos el procedimiento sancionador PS/00082/2017, instruido de oficio por la AEDP a la entidad Facebook, Inc., y que dio lugar a la resolución R/01870/2017 (Valdecantos Flores, 27 de septiembre de 2017), en la que:

> Se subraya la necesidad de que el consentimiento prestado lo sea porque se ha facilitado una información expresa, precisa e inequívoca no solo en relación con la existencia del fichero o tratamiento, sino también en relación con la finalidad específica perseguida con la recogida de datos, siendo que en el supuesto analizado, la referencia a la finalidad perseguida, se realiza mediante términos inconcretos de los que no cabe deducir, sin duda o equivocación, la finalidad, frustrando por tanto la posibilidad de que el interesado pueda conocer a qué uso se destinan, y oponerse a los mismos.

Lo que supone que:

> Los elementos esenciales del consentimiento se mantienen en el RGPD, por lo que el cambio principal radica en la forma en la que este se ha de obtener, delimitándose por el Reglamento que este deberá ser recabado mediante una declaración o mediante una clara acción afirmativa.

Consentimiento inequívoco puesto que:

> Tanto la Directiva 95/46/CE como la LOPD hacían alusión al mismo, pero el RGPD, basándose en la definición de la Directiva, aclara que el consentimiento válido requiere una indicación inequívoca por medio de una declaración o una clara acción afirmativa. Un «acto afirmativo claro» significa que el titular de los datos debe haber tomado una medida deliberada para dar su consentimiento al tratamiento en cuestión. El considerando 32 también establece una orientación al respecto, indicando que el consentimiento se puede recabar a través de una declaración oral, escrita o grabada, incluso por medios electrónicos (Valdecantos, 2018).

En fin, que a la luz del artículo 6.1 a) del RGPD se configura una base jurídica como es la licitud del tratamiento de datos personales con base en que el interesado dio su consentimiento para uno o varios fines específicos que:

> Se ciñe al supuesto que el interesado expresa su consentimiento por el que acepta el tratamiento de datos personales que le conciernen, mediante una declaración

> o una clara acción afirmativa y de modo libre, específico, inequívoco e informado. De no darse estos elementos el consentimiento no sería válido, como sería el caso del llamado «consentimiento tácito» al no derivar este de una «declaración» o una «clara acción afirmativa». [Para esta realidad de un consentimiento expresado de forma libre] en el ámbito de la Administración, puesto que el consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno, como prevé al respecto el considerando 42 del RGPD, y para garantizar que realmente el consentimiento se haya otorgado «libremente» como demanda el RGPD, añade su considerando 43 que «el consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular» (Brines Almiñana, 13 de diciembre de 2018).

Tratamiento de datos que se habilita cuando sea necesario para cumplir una obligación legal aplicable al responsable o para proteger intereses vitales del interesado, para una misión realizada en interés público o en el ejercicio de poderes públicos, y finalmente para que sean satisfechos intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, «siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño». Consentimiento que se podrá retirar en cualquier momento, y que aparecerá como factor determinante en cualquier conflicto en la aplicación de la nueva norma y en la protección de los derechos privados presentes en su tratamiento. Para ello que en su artículo 7, el RGPD prevea como condicionantes del mencionado consentimiento que el responsable del tratamiento deba poder demostrar que el interesado consintió el tratamiento de sus datos personales, aunque si ese consentimiento forma parte de una declaración escrita, si hubiera otros asuntos, la solicitud de consentimiento deberá manifestarse de forma que se diferencie claramente de estos demás asuntos.

6. Las medidas de seguridad

El RGPD estipula que las medidas de seguridad serán objeto de materialización práctica según criterios como la técnica, los costes de aplicación, el contexto y fines del tratamiento o los riesgos para las personas físicas, cuando en la regulación prevista en el Real Decreto 1720/2007, de 21 de diciembre, prevé la obligación de aplicar medidas de seguridad según criterios de nivel básico, medio o alto de los datos. En última instancia, y siguiendo la jurisprudencia del TJUE (sentencia de 8 de abril de 2014, asuntos acumulados

C-293/12 y C-594/12, apartado 52), como recordó la STS de 3 de octubre de 2014 (FD 9.º), las excepciones a la protección de los datos personales y las restricciones a dicha protección han de establecerse sin sobrepasar los límites de lo estrictamente necesarios, resultando, en el caso analizado, que la parte recurrente no acreditó la concurrencia de la necesidad de acudir al tratamiento de datos en cuestión, para la satisfacción de su interés legítimo de protección de los derechos de propiedad intelectual, pues si bien afirmó en su recurso que, a fin de poder concretar las conductas ilícitas de los usuarios de las redes P2P que motivan el ejercicio de su derecho a la tutela judicial efectiva, «no tiene más remedio» que tratar las direcciones IP de los usuarios de dichas redes, sin embargo, en criterio de la sala no se justificó de forma suficiente esa necesidad, por inexistencia de medidas protectoras alternativas en el ordenamiento jurídico, bien en el orden civil, en particular en la Ley de Propiedad Intelectual, bien en el orden penal, más respetuosas del derecho a la protección de los datos personales.

De esta manera que en el ámbito del responsable del tratamiento de los datos, llevará él y, en su caso, su representante, un registro de las actividades de tratamiento efectuadas bajo su responsabilidad con el contenido que señala el artículo 30 (nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos; fines del tratamiento; descripción de las categorías de interesados y de los datos personales; de destinatarios a quienes se comunicaron o comunicarán los datos personales o, en su caso, las transferencias de datos personales a un tercer país o una organización internacional), empleando además medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 32) y que deberá asumir la tarea cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, de realizar, antes del tratamiento, «una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales» (art. 35.1).

Fijando además el artículo 25.2 del RGPD 2016/679 que este:

> Aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Por otra parte, son objeto de una regulación específica los transferencias de datos personales a terceros países u organizaciones internacionales, siendo criterio primero la

posibilidad de realizarse este tipo de transferencias de datos personales, cuando el destinatario sea un tercer país u organización internacional, cuando la Comisión quede asegurada de que estos destinatarios garantizan un nivel de protección adecuado, supuesto en que la transferencia no requerirá ninguna autorización específica (art. 45.1), pudiendo en este ámbito la propia Comisión supervisar acontecimientos en estos países terceros y organizaciones internacionales si pudiera resultar afectada la efectiva aplicación de las decisiones adoptadas. Apareciendo como mecanismos que brinda el RGPD para asegura estos compromisos y la protección de datos en la transferencia, medios o garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas, ofrecidas en un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; normas corporativas vinculantes; cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control; un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país donde aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados o finalmente un mecanismo de certificación.

Además de manera concreta se reconoce que:

> Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo (art. 46.5).

El responsable y el encargado del tratamiento designarán un delegado de protección de datos (DPO) (Jiménez Asensio, 20 de marzo de 2018), designado según el artículo 37 del RGPD, siempre que:

> a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
>
> b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
>
> c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10,

para asegurar igualmente este control (Muro i Bas, 1998) y salvaguarda en el tratamiento y transferencia de datos se regulan dos figuras.

En cada Estado miembro se prevé la figura de una autoridadde control independiente, que como autoridad de control, el artículo 51.1 RGPD brinda que sea responsabilidad de esta autoridad, señalado por el Estado respectivo, «supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión», desempeñando las funciones que le delimita el artículo 57: controlar la aplicación del presente reglamento y hacerlo aplicar; promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento; asesorar jurídicamente a las instituciones del país sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento; promover la sensibilización para el cumplimiento de las obligacionesen el tratamiento de datos; facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente reglamento y cooperar a tal fin; tratar las reclamaciones presentadas por un interesado o por un organismo e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control. Siendo así que «el centro de su actividad se encuentra en el asesoramiento y en una labor de información tanto al responsable o al encargado del tratamiento como a las personas dependientes de ellos que tengan asignadas responsabilidades en el tratamiento de datos de carácter personal» (Davara Rodríguez, 2018).

Delegado sobre el que en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales seprevé su nombramiento en todo caso en «centros docentes, centros sanitarios, empresas de seguridad privada o colegios profesionales». Además, se establece que el DPO no podrá ser removido ni sancionado salvo en casos en los que actúe con dolo o negligencia grave.

En todo caso, aclara la norma que el régimen sancionador (que, recordemos, puede alcanzar los 20 millones de euros o el 4 % de la facturación mundial del grupo al que pertenezca la empresa infractora) no será de aplicación al DPO. Además, impulsa el nombramiento de DPO para entidades en las que no fuera obligatorio, al establecer que «será un criterio positivo a tener en cuenta a la hora de graduar una eventual sanción» (Monclús Cuatrecasas, 5 de diciembre de 2018). Y además citar al Comité Europeo de Protección de Datos como organismo de la Unión, que gozará de personalidad jurídica, actuando con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias, para realizar funciones tales como supervisar y garantizar la correcta aplicación del Reglamento 2016/679, asesorar a la Comisión en esta materia de la protección de datos; emitir directrices, recomendaciones y buenas prácticas y examinar su aplicación por sus destinatarios; examinar cualquier cuestión relativa a la aplicación del reglamento o alentar la elaboración

de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos (art. 70).

7. Conclusiones

En definitiva, sin perder el logro social de vivir en un sistema democrático de derecho y la interacción pública y social a través de las redes sociales, que:

> Ha producido un notable impacto en la forma de entender y ejercitar el derecho a la información, contenido en el artículo 20.1 d) de la CE (Cebrián Zazurca, 2016, p. 315) […], aunque el espíritu del Reglamento es homogeneizar al máximo las legislaciones europeas, flexibiliza ciertas cuestiones dejando a cada Estado la fijación de los requisitos, por ejemplo, la determinación de la edad del menor para poder recabar sus datos (aunque nunca por debajo de trece años), el procedimiento del ejercicio de los derechos, etc. (Iturmendi Rubia, 22 de mayo de 2018).

Aparecen hoy como elementos dignos de la mayor protección y son así 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».

Esta nueva normativa europea es de obligado cumplimiento y directamente aplicable «a cumplir con el RGPD por "encima" de lo que diga la LOPD. Teniendo en cuenta que el RGPD es, en varias cuestiones, más exigente que la LOPD» (Davara Rodríguez, 2017, p. 2.107), resultando trascendental su respeto por toda la actuación de la Administración pública en general y de la municipal (Sempere Samaniego y Pacheco Cifuentes, 17 de mayo de 2012) en particular, desde el punto de la posibilidad de aprobar disposiciones generales de creación, modificación o supresión de ficheros de datos de carácter personal de titularidad municipal que suponen una tenencia de información personal por las inmediatas «relaciones con los vecinos del municipio, con los proveedores o con los trabajadores, entre otras», por lo que «debe estar correctamente protegida, ya que en la mayoría de los casos estamos manejando información que dice mucho más de sus titulares de lo que *a priori* nos pudiera parecer» (Arias Pou, 2006, p. 4.365).

Sin olvidar su conexión con la realidad social y jurídica actual que supone que:

> El derecho de acceder a la información pública es una conquista que solo se ha globalizado como consecuencia de la cuasi generalización del sistema de democracia representativa y de la lucha en su seno por una profundización en los mecanismos de control democrático (Guichot Reina, 2016, p. 92).

Así se desprende de la STEHD, Gran Sala, de 8 de noviembre de 2016, caso Magyar, cuando afirmó que:

> El derecho a recibir la información no puede ser interpretado como que impone a un Estado obligaciones positivas de recopilar y difundir información de oficio […] el artículo 10 no confiere a los particulares un derecho de acceso a la información en poder de una autoridad pública, ni obliga al Gobierno a dar dicha información a la persona. Ahora bien «tal derecho u obligación puede surgir […] en circunstancias en que el acceso a la información es fundamental para el ejercicio individual del derecho a la libertad de expresión, en particular, de la libertad de recibir y difundir informaciones [art. 10 CEDH] y su negación constituye una interferencia con este derecho» (Cotino Hueso y Boix Palop, 2018, p. 269). Siendo así 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 (SSTC n.º 39/2016 de 3 de marzo de 2016, FD 3.º y n.º 292/2000, de 30 de noviembre, FD 7.º).

Asimismo, la transparencia en el ámbito de la nueva regulación comunitaria supone que:

> El RGPD contempla el principio de transparencia en una doble dimensión. Por una parte, desde el punto de vista de la acceso a la información, tal y como se señala en el considerando 58, cuando señala que el principio de transparencia exige que toda información dirigida al público, al interesado, sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice, precisando que esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web, caso que, como veremos, resulta coincidente con la modalidad de publicidad activa prevista en nuestro ordenamiento jurídico.
>
> En particular, señala que ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea, y que dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender. Por otra, en la dimensión que adquiere el deber de informar a los afectados en la línea de refuerzo de los derechos de los afectados, que constituye uno de los ejes del RGPD, pues la disponibilidad de la información y su acceso son fundamentales para su

ejercicio, a través del principio de transparencia, y que se concreta en su artículo 13 (Campos Acuña, 14 de mayo de 2018).

No obstante, sin perder de vista, como único parámetro con el que confrontar la protección de los límites a la transparencia y el acceso a la información,

> el valor que para la sociedad tiene el conocimiento de la información, un juicio abstracto desvinculado por completo de la cualidad y motivación del solicitante. Lo que, por lo demás, hace que una vez concedido el acceso, la información pueda circular libremente en la sociedad y ser conocida por cualquiera (de hecho, diversos sistemas prevén la publicación automática de la información una vez entregada a uno o varios solicitantes) (Ghichot Reina, 2014b, p. 101), [desarrollándose en un marco de globalización (Sorensen, 2010) que] ejerce su influencia sobre las relaciones entre Derechos públicos nacionales, mediante mecanismos, como antes reseñamos, de permeabilización, competencia y armonización. En este punto, el Derecho comparado se ve atribuido de una nueva función, ya no de erudición, sino de respuesta a necesidades concretas e inmediatas en un contexto de competencia e influencia mutuas entre sistemas jurídicos, con un papel preeminente en materia económica del análisis económico del Derecho (Guichot Reina, 2012, p. 319).

Referencias bibliográficas

Arias Pou, M. (2006). Las Entidades Locales como garantes de la protección de datos en la prestación de servicios de administración electrónica. *El Consultor de los Ayuntamientos*, La Ley, *24*.

Beato Espejo, M. (2014). El acceso al padrón municipal de habitantes por el propietario de una vivienda ocupada por el usuario. *El Consultor de los Ayuntamientos y de los Juzgados*. La Ley, *11*.

Boix Palop, A. (2016). La construcción de los límites a la libertad de expresión en las redes sociales. *Revista de Estudios Políticos*, *173*.

Brines Almiñana, J. (13 de diciembre de 2018). Bases jurídicas relevantes en el tratamiento de datos personales por los entes locales: apuntes en el marco del RGPD y la LOPDGDD (Ley Orgánica 3/2018, de 5 de diciembre). *El Consultor de los Ayuntamientos*, Wolters Kluwer.

Campos Acuña, C. (Coord.). (2016). El nuevo procedimiento administrativo local tras la ley 39/2015. *El Consultor de los Ayuntamientos y de los Juzgados*, marzo.

Campos Acuña, C. (14 de mayo de 2018). Obligaciones de publicidad y acceso a la información. Interacción normativa del

RGPD con la normativa sobre Transparencia. En *Administraciones Públicas y Protección* de Datos: adaptación al RGPD. La Ley.

Cebrián Zazurca, E. (2016). El impacto de Internet en el Estado Democrático. *Revista de Estudios Políticos*, *173*.

Cotino Hueso, L. (2017). El reconocimiento y contenido internacional del acceso a la información pública como derecho fundamental. *Teoría y Realidad Constitucional*. UNED, *40*.

Cotino Hueso, L. (2018). Confidencialidad y protección de datos en la mediación en la Unión Europea. *Revista del Instituto de Ciencias Jurídicas de Puebla* (Nueva época), (IUS), *12*(41).

Cotino Hueso, L. y Boix Palop, A. (2018). Algunas propuestas de mejora de la normativa del derecho de acceso a la información. En *El buen gobierno y la transparencia, a caballo entre la Ética y el Derecho.* Revista Internacional de Éticas Aplicadas (Dilemata), 27.

Davara Rodríguez, M. A. (2017). Algunas consideraciones sobre el Reglamento europeo de protección de datos. *El Consultor de los Ayuntamientos*, Wolters Kluwer, *17*.

Davara Rodríguez, M. A. (2018). Posición y funciones del delegado de protección de datos. *Actualidad Administrativa*, Wolters Kluwer, *1*.

De Miguel Asensio, P. A. (2017). Competencia y Derecho aplicable en el Reglamento General sobre Protección de datos dela Unión Europea. *Revista Española de Derecho Internacional*, *69*(1).

Díaz, L., Meseguer, A. y Romero de Ávila, F. (14 de julio de 2017). Los datos de contacto de los profesionales en el marco del RGPD y del anteproyecto de la nueva LOPD. *Diario La Ley*, Wolters Kluwer, *9*.

Fernández, C. B. (6 de diciembre de 2018). Los nuevos derechos digitales reconocidos por la Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales. Wolters Kluwer.

García Mexía, P. (1996). Reseña bibliográfica de La Ética en la Administración Pública de J. González Pérez. Madrid: Civitas, p. 143. *Revista Española de Derecho Constitucional*, *16*(48), 332.

Garrós Font, I. (2018). El principio de transparencia y el derecho a la protección de datos personales. (Comentarios a propósito del Reglamento sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos). *Actualidad Administrativa*, Wolters Kluwer, *2*.

Ghichot Reina, E. (2005). Derecho a la protección de datos y actividad administrativa. *Revista Vasca de Administración Pública*, *71*, 84.

Guichot Reina, E. (2012). Globalización jurídica y Derecho Público. Recientes aportaciones en la doctrina europea. *Revista de Administración Pública*, *187*.

Ghichot Reina, E. (2014a). La aplicación de la Ley Andaluza de transparencia en las entidades locales. *Revista Andaluza de Administración Pública*, *90*.

Ghichot Reina, E. (2014b). La nueva Ley de Transparencia, un reto para la gestión de las organizaciones públicas. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, *6*.

Guichot Reina, E. (2016). Reflexiones sobre la aplicación de la nueva normativa sobre transparencia. *Revista Andaluza de Administración Pública*, *94*.

Guichot Reina, E. (2017a). El acceso de los representantes políticos a la información y la nueva normativa sobre transparen-

cia y acceso a la información pública. En especial, la posibilidad de presentar reclamaciones ante las Autoridades de transparencia. *Reala* (Nueva época), *8*, 27-48.

Ghichot Reina, E. (2017b). La competencia de las Autoridades de control para conocer de reclamaciones en materia de información ambiental, de reutilización y archivística. *Revista Española de la Transparencia*, *4*.

Iturmendi Rubia, J. M. (22 de mayo de 2018). Artículo sobre el nuevo reglamento de europeo de protección de datos [Blog]. CES Cardenal Cisneros.

Jiménez Asensio, R. (20 de marzo de 2018). El delegado de protección de datos en las Administraciones Públicas. *Seminario de Actualización de Función Pública*, Federació de Municipis de Catalunya, IDEC-UPF, Barcelona.

Martínez, R. (2018). La protección de datos, un instrumento esencial para la garantía de los derechos fundamentales. *El Consultor de los Ayuntamientos*. Wolters Kluwer, La Ley, *8134*.

Mexía García, P. (2001). La Ética Pública. Perspectivas actuales. *Revista de Estudios Políticos* (Nueva época), *114*.

Mexía García, P. (2003). El Derecho de Internet y sus implicaciones para la Administración. *Documentación Administrativa*, *265-266*.

Monclús Cuatrecasas, J. (5 de diciembre de 2018). Habemus nueva ley de protección de datos ¿y ahora qué? Recuperado de <http://www.expansion.com/juridico/opinion>.

Muro i Bas, X. (1998). La Agencia de Protección de Datos. *Revista de Administración Pública*, *147*.

Negro, A. y Esteban A. (23 de noviembre de 2018). El Senado aprueba la nueva LOPD: A la espera de su publicación en el BOE. Recuperado de <https://blog.cuatrecasas.com/propiedad-intelectual/>.

Nogueira Guastavino, M. (2016). Sentencias sociales del Tribunal Constitucional y TEDH en el primer trimestre de 2016. *Actum Social*, *110*.

Pérez Cambero, R. (2016). Análisis de las últimas e importantes novedades en protección de datos: Reglamento Europeo de Protección de Datos y Escudo de Privacidad UE-EE.UU. *Actualidad Administrativa*, Wolters Kluwer, *11*.

Piñar Mañas, J. L. (2003). El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. *Cuadernos de Derecho Público*, *19-20*.

Piñar Mañas, J. L. (2011). Administración electrónica y protección de datos personales. *Dereito*, Monográfico: Estudios sobre la modernización administrativa.

Piñar Mañas, J. L. (2014). Transparencia y derecho de acceso a la información pública. Algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno. *Revista Catalana de Dret Públic*, *49*.

Piñar Mañas, J. L. (2017). Sociedad, Innovación y Privacidad. En *El cambio digital en la economía. Un proceso disruptivo*. *Revista de Economía*, ICE (Información Comercial Española), *897*.

Razquin Lizarraga, M. M. (2018). El principio de confidencialidad en la contratación pública. En J. M. Gimeno Feliú. (Dir.), *Estudio Sistemático de la Ley de Contratos del Sector Público* (pp. 867 a 912). Cizur Menor (Navarra): Thomson Reuters Aranzadi.

Sangüesa Cabezudo, A. M. (1 de diciembre de 2012). Autonomía del paciente. Consentimiento informado. *Revista de Jurisprudencia.* El Derecho Editores, *1*.

Sempere Samaniego, J. y Pacheco Cifuentes, A. (17 de mayo de 2012). Análisis del instrumento normativo de creación, modificación y supresión de ficheros de datos de carácter personal en la Administración local. *Diario La Ley*, *7860*.

Sorensen, G. (2010). *La Transformación del Estado. Más allá del mito del repliegue*. Valencia: Tirant lo Blanc.

Valdecantos, M. (2018). El consentimiento como base legitimadora del tratamiento en el Reglamento europeo de protección de datos. *Actualidad Civil*, Wolters Kluwer, *5*.

Valdecantos Flores, M. (27 de septiembre de 2017). Sanción de la AEPD a Facebook por infracciones graves y muy graves de la normativa en materia de protección de datos. *Diario La Ley*, Wolters Kluwer, *10*.