UNIFICACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA: DESAFÍOS E IMPLICACIONES

Unification of personal data protection in the European Union: Challenges and implications

Dolores-Fuensanta Martínez-Martínez

Note: This article can be read in its original English version on:
http://www.elprofesionaldelainformacion.com/contenidos/2018/ene/17.pdf

Dolores-Fuensanta Martínez-Martínez es doctora en Derecho por la *Universidad Católica San Antonio*, master en *Dirección y Gestión de Empresas* por la *Know How Business School* y licenciada en Derecho y Económicas por el *CEU San Pablo* y en Criminología por la *UEM*. Profesora de derecho de la empresa en la *Universidad de Murcia*, abogado y fiscal sustituto del *TSJM*. Miembro del equipo de trabajo del proyecto I+D *Comunicación móvil e información personal: Impacto en la industria mediática, el sistema publicitario y las percepciones de los usuarios* (CSO2013-47394-R).
https://orcid.org/0000-0002-8149-828X

Universidad de Murcia, Facultad de Comunicación y Documentación
Campus de Espinardo. 30100 Murcia, Spain
dfmartinez@um.es

Resumen

La Unión Europea afronta la cuarta revolución industrial y el mercado único digital con la unificación del régimen jurídico sobre protección de datos personales pretendida por el *Reglamento (UE) 2016/679 General de protección de datos*. Esta unificación es más teórica que real, toda vez que aspectos formales del reglamento y los materiales del contenido del derecho fundamental a la protección de datos dificultan este proceso. La entrada en vigor del *Reglamento* en mayo de 2018 proporcionará el primer marco legal de referencia para la implementación en las empresas de una verdadera cultura de la privacidad, de la protección de datos personales y el cumplimiento normativo en la UE.

Palabras clave

Economía digital; *Mercado único digital*; Derechos fundamentales; Protección de datos personales; Privacidad; Intimidad; *Reglamento general de protección de datos*; *RGPD*.

Abstract

The European Union faces the fourth industrial revolution and the digital single market with the unification of the legal status for personal data protection sought by the *General Data Protection Regulation (EU) 2016/679*. This legal unification is more theoretical than real, since formal aspects of the regulation and the content materials of the fundamental right to data protection make this process difficult. The entry into force of the *GDPR* in May 2018 provides the first legal reference framework for the implementation in companies of a true culture of privacy, and the protection of personal data and normative compliance in the EU.

Keywords

Digital economy; Digital single market; Fundamental rights; Protection of personal data; Privacy; *General data protection regulation*; *GDPR*.

Martínez-Martínez, Dolores-Fuensanta (2018). "Unification of personal data protection in the European Union: Challenges and implications". *El profesional de la información*, v. 27, n. 1, pp. 185-194.

https://doi.org/10.3145/epi.2018.ene.17

Artículo recibido el 09-09-2017
Aceptación definitiva: 05-12-2017

1. Introducción

A las puertas de la cuarta revolución industrial (*CNMC*, 2016) un número creciente de soluciones tecnológicas innovadoras [impresión 3D, 5G, realidad virtual y aumentada, internet de las cosas, computación en la nube, inteligencia artificial, datos masivos (*big data*), etc.] se sustentan sobre dos pilares esenciales:

- la conectividad e interoperabilidad de las tecnologías (*Comisión Europea*, 2016, 587, p. 3); y
- la digitalización de los datos/información o procesos de datificación de la información (**Santamaría**, 2016).

La era de la información acoge formas de capitalismo digital (**Costas**, 2017) que incluyen fenómenos socio-económicos diversos como:

- la economía colaborativa (*sharing economy*);
- el intercambio gratuito de bienes y servicios (*gift economy*);
- la economía del trueque (*barter economy*);
- la economía bajo demanda (*gig economy*).

todas ellas al amparo común de la "economía digital" o del concepto de "economía de la información" (**Cohen**, 2017).

Ésta se caracteriza por la desmaterialización de los factores de producción tradicionales del mercado al que se une un cuarto factor clave –los datos personales-, trasladando la función tradicional del mercado a las plataformas digitales (**Cohen**, 2017). Los datos y la información representan el principal factor de producción de un mercado digital anclado todavía sobre la teoría económica de los mercados bilaterales basados en la publicidad. El tratamiento de la información y de los datos mediante técnicas de *profiling* (elaboración de perfiles online de los usuarios) a partir de las *cookies* u otras técnicas de recopilación de datos proporciona la segmentación requerida por una publicidad comportamental online, el marketing *one to one*, o la publicidad programática (**Feijóo-González**; **Gómez-Barroso**; **Martínez-Martínez**, 2010; **Navas-Navarro**, 2015, p. 151; **Martínez-Martínez**; **Aguado**; **Boeykens**, 2017).

> Las nuevas soluciones tecnológicas plantean desafíos complejos por la recopilación y uso de la información personal en ámbitos muy distintos y, a la vez, interrelacionados

En este contexto no es arriesgado afirmar con **Gómez-Barroso** y **Feijóo-González** (2013) que los datos personales son la nueva moneda de la economía digital al posibilitar no sólo una publicidad personalizada (publicidad *one to one*) como modelo de negocio de los datos masivos, sino también la ubicuidad de la información con internet móvil (**Martínez-Martínez**; **Aguado**; **Boeykens**, 2017; **Martí-Parreño**; **Cabrera-García-Ochoa**; **Aldás-Manzano**, 2012).

Quizá el caso más paradigmático de la relevancia de los datos personales son las plataformas y servicios de redes sociales. Se ha llegado a afirmar que sus usuarios no son clientes sino productos, toda vez que la esencia del negocio de la red social se encuentra en los datos e información que los usuarios proporcionan y hacen públicos en sus perfiles (**Alonso-García**, 2015, p. 23).

Las nuevas soluciones tecnológicas plantean desafíos complejos relacionados con la recopilación y uso de la información personal en áreas muy distintas y, a la vez, interrelacionadas como la economía, las telecomunicaciones, la sanidad, las políticas sectoriales o el derecho. Desde la perspectiva legal, los datos y la información personal online siempre se han enfrentado al desafío de garantizar a los consumidores-usuarios la misma protección y seguridad jurídica que en un mercado físico. Un comercio electrónico eficaz exige la libre circulación transfronteriza de datos (personales o no) e información, pero además un marco legal de referencia uniforme confiable y garantista de los derechos de empresas y consumidores. Pero el mayor desafío de una sociedad digital es garantizar los derechos y libertades de los ciudadanos/usuarios online frente a las amenazas de un uso o tratamiento malintencionado de nuestro rastro o huella digital (información y datos personales que vamos dejando al interactuar con soportes electrónicos, navegar por internet o acceder a redes sociales), que pudiera derivar en delitos como las modalidades de ciber-acoso*: cyberbullying*, *happy slapping*, *grooming*, o las estafas informáticas como el *phishing* mediante la utilización de *malware* o código malicioso (**Alonso-García**, 2015, p. 35; **Hernández-Guerrero**, 2013).

El primer marco legal europeo de la sociedad de la información fue la *Directiva 2000/31/CE*, del *Parlamento Europeo* y del *Consejo*, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información (*Unión Europea*, 2000). Centrada en el comercio electrónico en el mercado interior (*Directiva sobre el comercio electrónico*) se incorpora a nuestro ordenamiento por *Ley 34/2002*, de 11 de julio, de *servicios de la sociedad de la información y del comercio electrónico* (*Lssic*) (*España*, 2002).

Esta *Ley* solventa las incertidumbres jurídicas generadas por internet y las TICs proporcionando el régimen jurídico de los servicios y la contratación electrónica, regulando:

- obligaciones de los prestadores de servicios incluidos los intermediarios de transmisión de contenidos por redes de telecomunicaciones;
- comunicaciones comerciales electrónicas;
- información previa y posterior a la celebración de contratos electrónicos;
- condiciones relativas a su validez y eficacia;
- régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información (art. 1 *Lssic*).

La norma pese a sus reformas (2003, 2007, 2011, 2012 y 2014) acoge un concepto amplio de servicios de la sociedad de la información (SSI) que comprende prácticamente la totalidad de las actividades actuales, sólo condicionadas por "representar para el prestador una actividad económica" permitiendo así incluir en el concepto futuros servicios o actividades aún hoy no conocidos. Los proveedores de plataformas online desarrollados a partir de la web 2.0 como las redes sociales o plataformas de economía colaborativa (*Blablacar*, *AirBnb*…) se someten a la *Lssic* y se consideran servicios de la sociedad de la información –pese a ser los propios usuarios consumidores los generadores de contenido e información mediante su interactuación en la Red (**Martínez-Martínez**, 2013; **Agustinoy-Guilayn**; **Monclús-Ruiz**, 2016, pp. 25)- porque constituyen una actividad económica,

suministran información a distancia por vía electrónica y se prestan a petición del usuario (**Ortiz-López**, 2013, p. 31).

La comunicación *Una estrategia para el mercado único digital de Europa* (*Comisión Europea*, 2015) marca el inicio de una nueva política legislativa comunitaria de la economía digital. Se abandonan los instrumentos armonizadores en favor de los unificadores como el reglamento comunitario, apostando por el fomento de las TICs como una política europea horizontal que afecta a todos los sectores económicos y al sector público. La estrategia de la UE es ambiciosa, con 22 acciones a corto plazo atendiendo al principio de legislar mejor y tres pilares básicos:

- la accesibilidad de consumidores y empresas a los bienes y servicios online eliminando barreras transfronterizas europeas;
- fomentar las infraestructuras de alta velocidad, contenidos digitales seguros y fiables con regulación adecuada;
- aprovechar el potencial de crecimiento de las TIC, computación en la nube, datos masivos e innovación para impulsar la competitividad.

La estrategia aborda reformas normativas transversales sobre telecomunicaciones, propiedad intelectual, protección de consumidores, contratación electrónica, ciberseguridad, privacidad y protección de datos, administración pública electrónica, competencia, iniciativas sobre la propiedad de los datos y su libre circulación, envíos de paquetería y la comunicación audiovisual, entre otras, que tratan de definir las líneas maestras de un mercado único digital sin barreras que permita a Europa liderar la economía digital mundial (*Comisión Europea*, 2015, p. 2).

> Los datos y la información representan el principal factor de producción del nuevo mercado digital

En este trabajo se aborda la nueva estrategia europea sobre protección de datos personales a partir de su normativa más reciente y con mayor repercusión económico-social. Después de más de 20 años de vigencia de la *Directiva 95/46/CE*, en el *DOUE* de 4 de mayo de 2016 se publicó el *Reglamento 2016/679 del Parlamento Europeo y el Consejo de 27 de abril* (*Unión Europea*, 2016), *relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos* (*Reglamento general de protección de datos – RGPD*) que será aplicable directamente en todos los Estados de la Unión Europea a partir del próximo 25 de mayo de 2018.

El *RGPD* proporciona un marco común más sólido y coherente con el avance tecnológico, la globalización y nivel de desarrollo de la economía digital en la UE aportando además la seguridad jurídica demandada por las personas físicas en el tratamiento de sus datos personales. Se generaliza el principio de control sobre los datos personales por la vía de la unificación normativa utilizada, si bien permite cierto margen de maniobra a los Estados miembros en determinadas materias que requieren una legislación nacional como en los supuestos de nombramiento y competencias de las autoridades nacionales de protección de datos o tratamiento de los datos sensibles. El *Reglamento* supone un hito legislativo en materia de privacidad y protección de datos personales y un cambio de enfoque muy sustancial al pretender instaurar una verdadera cultura de la privacidad y la protección de los datos personales (*Fundación ESYS*, 2016, p. 46) afectando a todos los operadores del mercado. En los siguientes apartados trataremos de esbozar sus principales líneas, empezando por la delimitación conceptual y legal del derecho fundamental a la protección de datos personales.

> La estrategia para el *Mercado Único Digital de Europa* marca el inicio de una nueva política legislativa comunitaria de la economía digital

2. La protección de datos personales como derecho fundamental

El *Convenio* n. 108 del *Consejo de Europa* de 28 de enero de 1981, suscrito actualmente por 47 países, es el primer instrumento internacional jurídicamente vinculante que reconoce la protección de las personas respecto del tratamiento automatizado de sus datos de carácter personal. El tratamiento de los datos personales se integra en el contenido del artículo 8 del *Convenio europeo sobre derechos humanos* (*CEDH*, 1950) garantizando el derecho de toda persona al respeto de su vida privada y familiar, su domicilio y su correspondencia, a excepción de las injerencias permitidas a la autoridad pública por una ley y por razones de seguridad nacional y/o pública, la defensa del orden y prevención del delito, protección de la salud o de la moral, o la protección de los derechos y libertades de los demás.

En el mismo sentido, el artículo 18 de la *Constitución española* en el capítulo segundo sobre los derechos fundamentales y libertades públicas, garantiza la protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen; así como la inviolabilidad del domicilio y el secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas salvo resolución judicial. El último apartado artículo 18.4 de la *Constitución española* establece que

> "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Este apartado sustenta el régimen jurídico y contenido del derecho a la protección de los datos personales desarrollado por leyes orgánicas posteriores como la derogada *LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal* (*Lortad*) y la actualmente vigente *LO 15/1999 de 13 de diciembre de protección de datos de carácter personal* (*LOPD*).

La *Sentencia del Tribunal Constitucional* (*STC*) *292/2000, de 30 de noviembre* define el derecho fundamental a la protección de datos de carácter personal como

> "un derecho o libertad fundamental […] frente a las potenciales agresiones a la dignidad y a la libertad de las personas provenientes de un uso ilegítimo del tratamiento mecanizado de datos lo que la *Constitución* llama la informática".

Se trata, según el *Tribunal Constitucional*, del derecho de control sobre los datos relativos a la propia persona insertos en un programa informático, *el habeas data* (*STC 254/1993*, *de 20 de julio*) también denominado como libertad informática en otras sentencias (*SSTC 143/1994*, *11/1998*, *94/1998*, *202/1999*, y *292/2000*). Afirma el *Tribunal Constitucional* que junto con un contenido negativo –limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos-, este derecho fundamental tiene un contenido positivo: la atribución al afectado de determinadas posibilidades de actuación, de ciertas acciones para exigir a terceros un determinado comportamiento, como la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (*SSTC 11/1998*, FJ 5; *94/1998*, FJ 4).

La vinculación entre ambos derechos fundamentales, el derecho a la intimidad (art. 18.1 *Constitución española*) y el derecho a la protección de datos personales (art. 18.4 *Constitución española*) se justifica por la finalidad común perseguida: ofrecer protección a la vida privada y familiar de las personas, si bien difieren en el objeto y el contenido tal y como advierte el propio *TC* (*STS 292/2000*, FJ 6).

> La estrategia de la UE es ambiciosa, con 22 acciones a corto plazo atendiendo a tres pilares básicos: accesibilidad, infraestructuras y crecimiento de las TIC

El objeto del derecho a la protección de datos es más amplio que el derecho a la intimidad (art. 18.1 *Constitución española*) afectando a la esfera de otros bienes de la personalidad como la dignidad personal, el honor y el pleno ejercicio de los derechos de la persona, de tal forma que su protección no se reduce sólo a los datos íntimos sino también:

> "a cualquier tipo de dato personal, íntimo o no, cuyo empleo o conocimiento por tercero pueda afectar a sus derechos".

Alcanza por tanto a los datos personales públicos (*Registro Civil*, *Registro Mercantil*, etc.), a los datos que identifiquen o permitan identificar a la persona y sirvan para confeccionar un perfil ideológico, racial, sexual o de cualquier otra índole, o cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo o tengan incidencia en el ejercicio de cualesquiera de los derechos de las personas, sean o no constitucionales.

Por otro lado, el contenido del derecho fundamental a la protección de datos se amplía respecto del derecho a la intimidad al conferir a su titular un haz de facultades como el consentimiento previo para la recogida de los datos; derecho a ser informado del destino y uso de sus datos; el derecho de acceso, rectificar o cancelar los datos; en suma un "poder de disposición y control de sus datos personales", distinto al contenido del derecho al honor, la intimidad personal y familiar y a la propia imagen que se protege civilmente "frente a todo tipo de injerencias o intromisiones ilegítimas" siendo estos derechos irrenunciables, inalienables e imprescriptibles (cfr. art. 1 *LO 1/1982*, de mayo, de *Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen*).

Es oportuno en este momento diferenciar entre intimidad, privacidad y protección de datos personales. Desde un punto de vista técnico-jurídico afecta a ámbitos diferenciados. De conformidad con la doctrina de nuestro *Tribunal Constitucional*, el derecho a la intimidad personal derivado del derecho fundamental a la dignidad personal

> "implica la existencia de un ámbito propio y reservado a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (art. 10.1 *Constitución española*).

La esfera de la intimidad personal se relaciona con la acotación que de la misma realice su titular, pudiendo cada persona reservarse un espacio concreto de la intimidad personal, familiar incluso profesional al conocimiento ajeno, garantizando así el secreto sobre la propia esfera de vida personal y consiguientemente vedando a los terceros, particulares o poderes públicos decidir sobre los contornos de la vida privada (*STC 241/2012*, FJ 3). El alcance de la protección de este derecho se matiza por la existencia de "una expectativa razonable de privacidad o confidencialidad". El *TC* utiliza la privacidad o más bien, "la expectativa de privacidad" como criterio delimitador del ámbito de cobertura del derecho a la intimidad. Así pues, las manifestaciones de la vida privada protegibles frente a intromisiones ilegítimas se supeditan a:

> "las expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observación o del escrutinio ajeno" (*SSTC 170/2013*, *12/2012*, FJ 5).

Por ejemplo, cuando una persona se encuentra en un lugar inaccesible o solitario debido a la hora del día, puede conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores o, por el contrario, no se puede abrigar expectativas razonables de privacidad, cuando se participa de actividades que por las circunstancias que la rodean claramente pueden ser objeto de registro o de información pública (criterio de privacidad que comparte con sentencias del *Tribunal Europeo de Derechos Humanos* de 25 de septiembre de 2001, *P.G.* y *J.H. c. Reino Unido*; y del 28 de enero de 2003, *Peck c. Reino Unido*).

Ninguna de nuestras normas de derecho positivo regula el contenido, área de protección o concepto legal de privacidad pese a ser uno de los términos más utilizados en internet. La exposición de motivos de la derogada *Lortad* de 1992 es el único que:

> "habla de privacidad y no de la intimidad" y expresamente "…la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado…. La privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo".

Así pues, *estricto sensu*, en nuestro ordenamiento se reconoce un derecho fundamental a la intimidad (art. 18.1 *Constitución española*) mientras que el llamado derecho a la privacidad que nace como anglicismo del término inglés *privacy* se relacionaría directamente con el "derecho fundamental a la protección de datos personales" (art. 18.4 *Constitución española*) definido como

> "el derecho fundamental a que las autoridades competentes protejan a todos los ciudadanos frente al posible uso no autorizado de sus datos de carácter personal para obtener un determinado perfil con una finalidad concreta, sin el conocimiento ni consentimiento del titular de los datos" (**Davara-Fernández-de-Marcos**, 2015, p. 30-31).

A nivel Comunitario, el reconocimiento expreso del derecho fundamental a la protección de datos de carácter personal del artículo 8 de la *Carta de los derechos fundamentales* de la Unión Europea del año 2000 es jurídicamente vinculante como derecho primario con la entrada en vigor del *Tratado de Lisboa* de 1 de diciembre de 2009; y en el mismo sentido el artículo 16.1 del *Tratado de funcionamiento de la Unión Europea* (*TFUE*). Los apartados 2 y 3 del artículo 8 de la *Carta* establecen los principios y contenido básicos de este derecho:

> "…2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación.
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente"

que son objeto de desarrollo posterior merced al acervo comunitario.

El derecho fundamental a la protección de datos personales o libertad informática (*habeas data*) ha evolucionado como también lo ha hecho el objeto de su regulación. Inicialmente considerado como un derecho dependiente y subordinado al derecho de la intimidad personal (art. 18 *Constitución española*) pensado para una sociedad no digital, en el siglo XXI es un derecho fundamental autónomo e independiente que conserva sus objetivos iniciales de garantía de otros derechos y libertades (intimidad, propia imagen, honor, libertad de pensamiento, conciencia, libertad de empresa…) pero que afronta el reto de un flujo de datos personales transfronterizos a una escala sin precedentes propiciado por la rápida evolución tecnológica y la globalización (considerando 6 *RGPD*).

El contenido y la lógica interna del derecho fundamental a la protección de datos en la Unión Europea se ha ido configurando por resoluciones jurisprudenciales nacionales y europeas: *STC 292/2000*, 30 de noviembre; *Stjue de 18.12.2008*, caso C-73/07 *Tietosuojavaltuutettu y Satakunnan Markkinapörssi Oy*, *Satamedia Oy; Stjue de 13.05.2014*, caso C-131/12 *Google Spain SL; Google Inc y Agencia Española de Protección de Datos*. También por los trabajos del *Grupo Europeo de Protección de Datos del Artículo 29* de la *Directiva 95/46/CE* (*GT 29* integrado por las *Autoridades Nacionales de Protección de Datos*, *Supervisor Europeo de Protección de Datos* y la *Comisión Europea*) y el desarrollo de otras normas sectoriales (sanidad, criminalidad, protección de menores). Los estándares de calidad alcanzados en este sentido permiten a la UE aspirar a imponerlos a nivel internacional, especialmente en las relaciones entre Europa y Estados Unidos y liderar la regulación del mercado digital global (cfr. art. 3 *RGPD* sobre el territorio de aplicación del *Reglamento*) (**Fernández-Villazón**, 2016).

3. *Reglamento europeo general de protección de datos*

3.1. Nueva estrategia legislativa

El *Reglamento 2016/679* (*Unión Europea*, 2016) negociado durante más de 4 años es uno de los procesos legislativos más importantes en la historia de la Unión Europea. Moderniza y mejora la regulación anterior (*Directiva 95/46/CE*) aumentando la seguridad jurídica que proporciona su "ejecución estricta" como reglamento comunitario o en su consideración de auténtica ley europea. Se concibe como ley marco para homogeneizar la protección de datos personales en toda la UE y dotar de consistencia y coherencia a otras disposiciones integrantes del llamado paquete de protección de datos. Así lo manifiesta el *Supervisor Europeo de Protección de Datos* en su resumen de dictamen publicado en el *DOUE* de 20.7.17 (*C 234/3-5*) sobre la *Propuesta de reglamento relativo a la privacidad y las comunicaciones electrónicas* [*COM* (2017) 10 final Bruselas 10.1.17] (*Reglamento ePrivacy*) que deroga la *Directiva 2002/58/CE* al exigir que ésta se adapte al *RGPD* y se eviten lagunas sobre la protección de datos personales.

> "El nuevo *RGPD* proporciona un marco común más coherente con el avance tecnológico y la globalización, aportando seguridad jurídica al tratamiento de los datos personales"

El *RGPD*, pese a su persistente objetivo de garantizar una protección uniforme y coherente en el tratamiento de los datos personales en la Unión Europea que fomente la libre circulación de éstos, presenta limitaciones o excepciones.

De una parte, limitaciones naturales o propias del contenido del derecho a la protección de datos personales toda vez que, no es un

> "derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales con arreglo al principio de proporcionalidad" (considerando 4 *RGPD*).

Son excepciones amparadas por una ley y justificadas por el interés público, seguridad o defensa nacional, prevención de delitos o el respeto a los demás derechos fundamentales y libertades públicas, como por ejemplo el derecho a la información.

De otra parte, limitaciones estructurales o formales previstas por el *RGPD*, como la pervivencia de las leyes nacionales de protección de datos, excepciones concretas en materia

de llevanza de registro para micro, pequeñas y medianas empresas, o excepciones en el tratamiento de las categorías especiales de datos personales como los datos sensibles. El *RGPD* contiene habilitaciones e imposiciones a los Estados miembros para regular determinadas materias obstaculizando la unificación pretendida y contribuyendo a perpetuar distintos niveles de protección en la Unión. Sobre los Estados miembros recae la responsabilidad última de armonizar sus legislaciones nacionales partiendo de un régimen uniforme en toda la Unión, aunque preservando en lo que no contradiga ese régimen sus principios y tradición jurídica. Los Estados miembros disponen de una *vacatio legis* de 2 años para atender este mandato, hasta el 25 mayo 2018, fecha de aplicación del *Reglamento* y límite para que los empresarios se adapten al nuevo régimen. El 5 de mayo 2017 el *Consejo Federal de Alemania* aprobó la *Gesetz zur anpassung des datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie* (*EU*) 2016/680 o *Bundesdatenschutzgesetz - BDSG* (*Ley Federal de Protección de Datos*) primera norma nacional adaptada a las disposiciones del *RGPD*, mientras que en España el nuevo anteproyecto de *Ley orgánica de protección de datos*, sometido a informe del *Consejo de Ministros* el 7 de julio de 2017 cuenta con el nada desdeñable número de 78 artículos para su adaptación y desarrollo del *Reglamento Europeo* (el anteproyecto contempla, por ejemplo, el tratamiento de los datos de las personas fallecidas –art. 3 y D. A. séptima, pese a su exclusión por parte del *RGPD*).

> El *Tribunal Constitucional* consagra el derecho de control sobre los datos relativos a la propia persona insertos en un programa informático, el *habeas data* también denominado *libertad informática*

3.1.1. Implicaciones en el mercado digital único

El cambio de estrategia legislativa de directiva a reglamento directamente aplicable a los ciudadanos y operadores económicos comporta retos importantes. El *RGPD* es una norma extensa y compleja con 11 capítulos, 99 artículos y 173 considerandos, que ha obligado a tratar con más detalle y exhaustividad los diferentes aspectos del tratamiento de los datos personales (no meras directrices), muchos de ellos excesivamente técnicos (seudonimización, datos genéticos, biométricos…) y burocráticos que no ayudan a concienciar al ciudadano de los riesgos que comporta para sus derechos la manipulación indebida de sus datos personales y por ende, condicionaría la eficacia última de la norma (**Fernández-Villazón**, 2016).

Por otro lado, la nueva reglamentación implica retos de organización y gestión empresarial para los operadores económicos del mercado digital europeo. Se podría hablar de una revalorización de los datos personales europeos frente a otros Estados con legislaciones más *laxas* toda vez que, la implementación de sistemas de gestión de riesgos y protección de los datos personales acordes con las exigencias del *RGPD* lleva aparejados unos costes que recaen sobre el valor del activo protegido (los datos personales). La alternativa al no cumplimiento del *RGPD* comporta igualmente costes empresariales como consecuencia de las sanciones administrativas previstas. El *RGPD* es aplicable a datos personales de usuarios residentes en la Unión obtenidos por la oferta de bienes o servicios a esos usuarios, independientemente de que el responsable y/o encargado del tratamiento y el tratamiento de los datos personales esté/se realice en un Estado fuera de la Unión.

> El derecho fundamental a la protección de datos personales afronta el reto de un flujo de datos personales transfronterizos a una escala sin precedentes propiciado por la rápida evolución tecnológica y la globalización

Para las personas físicas usuarias de internet, el *RGPD* supone el empoderamiento de su información personal digital y un incremento de su poder de control y disposición (derecho de información, de supresión, portabilidad), esto es, mayores garantías de privacidad en el tratamiento de sus datos personales en toda la Unión lo que debería a su vez, fomentar el comercio electrónico transfronterizo y la dinamización del mercado único digital.

3.2. Novedades más relevantes del *RGPD*

El *Reglamento* y la *Directiva 95/46/CE* que deroga comparten el mismo principio:

> "las personas físicas deben tener el control de sus datos personales"

aunque el marco jurídico homogéneo que pretende crear el *Reglamento* supone un cambio sustancial de enfoque hacia una verdadera cultura de la prevención y protección de los datos personales en la Unión. Abordamos la enumeración de las principales novedades del articulado siguiendo el *Informe ESYS* (*Fundación ESYS*, 2016), clasificándolas en atención al área que consideramos más afectada:

3.2.1. Novedades que afectan a la gobernanza empresarial y cumplimiento normativo (*compliance*)

El *RGPD* trata de simplificar la burocracia que la implementación de sistemas de protección de datos implica para las empresas y responsables de tratamiento de datos personales. Desaparece la notificación previa a la autoridad de control exigida por la *Directiva* para poder realizar un tratamiento de datos personales, pero incorpora en su articulado obligaciones y principios directamente relacionados con la gobernanza empresarial, los modelos de gestión de riesgos y el cumplimiento normativo, ya exigidos en otras áreas jurídicas como la prevención de riesgos laborales o el *compliance* penal.

A este respecto, se introducen nuevos principios de protección de datos personales (art. 5) como:

- transparencia en la forma de tratar los datos, la responsabilidad proactiva en el cumplimiento de los principios y su acreditación (*accountability*);
- protección de datos desde el diseño (*privacy by design*)

o responsabilidad proactiva como modelo global y predeterminado de cumplimiento normativo de protección de la privacidad incrustada en el diseño de los sistemas informáticos (**Agustinoy-Guilayn**; **Monclús-Ruiz**, 2016; **Megías-Terol**, 2013);
- protección de datos por defecto, es decir, la obligación de que por defecto sólo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos (*privacy by default*), y la obligación de una evaluación de impacto previa (*privacy impact assessment* - PIA) en los tratamientos que entrañen un alto riesgo para los derechos y libertades de las personas físicas;
- obligación de designar un *Delegado de protección de datos* (*data protection officer*, DPO) contenida en los artículos 37 a 39 *RGPD* para las empresas que realicen tratamiento de datos personales a gran escala en su actividad principal. El DPO asesora e informa al responsable y/o encargado de tratamientos y a los empleados desempeñando un papel crucial en la garantía del cumplimiento normativo;
- obligación de llevar un registro interno por escrito o en formato electrónico de las actividades de tratamiento efectuadas (art. 30) que no se aplica para empresas con menos de 250 trabajadores.

El *RGPD* también promociona, como ya hacía la *Directiva*, la adhesión a códigos de conducta y el sometimiento a mecanismos de certificación como el *Sello europeo de protección de datos* (arts. 40 a 43).

3.2.2. Fortalecimiento y nuevos derechos de los ciudadanos

El artículo 7 *RGPD* desarrolla las nuevas condiciones de validez del consentimiento de los interesados para el tratamiento de sus datos personales que ya no sólo ha de ser inequívoco, libre y revocable, sino una declaración o clara acción afirmativa exigiendo al responsable del tratamiento que sea

> "capaz de demostrar que aquél (el interesado) consintió en el tratamiento de sus datos personales".

Se sigue admitiendo el consentimiento tácito salvo que afecte a categorías especiales de datos y siempre que el responsable pueda demostrar que cumple los requisitos legales. El art. 8 regula el consentimiento de los menores estableciendo una especie de "mayoría de edad informática" al reconocer como válido el consentimiento dado por los mayores de 16 años (los Estados miembros pueden reducirla hasta 13 años). Por debajo de esa edad se necesita la autorización del titular de la patria potestad.

Se refuerza y amplía el contenido del derecho de información al interesado (art. 12) exigiendo a las cláusulas de privacidad una "forma concisa, transparente, inteligible y de fácil acceso". Incluso se prevé la utilización de iconos normalizados que faciliten la comprensión de la información contenida en muchas de las políticas de privacidad, demasiado técnicas para un ciudadano medio. También se fortalece el derecho a no ser sometido a decisiones automatizadas, incluida la elaboración de perfiles (art. 22). No se prohíben estas prácticas, sino que se trata de garantizar el derecho del afectado a tener intervención humana, a expresar su punto de vista y a impugnar la decisión; posibilidades imprescindibles ante las consecuencias que se puedan derivar de técnicas como de datos masivos (*big data*) y la elaboración de predicciones sobre el rendimiento laboral, situación económica, comportamiento individual, etc. (**De-Roselló-Moreno**, 2016; **Recio-Gayo**, 2017).

A los tradicionales derechos ARCO (derecho de acceso, rectificación, cancelación y oposición) se añaden nuevos derechos como:
- derecho al olvido o derecho a exigir la supresión de los datos personales que le conciernan (art. 17);
- derecho a la limitación del tratamiento (art. 18): supuestos en los que los datos no se suprimen, pero dejan de ser tratados y se conservan únicamente a efectos procesales o de prueba;
- derecho a la portabilidad de los datos (art. 20), que reconoce el derecho a recibir los datos personales que nos incumban en un formato estructurado de uso común y lectura mecánica y transmitirlos a otro responsable de tratamiento sin que pueda oponerse el primero. Se permite la portabilidad directa entre responsables cuando técnicamente sea posible (situación frecuente entre los operadores de telefonía móvil).

> "El *RGPD* supone un cambio sustancial de enfoque hacia una verdadera cultura de la prevención y protección de los datos personales en la UE"

3.2.3. Novedades que afectan al control y supervisión del cumplimiento normativo

Se crea el *Comité Europeo de Protección de Datos* como organismo encargado de velar por el cumplimiento de la norma y asesorar a la *Comisión Europea* sustituyendo al actual *GT-29*. Se establece el sistema de ventanilla única (*one-stop shop*) de tal forma que las empresas con tratamiento de datos personales en diferentes Estados miembros tengan una única *Autoridad Nacional de Control* como interlocutora (arts. 56 a 76). Las *Autoridades de Control* tienen la obligación de cooperar entre sí y prestarse asistencia mutua. Se arbitra además el mecanismo de coherencia para la solución de conflictos entre *Autoridades Nacionales de Control* o para unificar criterios de interpretación y aplicación del *RGPD*. Al *Comité Europeo de Protección de Datos* competente le corresponde arbitrar el mecanismo de coherencia y sus decisiones tienen carácter vinculante.

El *Reglamento* prevé sanciones administrativas con multas de hasta 20 millones de euros o el 4% del volumen de negocio anual de la empresa infractora (art. 83 y 84). Las multas administrativas se conciben como un sistema disuasorio, proporcional y efectivo que atenderá a las circunstancias individuales del caso concreto y donde la colaboración con la *Autoridad de Control*, la adhesión a *Códigos de conducta*, la intencionalidad o la naturaleza de la infracción operan como atenuantes de la responsabilidad por incumplimiento normativo. Se regula también la obligación de comunicar brechas o violaciones de la seguridad de los datos a las *Autoridades Nacionales de Control* en el plazo de 72 horas y sin dilación indebida (arts. 33 y 34). En su caso, también se in-

formará directamente a los usuarios cuando las violaciones de seguridad de los datos personales entrañen un alto riesgo para sus derechos y libertades, adoptando las medidas necesarias para no generar alarmas indebidas y tras haber realizado la evaluación correspondiente (**Olejnik**, 2017).

El *RGPD* amplía el concepto de dato personal (art. 4). Se mantiene como "toda información sobre una persona física identificada o identificable" especificando que la persona física identificable es toda aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como un nombre, un número de identificación, datos de localización, un identificador online o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Las categorías "especiales" de datos personales se amplían añadiendo a los tradicionales "datos sensibles" (origen étnico o racial, opinión política, religión, afiliación sindical, salud y vida sexual), los datos genéticos, los biométricos que identifican de una manera unívoca a una persona física, las convicciones filosóficas y las orientaciones sexuales. Introduce nuevos conceptos como los datos personales seudonimizados con un tratamiento específico.

> "El *RGPD* amplía el concepto de dato personal"

4. Conclusiones

El papel de las políticas de la UE en el desarrollo del mercado digital y sus implicaciones sobre el tratamiento de la información personal online resulta decisivo por su vinculación con derechos y libertades fundamentales en torno a la privacidad. El *Reglamento 2016/679 general de protección de datos* (*Unión Europea*, 2016) se presenta como un hito en la historia jurídica de la Unión Europea (más de 20 años desde la *Directiva 95/46/CE* que deroga) si bien, entendemos que comparte alguna consideración similar a otros hitos jurídicos europeos como el *Reglamento (CE) 2157/2001, sobre el Estatuto de la sociedad anónima europea (SE)*.

En primer lugar, por el objeto o materia regulada. Si durante el siglo XX la sociedad anónima europea o "SE" fue considerado el "buque insignia" del derecho societario europeo para la consecución del mercado interior con un proceso legislativo de más de 30 años (**Martínez-Martínez**, 2014, p. 17), tal consideración puede predicarse de la protección de datos personales. En el siglo XXI y ante las expectativas de un mercado único digital, los datos, y en concreto los personales adquieren doble relevancia no sólo como derecho fundamental (art. 8 *Carta europea* y art. 18.3 *Constitución española*) sino también como nuevo factor de producción o "una nueva moneda de cambio" de la economía digital (**Gómez-Barroso**; **Feijóo-González**, 2013).

El nuevo régimen jurídico proteccionista y garantista de la privacidad del *RGPD* empodera y revaloriza el tratamiento de los datos personales de los usuarios europeos frente a las legislaciones más permisivas. No obstante, la información y los datos personales en su consideración como factor de producción y moneda de cambio del mercado digital, exigirían un proceso de "cosificación", de conformidad con nuestra tradición jurídica donde la intimidad personal y familiar, el honor y la propia imagen son derechos inalienables (**Navas-Navarro**, 2015). Igualmente exigirían un reconocimiento como "bien intangible" y derecho patrimonial, de tal manera que atribuyera a su titular derechos exclusivos de explotación mediante la cesión de su uso (que no la venta) a terceros a cambio de una contraprestación económica (precio) o de cualquier otra naturaleza (un tipo de cambio de datos por servicios).

El nuevo *RGPD* afronta el régimen jurídico de una materia exigente de los mayores estándares de seguridad jurídica por ser derecho fundamental. El contenido de este derecho no es absoluto y evoluciona al amparo de resoluciones de distintos órdenes jurisdiccionales y aunque persiga una protección de las personas físicas tecnológicamente neutra. En todo caso se encuentra *al socaire* de la evolución de las propias TICs (*internet of things*, inteligencia artificial, datos masivos, etc.).

Desde el punto de vista formal, la utilización del reglamento europeo como instrumento jurídico de unificación y uniformidad del régimen jurídico de los datos personales en la Unión es más teórico que real: el *RGPD* no puede garantizar el mismo nivel de protección de los datos personales de las personas físicas en todos los Estados miembros por dos razones:

- por las habilitaciones y remisiones expresas del propio *RGPD* a las legislaciones nacionales sobre protección de datos que genera nuevas fuentes normativas;
- porque coexisten con el *RGPD* reglamentaciones sectoriales específicas que excepcionan el régimen general, como las normas para la prevención, investigación, detección o enjuiciamiento de infracciones penales y/o ejecución de sanciones penales, o normas sobre protección frente a las amenazas contra la seguridad pública o terrorismo, entre otras.

El *RGPD* formalmente es un instrumento de unificación directamente aplicable en todos los Estados miembros, pero funcionalmente exige la adaptación y armonización de las legislaciones nacionales como si de una directiva se tratase. Un régimen jurídico uniforme pero fragmentado territorialmente.

Sin duda, la aportación más relevante del RGPD es la modernización del régimen jurídico sobre el derecho fundamental a la protección de datos personales. Define sus principios generales y proporciona una ley marco de referencia en toda la Unión para la implementación de sistemas de gestión inspirados en la cultura de la prevención y cumplimiento normativo de la privacidad y la protección de los datos personales. El *Comité Europeo de Protección de Datos* y las *Agencias Nacionales* serán los encargados, en todo caso, de velar por la eficacia y coherencia del nuevo sistema en el mercado único digital.

5. Referencias

Agencia de los Derechos Fundamentales de la Unión Europea (2014). *Manual de legislación europea en materia de protección de datos*. Bruselas: Agencia de los Derechos Fundamentales de la Unión Europea; Consejo de Europa. *https://rm.coe.int/16806ae663*

Agustinoy-Guilayn, Albert; **Monclús-Ruiz, Jorge** (2016). *Aspectos legales de las redes sociales. Estudio introductorio. Problemática jurisprudencial ordenada y sistematizada.*

Esquemas procesales. Formularios generales. Normativa reguladora. Barcelona: Bosch. ISBN: 978 84 9090 105 2

Alonso-García, Javier (2015). *Derecho penal y redes sociales*. Pamplona: Aranzadi. ISBN: 978 84 90983263

CNMC (2016). *Informe económico sectorial de las telecomunicaciones y el audiovisual 2016*. Comisión Nacional de los Mercados y la Competencia.
https://www.cnmc.es/expedientes/estadcnmc00516

Cohen, Julie E. (2017). "Property and the construction of the information economy: A neo-Polanyian ontology". En: Lievrouw, Leah; Loader, Brian (eds.). *Handbook of digital media and communication*. Routledge, forthcoming. ISBN: 978 1 138672093
https://ssrn.com/abstract=2991271

Comisión Europea (2015). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una estrategia para el mercado único digital de Europa.* Bruselas, 6 mayo.
https://goo.gl/Gf9ZyA

Comisión Europea (2016). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones. La conectividad para un mercado digital único competitivo. Hacia una sociedad europea del Gigabit*. Bruselas, 14 septiembre.
https://goo.gl/64xNgR

Comisión Europea (2017). *Propuesta de Reglamento del Parlamento Europeo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la directiva 2002/58/CE* (*Reglamento sobre la privacidad y las comunicaciones electrónicas*). Bruselas, 10 enero.
https://goo.gl/fs1tQx

Costas, Antón (2017). "Economía digital, ¿vidas precarias?". *La vanguardia*, 5 abril.
https://goo.gl/VDqwYK

Davara-Fernández-de-Marcos, Laura (2015). *Implicaciones socio-jurídicas de las redes sociales*. Pamplona: Aranzadi. ISBN: 978 84 9098 912 8

De-Roselló-Moreno, Rocío (2016). "Nuestros datos personales, fuente de negocio y actividades de *profiling*". *Blog Consejo General Abogacía Española*, 21 septiembre.
https://goo.gl/CvaucG

España (2002). "Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico". *Boletín oficial del Estado*, n. 166, 12 julio.
https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Feijóo-González, Claudio; Gómez-Barroso, José-Luis; **Martínez-Martínez, Inmaculada J.** (2010). "Nuevas vías para la comunicación empresarial: publicidad en el móvil." *El profesional de la información*, v. 19, n. 2, pp. 140-148.
https://doi.org/10.3145/epi.2010.mar.04

Fernández-Villazón, Luis-Antonio (2016). "El nuevo Reglamento europeo de protección de datos". *Foro. Nueva época*, v. 19, n. 1, pp. 395-411.
https://goo.gl/2vk2fq

Fundación ESYS (2016). *El Reglamento general de protección de datos de la UE: una perspectiva empresarial*, octubre.
https://goo.gl/Y96Abt

Gómez-Barroso, José-Luis; **Feijóo-González, Claudio** (2013). "Información personal: la nueva moneda de la economía digital". *El profesional de la información*, v. 22, n. 4, pp. 290-297.
https://doi.org/10.3145/epi.2013.jul.03

Hernández-Guerrero, Francisco (2013). "Las conductas de acoso por medio de las tecnologías de la información y de las comunicaciones". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard. *Derecho y redes sociales* (eds.). Civitas Ediciones, pp. 259-298. ISBN: 978 84 470 3578 4

Martí-Parreño, José; **Cabrera-García-Ochoa, Yolanda**; **Aldás-Manzano, Joaquín,** (2012). "La publicidad actual: retos y oportunidades". *Pensar la publicidad*, v. 6, n. 2, pp. 327-343.
http://dx.doi.org/10.5209/rev_PEPU.2012.v6.n2.41219

Martínez-Martínez, Dolores-Fuensanta (2014). *El proceso de constitución de una sociedad europea-filial en España*. Murcia: Iuris Universal Ediciones. ISBN: 978 84 94187865

Martínez-Martínez, Inmaculada J.; **Aguado, Juan-Miguel**; **Boeykens, Yannick** (2017). "Ethical implications of digital advertising automation: The case of programmatic advertising in Spain". *El profesional de la información*, v. 26, n. 2, pp. 201-210.
https://doi.org/10.3145/epi.2017.mar.06

Martínez-Martínez, Ricard (2013). "Protección de datos personales y redes sociales: un cambio de paradigma". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard (eds.). *Derecho y redes sociales*. Civitas Ediciones, pp. 83-116. ISBN: 978 84 470 3578 4

Megías-Terol, Javier (2013). "Privacy by design, construcción de redes sociales garantes de la privacidad". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard (eds.). *Derecho y redes sociales*. Civitas Ediciones, pp. 319-334. ISBN: 978 84 470 3578 4

Navas-Navarro, Susana (2015*). La personalidad virtual del usuario de internet. Tratamiento de la información personal recogida mediante cookies y tecnología análoga*. Valencia: Tirant lo Blanch. ISBN: 978 84 9086 081 6

Olejnik, Lukasz (2017). "Organizations must inform users about privacy breaches". *Lukasz Olejnik*, 13 Nov.
https://blog.lukaszolejnik.com/organizations-must-inform-users-about-privacy-breaches

Ortiz-López, Paula (2013). "Redes sociales: funcionamiento y tratamiento de información personal". En: Rallo-Lombarte, Artemi; Martínez-Martínez, Ricard (eds.). *Derecho y redes sociales*. Civitas Ediciones, pp. 23-36. ISBN: 978 84 470 3578 4

Recio-Gayo, Miguel (2017). "Nuevo dictamen del GT-29 sobre tratamiento de datos en el trabajo: el interés legítimo". *Diario la ley*, Sección ciberderecho, n. 8, 19 de julio.
https://goo.gl/6kPKBR

Santamaría, Fernando (2016). "Datificación: una alternativa de control de información para grandes empresas". *Reporte digital*, 11 de mayo.
https://goo.gl/ij5zy4

Unión Europea (2000). "Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (directiva sobre el comercio electrónico)". *Diario oficial de las Comunidades Europeas*, 17 julio. *http://www.wipo.int/edocs/lexdocs/laws/es/eu/eu107es.pdf*

Unión Europea (2016). "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos". *Diario oficial de la Unión Europea*, 4 mayo. *https://www.boe.es/doue/2016/119/L00001-00088.pdf*

Unión Europea (2017). "Resumen del Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento relativo a la privacidad y las comunicaciones electrónicas (Reglamento ePrivacy)". *Diario oficial de la Unión Europea*, 20 julio. *https://edps.europa.eu/sites/edp/files/publication/17-07-20_eprivacyreg_ex_summ_es.pdf*

Valera-Ferrío, José (2015). *La brecha digital en España. Estudio sobre la desigualdad postergada*. Madrid: Comisión Ejecutiva Confederal de UGT. *http://www.ugt.es/Publicaciones/BRECHADIGITAL_WEB.pdf*

Vilajoana-Alejandre, Sandra; **Rom-Rodríguez, Josep** (2017). "Sistema de autorregulación publicitaria: del compromiso ético al control efectivo de la publicidad en España". *El profesional de la información*, v. 26, n. 2, pp. 192-200. *https://doi.org/10.3145/epi.2017.mar.05*