EL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS PERSONALES. ANÁLISIS DE SU EFICACIA EN LA DETERMINACIÓN DE SU ÁMBITO TERRITORIAL Y LOS REMEDIOS EN CASO DE TRATAMIENTO ILÍCITO*

THE NEW DATA PROTECTION REGULATION. AN ANALYSIS OF THE TERRITORIAL SCOPE OF ITS CONTENT AND THE MECHANISMS ORIENTATED TO RESOLVE ILLEGAL PROCESSING

Alicia Durán Arroyo**

Resumen: La Directiva 95/46/CE convirtió en pionera a la Unión Europea en la regulación del derecho fundamental a la protección de datos. Sin embargo, sus insuficiencias llevaron a la promulgación del nuevo Reglamento de Protección de Datos (2016/769), aplicable a partir de mayo de 2018. Este trabajo analiza dos puntos de la regulación europea: su ámbito territorial y los mecanismos en caso de tratamiento ilícito de datos, para comprobar si realmente el Reglamento ha sido capaz de colmar las lagunas de la Directiva y garantizar una protección real y efectiva de los titulares de datos.
Palabras clave: derecho a la protección de datos; Directiva 95/46/CE; Reglamento 2016/769 General de Protección de Datos; ámbito territorial de la norma; tutela administrativa y judicial.

Abstract: Thanks to Directive 95/46/EC, the European Union led the way on this fundamental right regulation. However, the legal practice revealed different problems, provoking the promulgation of the new Data Protection Regulation, applicable since May 2018. This paper is focused on two concrete aspects of the European law: the territorial scope of its content and the mechanisms orientated to resolve illegal processing, in order to verify whether the Regulation has solved the Directive's problems and guarantees a real and effective protection of data subjects.
Keywords: data protection right; Directive 95/46/CE; Data Protection Regulation (2016/769); territorial scope; administrative and civil remedies.

* Fecha de recepción: 31 de enero de 2018.
Fecha de aceptación: 26 de febrero de 2018.

** Accésit en la modalidad de Derecho privado, social y económico del VII Premio Jóvenes Investigadores. Graduada en Derecho y Ciencias Políticas y de la Administración Pública (Universidad Autónoma de Madrid) y Máster en Acceso a la Profesión de Abogado (Universidad Autónoma de Madrid). Correo electrónico: a.duranarroyo@gmail.com.

Este artículo parte del Trabajo de Fin de Máster «La protección de datos en el Derecho internacional privado. El Reglamento 2016/769», tutelado por la profesora Dª. Elena Rodríguez Pineau. Este trabajo se ha enriquecido gracias a los comentarios realizados por los miembros del tribunal del VII Premio Joven Investigador: Dª. Alma María Rodríguez Guitián, D. Sebastián López Maza, y Dª. Nuria Bermejo Gutiérrez.

Sumario: I. INTRODUCCIÓN; II. EL SISTEMA DE PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA; III. PUNTOS COMUNES DE LA DIRECTIVA Y EL REGLAMENTO; IV. DERECHO APLICABLE AL TRATAMIENTO DE DATOS; V. REMEDIOS EN CASO DE TRATAMIENTO ILÍCITO; 1. Tutela administrativa; 2. Tutela judicial civil ante la actuación de responsables y encargados; VI. ENCAJE DEL REGLAMENTO DE PROTECCIÓN DE DATOS EN EL MARCO DE LA UNIÓN; 1. Relación con normas dirigidas a la protección de datos; 2. Relación con otras normas del Derecho de la Unión; VII. CONCLUSIONES. VIII. BIBLIOGRAFÍA. IX. JURISPRUDENCIA CITADA.

I. INTRODUCCIÓN

El *derecho a la protección de datos*, pese a estar íntimamente relacionado con el derecho a la privacidad y poder considerarse implícito en textos de referencia como la Declaración Universal de los Derechos Humanos (artículo 12[1]), y aunque no exista un instrumento legal internacional común que aborde específicamente su protección[2], es un derecho autónomo que atribuye al titular un «un poder de disposición sobre sus propios datos personales»[3]; esto es, un poder que abarca desde el derecho del afectado a que se solicite su previo consentimiento para recoger y usar sus datos personales, hasta su derecho a ser informado sobre el destino de estos y a acceder, rectificar y cancelar dichos datos[4].

Tal poder de disposición es otorgado por la normativa que desarrolla la protección de datos, a través de los mecanismos necesarios para garantizar al titular una defensa y protección adecuadas frente a operaciones sobre sus datos, manuales o automatizadas, que por incumplimiento de la normativa no sean respetuosas con este derecho. Sin embargo, la regulación de esas garantías, que son el fin de la protección de datos, resulta compleja y se trata de una cuestión de plena actualidad jurídica, lo cual puede observarse desde diferentes perspectivas.

En primer lugar, desde una perspectiva jurídica, la protección de datos debe enfrentarse a la ya mencionada inexistencia de un instrumento internacional común sobre este derecho,

[1] «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

[2] BYGRAVE, L.A., «Privacy and Data Protection in an International Perspective», *Stockholm Institute for Scandinavian Law*, 2010, p. 181. Disponible en <http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf> [Consultado el 12/07/2017].

[3] PIÑAR MAÑAS, J.L., «Seguridad, transparencia y protección de datos», 2009, p. 5. Disponible en <http://www.cepc.gob.es/docs/ley-de-transparencia/ponencia-j-luis-pi%C3%B1ar.pdf?sfvrsn=0> [Consultado el 15/07/2016].

[4] MINERO ALEJANDRE, G., «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», *Anuario Jurídico y Económico Escurialense,* L (2017), 13-58/ISSN: 1133-3677, p. 20. Disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=5876163> [Consultado el 15/12/2017].

así como a un limitado impacto efectivo de la armonización internacional en la eliminación de diferencias entre ordenamientos[5], lo que dificulta la protección en casos de transferencias de datos entre países. Por otro lado, desde una perspectiva de política económica, no estamos ante un derecho absoluto[6] y el desarrollo económico exige a la regulación conseguir una libre circulación de datos que estimule la economía y que conviva en adecuado equilibrio con una efectiva protección de los titulares. Se trata, además, de un derecho de «cuarta generación»[7], es decir, desarrollado como consecuencia de Internet, cuyas características permiten la difusión, manipulación, copia o destrucción de los datos sin control ni consentimiento del titular[8], así como su rápida difusión, que lleva a su circulación por múltiples jurisdicciones. A ello deben sumarse otros desafíos que la Red y las grandes empresas cuyos principales activos son los datos personales – especialmente las redes sociales – plantean a la hora de garantizar la privacidad de los usuarios, teniendo en cuenta que el uso de la información personal es en la actualidad para ciertas ofertas y prestaciones de Internet un elemento esencial[9]. Son las características del actual funcionamiento de la Red las que son origen de la preocupación que está detrás de la nueva normativa europea de protección de datos[10].

Por último, desde una perspectiva social, vemos, por un lado, como el mundo virtual y especialmente las redes sociales han cambiado la concepción de privacidad de los individuos, que exponen con menores reticencias que en otros contextos aspectos de su vida privada, y, vemos, por otro lado, el aumento de procedimientos, operaciones y transacciones realizados a través de Internet en el ámbito privado y en la relación de los ciudadanos con las administraciones públicas. Estas características de la realidad virtual que vivimos han llevado a la denominación «sociedad de riesgo»[11] y a un aumento de la preocupación tanto de legisladores y juristas en lo referido a la protección, entre otros, del derecho de protección de datos personales, como de los propios usuarios, que empiezan a tomar conciencia de los posibles perjuicios que puede suponer la circulación de datos sin ningún tipo de control ni garantías. En este último sentido, tal y como apunta Minero Alejandre, a partir del Euroba-

---

[5] DE MIGUEL ASENSIO, P.A., *Derecho Privado de Internet*, 5ª edición, Navarra (Thomson Reuters), 2015, p. 300.

[6] Debe ponderarse en relación con su función en la sociedad, tal y como expresa en su párrafo 58 la STJUE 9 de noviembre 2010, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Scheche GbR (C-92/09) y Hartmut Eifert (C-93/09) contra Land Hessen* (ECLI:EU:C:2010:662).

[7] GARCÍA MEXÍA, P., *Derecho Europeo de Internet,* 1ª edición, La Coruña (Netbiblio), 2009, p. 83.

[8] WALTER-ECHOLS, M., «Panopticon – Surveillance and Privacy in the Internet Age», *Worcester Polytechnic Institute*, 2009, p. 7. Disponible en: <https://www.wpi.edu/Pubs/E-project/Available/E-project022709-132355/unrestricted/Panopticon.pdf> [Consultado el 25/06/2016].

[9] DE MIGUEL ASENSIO, P.A., «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», *Revista Española de Derecho Internacional*, vol. 69, núm. 1, enero-junio 2017, Madrid, párr. 2. Disponible en: <http://eprints.ucm.es/41156/> [Consultado el 02/06/2017].

[10] MINERO ALEJANDRE, G., «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», cit., p. 15.

[11] GIL ANTÓN, A.M., «El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales», *Revista de Derecho UNED*, núm. 10, 2012, p. 214.

rómetro 2015, vemos una creciente concienciación sobre el valor de los datos personales y las políticas de privacidad[12].

Ante la imposibilidad de abordar un análisis global, nos centraremos en la legislación de la Unión Europea (UE), por ser el ámbito de mayores progresos en términos de armonización normativa, dirigida a asegurar tanto los derechos de los titulares como la libre circulación de datos en la formación del mercado único. En este contexto, partiremos de un análisis breve de la forma en que la UE ha legislado el contenido del derecho y cómo se ha llegado al nuevo Reglamento. Posteriormente, nos centraremos en el objeto del trabajo: la determinación del ámbito territorial de la normativa europea y los remedios en caso de incumplimiento de la misma, y ello desde la perspectiva de la evolución y el desarrollo en la legislación de tales previsiones.

II. EL SISTEMA DE PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA

En el Derecho de la Unión (DUE), la protección de datos se configura como derecho fundamental (arts. 8.1 de la Carta de Derechos Fundamentales de la UE y 16.1 del Tratado de Funcionamiento de la UE[13]), desarrollado por una legislación considerada como la más influyente del mundo, debido a su modernidad y sus altos estándares de protección[14]. De entre las distintas fuentes normativas[15], la *Directiva 95/46/CE*[16], cuyo objeto es la protección en particular del derecho a la intimidad de las personas físicas (art.1), fue el principal instrumento jurídico aplicable al mercado interior, transpuesto en los Estados miembros (EM) y en el Espacio Económico Europeo (Noruega, Islandia y Liechtenstein).

Sin embargo, pese a su importancia inicial, a largo plazo esta Directiva presentaba ciertos defectos de contenido por no estar adaptada a la realidad social y jurídica que supone Internet, y por las dudas que suscitaban algunos de sus preceptos, como el relativo al ámbito de aplicación territorial; además, el alcance de la uniformización jurídica era limitado,

[12] MINERO ALEJANDRE, G., «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», cit., p. 15.

[13] DE MIGUEL ASENSIO, P.A., «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», cit., párr.1.

[14] SVANTESSON, D., *Extraterritoriality in Data Privacy Law*, 1ª edición, Copenhague (Ex Tuto), 2013, pp. 89 a 90.

[15] Como por ejemplo el Reglamento (CE) Nº45/2001, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales por las Instituciones y organismos de la UE y la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

[16] Esta Directiva nace con la voluntad de solventar las insuficiencias del Convenio 108 del Consejo de Europa, primer instrumento internacional sobre protección de datos jurídicamente vinculante. Ello es así porque el Convenio 108 no permitía asegurar por sí solo el cumplimiento de tutelar la intimidad de los titulares de datos y al mismo tiempo garantizar el funcionamiento del mercado interior y la libre circulación de datos entre los Estados miembros (MINERO ALEJANDRE, G., «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», cit., p. 21).

debido a la necesaria transposición en cada EM, que daba lugar a múltiples normativas con unos rasgos comunes. Hasta el año 2012, momento en que la Comisión Europea decidió abordar una modificación legislativa aplicando el artículo 33 de la Directiva[17], el Tribunal de Justicia de la Unión Europea (TJUE) había ido colmando las lagunas de la misma reveladas por la práctica jurídica. Así, la Comisión pretendía una reforma que fuera capaz de mantener y modernizar los principios originarios de este derecho, estableciendo un marco legal claro y único para toda la UE[18] que partiera de las mismas fuentes jurídicas de la Directiva[19], así como de sus bases y los pronunciamientos del TJUE sobre su contenido.

Ello llevó finalmente a la promulgación del *Reglamento 2016/769 de Protección de Datos* (RPD)[20], aplicable a partir del 25 de mayo de 2018, como sucesor de la Directiva. Mientras que en 1995 se buscaba la armonización y equivalencia en los niveles de protección entre los EM a través de la transposición, con el Reglamento se pretende, a través de la unificación normativa, mejorar la regulación y acabar la elevada fragmentación de instrumentos jurídicos en el territorio de la UE, para así garantizar una mayor seguridad jurídica tanto para los titulares de los derechos como para responsables y encargados del tratamiento. Todo ello mientras se sigue contribuyendo a la libertad de circulación de datos en los EM y al desarrollo del mercado interior[21].

Un análisis de ambos textos permitirá determinar si el RPD ha supuesto una mejora en la regulación de la aplicación territorial de la normativa y en sus mecanismos de defensa, y

[17] Sobre la presentación de propuestas necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información.

[18] Como remarcó Jan Philipp Albrecht, eurodiputado alemán del grupo Los Verdes-Alianza Libre Europea: «Los datos, por definición, cruzan las fronteras. Debemos disponer de normas comunes y de un sistema legal unificado para que todas las empresas compitan en igualdad de condiciones y para que los consumidores confíen en el mercado único europeo (…) además, los ciudadanos se verán beneficiados al estar mejor informados para decidir de manera más consciente». Disponible en: <http://www.europarl.europa.eu/news/es/news-room/20150616STO66729/Albrecht-se-dispone-a-negociar-la-reforma-de-la-protecci%C3%B3n-de-datos> [Consultado el 12/08/2016].

[19] OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, el sistema del Convenio Europeo de Derechos Humanos y el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal de 1981 (Convenio 108), además de la Carta y el TFUE. El Convenio Europeo de Derechos Humanos y la Carta se encuentran conectados a través del artículo 53.2 de esta última y por el artículo 6.3 del Tratado de la Unión Europea (AGENCIA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA (ADFUE), *Manual de legislación europea en materia de protección de datos*, 1ª edición, Luxemburgo (Oficina de Publicaciones de la Unión Europea) 2014, p. 18).

[20] Hay que tener en cuenta que, para la consecución de las pretensiones de la Comisión, se presentó, además del Reglamento, la Directiva 2016/680, sustitutiva de la Decisión 2008/977/JHA relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Por tanto, el Reglamento no se aplica a las actividades de tratamiento destinadas a los fines contemplados en la nueva Directiva.

[21] REDING, V., «The European data protection framework for the twenty-first century», *International Data Privacy Law*, vol. 2, núm. 3, 2012, p. 121. Disponible en: <http://idpl.oxfordjournals.org/content/2/3/119.full.pdf+html> [Consultado el 6/9/2017].

si todavía quedan lagunas por resolver. Así, comenzaremos con una serie de puntos comunes de uno y otro texto elegidos para el desarrollo posterior del trabajo.

III. PUNTOS COMUNES DE LA DIRECTIVA Y EL REGLAMENTO

El RPD, partiendo de las bases de la Directiva, adapta procedimientos y garantías a la nueva realidad social: se imponen nuevas obligaciones para las empresas y se pretende mejorar la eficacia en la protección de los titulares[22]. La necesidad de renovación de la normativa existente no supone, por tanto, el abandono del modelo de protección implantado por la Directiva ni romper con la jurisprudencia que sobre ella ha asentado el TJUE. Tal y como establece en su considerando segundo, el RPD tiene como base la continuidad de los principios que conforman el contenido esencial del derecho a la protección de datos. A partir de tal base, su finalidad es la de garantizar coherencia y uniformidad en una regulación de aplicación estricta, así como el desarrollo económico en el mercado interior y el otorgamiento de un mayor control a los ciudadanos sobre sus derechos y mayor seguridad jurídica y práctica[23].

De esta forma, ambos textos comparten conceptos y definiciones, siendo «dato personal» (art. 2.a) Directiva y 4.1) RPD) toda información que pueda relacionarse con una persona física – «interesado» – que de forma directa o indirecta pueda ser identificada o identificable. La idea de que la vida privada está relacionada directamente con los seres humanos[24] supone la exclusión de las personas jurídicas, aunque en ciertos casos podrían quedar protegidas[25]. Los elementos de la definición llevan a un concepto muy amplio y cualquier tipo de información, ya se refiera directa o indirectamente a un individuo, puede convertirse en un dato personal, siempre que, mediante la aplicación de técnicas, automatizadas o manuales, pueda llegar a ser posible identificar a una persona física concreta

[22] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), «El futuro de la protección de datos», *Monográfico de ASOCIACIÓN PROFESIONAL ESPAÑOLA DE LA PRIVACIDAD por el Día Europeo del Derecho a la Protección de Datos*, 2016. Disponible en <http://www.apep.es/aepd-el-futuro-de-la-proteccion-de-datos/> [Consultado el 25/09/2016].

[23] PERALES, A., «La vigencia del consentimiento en el futuro de la protección de datos personales», *Monográfico de la ASOCIACIÓN PROFESIONAL ESPAÑOLA DE LA PRIVACIDAD por el Día Europeo del Derecho a la Protección de datos,* 2016. Disponible en: <http://www.apep.es/aepd-el-futuro-de-la-proteccion-de-datos/> [Consultado el 22/09/2016].

[24] ADFUE, *Manual de legislación europea en materia de protección de datos*, cit., p. 14.

[25] En la medida en que pueda identificarse en la razón social a personas físicas (Sentencia Tribunal de Justicia de la Unión Europea (STJUE) 9 de noviembre de 2010, asuntos acumulados C-92/09 y C-93/09, *Schecke,* párr. 53). También si el responsable recoge datos de personas físicas y jurídicas indistintamente y los incluya en los mismos grupos de datos, pudiéndose entonces diseñar los mecanismos de tratamiento y el sistema de auditoría para que cumplan la normativa (GRUPO DEL ARTÍCULO 29, «Dictamen 4/2007 sobre el concepto de datos personales», 2007, p. 26. Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf> [Consultado el 19/07/2016].

por datos de su vida privada, sensibles[26] o no, o por imágenes[27]. Por otro lado, comparten el mismo objeto, que es proteger los derechos y libertades de los titulares, estableciendo criterios fundamentales que permitan calificar como lícito un tratamiento de datos por parte de responsables y encargados[28]. Por último, tanto el significado de tratamiento[29] como el ámbito de aplicación material es esencialmente el mismo (art. 3 de la Directiva y 2 del RPD).

Así, podemos partir de la idea de que para que un tratamiento de datos que encaje en el ámbito material del DUE[30] sea posible, este debe ser lícito en los términos de la norma, para proteger los derechos de los titulares. Sin embargo, ninguno de los dos textos tiene aplicación universal, por lo que cabe preguntarse cuándo quedan responsables y encargados sujetos al DUE. Aquí entran en juego los artículos 4 de la Directiva y 3 del RPD, que comparten la función de determinar el ámbito de aplicación territorial de la normativa europea.

IV. DERECHO APLICABLE AL TRATAMIENTO DE DATOS

En este punto se observan modificaciones por parte del RPD, en primer lugar, por las diferencias de la propia naturaleza de los instrumentos. Mientras que en la Directiva el artículo 4 cumple la doble función de determinar los supuestos en que será aplicable el DUE y, posteriormente, cuál es el EM que deberá aplicar su ley nacional fruto de la transposición[31]; en el RPD esta segunda función desaparece, pues en teoría el texto normativo va a ser el mismo en todos los EM, aunque sigan teniendo la posibilidad de regular algunas cuestiones. En ambos textos, la aplicación de los supuestos del artículo sobre el ámbito territorial de la norma debe hacerse de forma sucesiva. Dejando a un lado el supuesto por el que la normativa europea de protección de datos resulta aplicable en virtud de normas de Derecho internacional público[32], que se encuentra en segundo lugar en la Directiva y el

[26] Sobre el origen racial y étnico, opiniones políticas, religiosas y otras creencias, así como la afiliación sindical, y datos relativos a la salud o la vida sexual (art. 8 Directiva y 51 del RPD).

[27] En su párrafo 22, la STJUE de 11 de diciembre de 2014 consideró que la imagen de una persona grabada por una cámara constituye un dato personal (asunto C-212/13, *Rynes (František Ryneš contra* Úřad *pro ochranu osobních* údajů*,* ECLI:EU:C:2014:2428).

[28] Responsable es aquella persona física o jurídica que decide los fines y medios del tratamiento (art. 2.d) Directiva y 4.7 RPD). El encargado trata los datos por cuenta del responsable (2.e) Directiva y art. 4.8 RPD). Mientras que la Directiva solo atribuía obligaciones al responsable, el nuevo RPD reconoce también obligaciones del encargado de las que responde directamente.

[29] Todo tipo de operaciones realizadas sobre los datos, desde su recogida hasta su gestión, proceso o cesión a un tercero (art. 2.b) Directiva y art. 4.2) RPD).

[30] 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 (art. 3.1 Directiva y art. 2.1 RPD).

[31] BRKAN, M., «Data protection and European Private International Law», *EUI Working Paper RSCAS 2015/40,* Florence School of Regulation, Robert Schuman Centre for Advanced Studies, European University Institute, 2015, p. 32.

[32] Supuesto poco común en la práctica y que se mantiene en el cuerpo del Reglamento, si bien como tercer supuesto. El contenido de este apartado se refiere a situaciones en los que el Derecho internacional público

tercero en el RPD a la hora de realizar tal comprobación sucesiva, podemos identificar los otros dos supuestos de ambos textos según si el responsable –o encargado, en el caso del RPD– se encuentra o no establecido en el territorio de la Unión.

En el primer caso, tanto Directiva (art. 4.1.a)) como RPD, introduciendo algunos cambios en la terminología (art. 3.1), exigen dos condiciones: 1) un *establecimiento* del responsable en el territorio de la UE y 2) un tratamiento de datos en el *marco de las actividades – contexto de actividades* en el RPD – de tal establecimiento. En el ámbito de la Directiva, ambas condiciones arrastraron problemas interpretativos que intentaron ser resueltos por TJUE y el Grupo de Trabajo del Artículo 29 (GT29[33]), cuyas conclusiones se mantienen en el RPD, ya que este no incluye una definición expresa de *contexto de actividades* e incorpora en el considerando 22 la definición realizada sobre el término *establecimiento* por el TJUE y el considerando 19 de la Directiva. En ambos conceptos, se apuesta por una interpretación flexible y casuística.

Así, en lo que se refiere a la interpretación acerca de qué debe considerarse *establecimiento,* de la jurisprudencia y el considerando 19 de la Directiva se extrae la idea de un análisis caso por caso que determine si nos encontrarnos ante una «instalación estable» que realice una actividad real y efectiva, pudiendo bastar con que exista un único representante de una sociedad en un EM. Esta interpretación tan amplia permitió identificar los supuestos en los que un responsable tiene presencia en más de un EM, ya sea física o a través de un sitio de Internet –como ocurría en los asuntos *Weltimmo* y *Amazon EU Sárl*[34]–, lo que tenía su importancia a la hora de identificar la legislación de qué EM es aplicable al tratamiento. En cuanto al *marco o contexto de actividades,* el GT29 propone también una definición amplia y un análisis casuístico, en el que se determine cuál es el auténtico papel de cada establecimiento y qué actividades se efectúan en su marco, lo que puede ser perjudicial para los responsables a la hora de identificar la ley aplicable[35] en el ámbito de la Directiva. Un ejemplo claro de esta interpretación amplia es el asunto *Google Spain*[36], que analizaremos más adelante.

---

o acuerdos internacionales determinan el Derecho aplicable a una embajada, consulado, buque o aeronave (GT29, «Dictamen 8/2010 sobre el Derecho aplicable», 2010, p. 20, Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf> [Consultado el 09/11/2016]).

[33] Órgano consultivo independiente integrado por las Autoridades de Protección de Datos de los EM. Disponible en: <https://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php>. [Consultado el 22/09/2016]. El RPD sustituye al GT29 por el Comité Europeo de Protección de Datos cuyo objetivo es garantizar la aplicación coherente del Reglamento (cdo. 138 y 139; arts. 68 y ss. del RPD).

[34] STJUE, asunto C-230/14, 1 de octubre de 2015, *Weltimmo s.r.o contra Nemzeti Adatvédelmi és Információszabadság Hatóság* (ECLI:EU:C:2015:639). STJUE asunto C-612/16, 28 de julio de 2016, *Verein für Konsumenteninformation contra Amazon EU Sàrl* (ECLI:EU:C:2016:612).

[35] GT29, «Dictamen 8/2010 sobre el Derecho aplicable», cit., p. 18.

[36] STJUE, asunto C-131/12, 13 de mayo de 2014, *Google Spain SL y Google Inc. Contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (ECLI:EU:C:2014:317).

Si bien es cierto que los problemas que planteaba este apartado en la Directiva sobre qué ley nacional resultaba aplicable al tratamiento de datos han desaparecido gracias a la unificación jurídica, y que el Reglamento ha precisado que lo importante es el cumplimiento de esas dos condiciones, independientemente de que el responsable trate esos datos fuera de la Unión, es decir, sin que sea relevante su localización[37]; hubiera sido deseable una definición expresa de ambos conceptos en el cuerpo de la norma para otorgar una mayor seguridad jurídica en la aplicación del supuesto, ayudando a los responsables a conocer con exactitud la extensión de este apartado y a los titulares de datos ejercer sus derechos.

Donde mayores diferencias se aprecian entre uno y otro texto es en el caso de que el responsable – o encargado – no tenga un establecimiento en el territorio de algún EM. Esto es, aquellos supuestos en los que resulta aplicable el DUE aunque el responsable se encuentre fuera de la Unión. Tanto en la Directiva (art. 4.1.b)) como en el RPD (art. 3.2) se recogen condiciones o conexiones necesarias para ligar el tratamiento de datos realizado por un responsable fuera de la UE con la normativa de protección de datos europea. En la Directiva, tal conexión necesaria es la utilización de *medios*[38] –no con meros fines de tránsito– situados en territorio europeo. Ello implica como mínimo una actividad del responsable con intención de procesar los datos recogidos[39]. Esta previsión, que tenía por objetivo evitar la desprotección del interesado y comportamientos fraudulentos, como ubicarse artificialmente fuera de la UE para evitar aplicar su normativa al tratamiento[40], fue criticada por su amplitud por el GT29[41], pues podía llevar a la aplicación del DUE en supuestos que mantienen pocos lazos de conexión con la Unión, como puede suceder en el caso de un responsable que solo utilice medios ubicados en su territorio pero sin realizar el tratamiento en el mismo ni sobre sus residentes. Ello podría derivar en prácticamente una aplicación universal de la normativa que en realidad no tiene[42].

---

[37] GDPR Portal, «Frequently Asked Questions about the incoming GDPR». Disponible en <https://www.eugdpr.org/gdpr-faqs.html> [Consultado el 17/12/2017].

[38] Se apuesta por una amplia interpretación del criterio *medios*, que, por lo tanto, «incluye intermediarios humanos y/o técnicos tales como las muestras o encuestas. En consecuencia, se aplica a la recogida de información mediante cuestionarios, como ocurre, por ejemplo, en algunas pruebas farmacéuticas». (GT29, «Dictamen 8/2010 sobre el Derecho aplicable», cit., p. 23).

[39] GT29, «Dictamen 8/2010 sobre el Derecho aplicable», cit., p. 23.

[40] DE MIGUEL ASENSIO, P.A., «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», *Revista de la Facultad de Derecho de la Universidad de Granada*, 3ª. época, núm. 7, 2004, p. 412.

[41] «A modo de ejemplo, no es evidente en qué medida las terminales de telecomunicación o las partes de las mismas deban considerarse como medios. El hecho de que la herramienta se destine o use fundamentalmente para recoger o tratar ulteriormente datos personales puede considerarse un indicador a este respecto. Sin embargo, el que un responsable del tratamiento deliberadamente recoja datos personales, incluso incidentalmente, recurriendo a algún medio en la UE, también desencadena la aplicación de la Directiva» (GT29, «Dictamen 8/2010 sobre el Derecho aplicable», cit., p. 24).

[42] GT29, «Dictamen 8/2010 sobre el Derecho aplicable», cit., p. 27.

El RPD, siguiendo el contenido de la Directiva y las críticas del GT29[43], incluye dos tipos de condiciones que operarían como lazos de conexión en este último supuesto de responsables y encargados establecidos fuera de la Unión, para no acusar de injustificada la aplicación extraterritorial de la legislación europea. En primer lugar, el tratamiento debe ser sobre datos de *interesados que se encuentren en la Unión*[44]; y en segundo lugar que o *dirijan una oferta de bienes y servicios* o bien *controlen su comportamiento* – se moderniza la ley con supuestos como el uso de «cookies» y otros archivos informáticos que permiten el acceso a información en el equipo del usuario[45]; así como la actividad de empresas que utilizan información sobre el comportamiento para fines comerciales y publicitarios[46] –. Para que la aplicación de la legislación europea sea efectiva a partir de estas condiciones, se impone el nombramiento de un representante en la UE que actúe como contacto con Autoridades y ciudadanos[47], sin perjuicio de las acciones que puedan emprenderse contra el propio responsable o encargado.

La importancia de este cambio puede verse reflejada a través del asunto *Google Spain* ya mencionado. En este caso, la acción se dirigía contra Google Inc, sociedad ubicada en Estados Unidos, como responsable del tratamiento de datos cuya licitud se cuestionaba, ya que el establecimiento de Google en España, su filial *Google Spain*, desarrollaba una actividad de publicidad en apariencia ajena al tratamiento de datos objeto de controversia. Conforme a la legislación europea, el responsable que trataba los datos, Google Inc, lo hacía en el marco de sus actividades, pero en un establecimiento ubicado fuera del territorio de la UE (art. 4.1.a) Directiva). Ello implicaba que no era posible la aplicación de la legislación europea a menos que fuera posible demostrar la utilización de medios en el territorio como conexión necesaria (art. 4.1.c) Directiva), lo cual, como se ha adelantado, era una cuestión controvertida y compleja. Finalmente, para someter el tratamiento de datos a la legislación española, el Tribunal de Justicia razonó que la estrecha vinculación que existía entre la matriz Google en Estados Unidos y su filial en España permitía considerar que el marco de actividades de la primera se extendía al marco de actividades de la segunda, y, por tanto, se estaba ante los requisitos necesarios para aplicar la legislación europea (art. 4.1.a), pues

[43] El GT29 consideró que «existe una obvia necesidad de una mayor claridad y de ulteriores condiciones en la aplicación de este criterio para aportar mayor seguridad jurídica en el futuro marco de protección de datos» (GT29, «Dictamen 8/2010 sobre el Derecho aplicable», cit., p. 24).

[44] El texto literal en su versión española recoge la expresión «que residan en la Unión», sin embargo, un análisis comparado del texto en otros idiomas lleva a la conclusión de que su voluntad no se limita a residentes en la Unión (DE MIGUEL ASENSIO, P.A., «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», cit., párr. 14).

[45] DE MIGUEL ASENSIO, P.A., «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», cit., párr. 18.

[46] BRKAN, M., «Data Protection and Conflict-of-laws: A Challenging Relationship», *European Data Protection Law Review* 324, 341, 2016, p. 340.

[47] AEPD, «El Reglamento de protección de datos en 12 preguntas». Disponible en <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php> [Consultado el 10/09/2017].

existía un establecimiento del responsable en la UE, *Google Spain* (párr. 49), que trataba datos en el marco de sus actividades (párr. 52-56, 60)[48].

Con el nuevo Reglamento, los lazos de conexión con la Unión se aclaran y se otorga mayor seguridad jurídica en la aplicación de las normas europeas en caso de que el responsable no se encuentre establecido en el territorio de la UE, pues ya no se basan en la condición del uso de medios ubicados en el territorio. En el marco del RPD el caso *Google Spain* se habría resuelto de una manera más sencilla, dirigiendo la acción contra Google Inc, ya que estamos ante interesados ubicados en la UE sobre los que trata datos un responsable fuera de la misma. Todo ello en la medida en que el supuesto cumpliera además con las dos nuevas condiciones de conexión del RPD a partir de un análisis de su actividad, sin necesidad de acudir a estrategias interpretativas como la realizada por el TJUE, quizá difícilmente extrapolables a otros supuestos. Sin embargo, pese a las mejoras introducidas por el RPD en estos casos en los que el responsable no se encuentra ubicado en la UE, aclarando la aplicación de la norma[49], no se han conseguido superar las críticas sobre una posible extensión global y extraterritorial de la legislación de la UE[50], especialmente en lo que se refiere a la primera condición[51].

---

[48] Además, desde una perspectiva de Derecho de grupos, Alfaro Águila-Real considera que es «contrario a la buena fe desarrollar la actividad mediante la cooperación estrecha entre las distintas sociedades que forman el grupo para, a continuación, ordenar a las sociedades del grupo que rechacen las reclamaciones de terceros que no tienen relación contractual con las sociedades del grupo porque dichas reclamaciones deban dirigirse, según decida la matriz, a una o a otra sociedad del grupo» (ALFARO ÁGUILA-REAL, J., «La sentencia Google del Tribunal Supremo: Derecho de grupos y levantamiento del velo», entrada blog 14 abril 2016. Disponible en <http://almacendederecho.org/la-sentencia-google-del-tribunal-supremo-derecho-de-grupos-y-levantamiento-del-velo/> [Consultado el 30/01/2018]).

[49] «Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU» (GDPR Portal, «An overview of the main changes under GPDR and how they differ from the previous directive». Disponible en <https://www.eugdpr.org/key-changes.html> [Consultado el 17/12/2017]).

[50] BRKAN, M., «Data Protection and Conflict-of-laws: A Challenging Relationship», cit., p. 338.

[51] « (…) this protection would them seem to attach to the very person of EU residents so as to enable them to rely on this protection also when travelling outside the EU. For example, an EU resident providing personal information during a holiday in New York would be protected by the EU data protection Regulation by virtue of the EU residence. This is so clearly inappropriate (…) » (SVANTESSON, D., *Extraterritoriality in Data Privacy Law*, cit., pp. 107-108).

V. REMEDIOS EN CASO DE TRATAMIENTO ILÍCITO

Si el titular desea reclamar por la forma en que han tratado sus datos, existen en ambos textos dos tipos de remedios: 1) una tutela administrativa ante las autoridades de control, cuya actuación puede ser objeto de reclamación judicial y 2) aquellos que se dirigen contra los responsables del tratamiento y, en el caso del RPD, contra los encargados, en lo referente a las obligaciones por las que responden directamente. En este ámbito vemos sustanciales diferencias entre la Directiva y el RPD.

1. Tutela administrativa

Sobre la tutela administrativa, debe señalarse, en primer lugar, que con el RPD las autoridades de control, como «guardianas de los derechos relacionados con el tratamiento de datos personales»[52] establecidas en todos los EM, han experimentado un empoderamiento no solo en términos de una mayor profundización en sus competencias y funciones, sino también en su jurisdicción. A partir del supuesto de hecho del asunto *Schrems*[53]*,* podrán apreciarse con mayor claridad los cambios introducidos por el RPD en este sentido.

En este asunto, el señor Schrems, residente en Austria, era usuario de la red social Facebook, lo que implica la existencia de un contrato con Facebook Ireland, filial en el territorio europeo de la matriz Facebook Inc, con domicilio en Estados Unidos. El señor Schrems, al no estar conforme con el tratamiento de datos que realiza Facebook, opta por la vía administrativa y se dirige ante las autoridades de control y no directamente contra los responsables. Sin embargo, en el marco de la Directiva, la autoridad de control competente para conocer la reclamación queda determinada por la legislación nacional que resulte aplicable. Es decir, existe una correlación entre ley aplicable y competencia de las autoridades de control (art. 28.6 Directiva). En este caso, la ley aplicable al tratamiento era la irlandesa, pues Facebook Ireland, establecida en Irlanda, trataba los datos del señor Schrems en el marco de sus actividades (art. 4.1.a) Directiva). De esta forma, pese a que su residencia habitual se encuentre en Austria, el señor Schrems debe dirigir su reclamación ante la autoridad de control irlandesa, que es la única competente para conocer el asunto (art. 28.4 y 28.6 Directiva).

Las desventajas de esta correlación entre ley aplicable y competencia no se reducen a los inconvenientes que puedan suponer el interponer una reclamación fuera de la residencia habitual del titular de datos, pues, además, la posible sanción impuesta por la autoridad, irlandesa en nuestro caso, sólo tendrá efectos en Irlanda. Si el señor Schrems se dirige a

[52] Párrafo 23, STJUE 9 de marzo de 2010, asunto C-518/07, *Comisión Europea/Alemania*, (ECLI:EU:C:2010:125).

[53] STJUE 6 octubre 2015, asunto C-362/14, *Maximillian Schrems contra Data Protection Commisioner*, (ECLI:EU:C:2015:650).

la autoridad de control de su EM, esta no tendría competencia para imponer sanciones a Facebook Ireland. Tal y como reconoció el TJUE en el asunto *Weltimmo* (párr.57): «si [la autoridad de control] llega a la conclusión de que es aplicable el Derecho de otro EM, no puede imponer sanciones fuera del territorio del propio EM. En tal situación, le corresponde instar, en ejecución de la obligación de cooperación que se establece en el artículo 28.6 (…) a la autoridad de control de ese otro EM a declarar una eventual infracción de ese Derecho y a imponer sanciones si este lo permite, basándose, en su caso, en la información que ella le haya remitido.».

Como señalábamos anteriormente, el nuevo RPD introduce modificaciones en la jurisdicción en la que las autoridades de control pueden ejercer sus competencias y poderes, pues se elimina esa correlación de ley nacional y competencia en la medida en que existe unificación normativa. Su ámbito de actuación y competencias ya no se limita exclusivamente al EM al que pertenecen[54]. Si bien se mantiene la competencia de las autoridades de control para desempeñar las funciones que se les asignen y ejercer los poderes que se le confieran en el territorio de su EM (art. 56.2 RPD), se prevé también la posibilidad de que la autoridad de control de un EM pueda actuar en el territorio de otro EM. Ello resultará especialmente relevante para los «tratamientos transfronterizos» de datos (art. 4.23 RPD) dentro del territorio de la UE, como puede ser el asunto *Schrems.*

Según el RPD, pueden identificarse dos supuestos de tratamientos transfronterizos: 1) o bien el tratamiento se realiza en el contexto de las actividades de un establecimiento de un responsable o encargado de la UE y el responsable o encargado está establecido en más de un EM; 2) o bien el tratamiento tiene lugar en el contexto de las actividades de un único establecimiento de un responsable o encargado afecta o es probable que afecte sustancialmente a interesados en más de un EM. Es en este segundo supuesto se encontraría el asunto *Schrems*.

En estos casos en los que varios EM resultan afectados por un tratamiento, el RPD prevé un régimen específico de determinación de la autoridad competente, de la autoridad cuyas decisiones serán vinculantes (art. 56.1 RPD), y podrán tener efectos en otros territorios. Este régimen específico es el denominado mecanismo de *ventanilla única* o mecanismo de coordinación. Conforme a este mecanismo, la autoridad competente será la que se identifique como *autoridad principal*, es decir, la autoridad de control del EM del establecimiento principal o del único establecimiento del responsable o encargado en la UE. El resto de autoridades de control afectadas por el mismo tratamiento serán consideradas como *autoridades interesadas* que participan en el proceso de decisión, si bien la competencia la ostenta la principal (arts. 4.22, 55, 56.1, 60-62 RPD). En teoría, este mecanismo de coordinación o ventanilla única, que no debe aplicarse cuando el tratamiento sea realizado por autoridades públicas u organismos privados en interés público (art. 55.2 RPD), pretende conseguir una mayor armonización y uniformidad en la aplicación del RPD, aunque habrá

[54] STJUE 1 de octubre 2015, asunto C-230/14, *Weltimmo* (párr. 57).

que esperar a ver cómo funciona realmente este mecanismo en la práctica, que supone la actuación de una autoridad de control en jurisdicciones que no son la suya.

Volviendo al supuesto de hecho del asunto *Schrems,* la autoridad principal o autoridad competente será la autoridad irlandesa, como ocurría anteriormente, pero por ser la autoridad de control del territorio en el que se ubica el único establecimiento del responsable del tratamiento. Además, a diferencia de lo que ocurría en el marco de la Directiva, con el nuevo Reglamento las decisiones que adopte tendrán efectos y serán vinculantes en otros EM, como sería el caso de Austria. Es importante destacar que estas normas de competencia no se refieren a la autoridad de control ante la que los titulares de datos deben presentar su reclamación, pues el nuevo RPD prevé la posibilidad de que cualquier interesado pueda presentar reclamación ante una autoridad de control en el lugar de su residencia habitual, en el EM de su lugar de trabajo o en el EM en el que se haya cometido la infracción (art.77).

La gestión que de esa reclamación presentada por el interesado haga la autoridad de control podrá ser objeto de reclamación judicial (art. 78 RPD), y la competencia de los tribunales para conocer la misma va a depender de su actuación. Así, si la autoridad de control toma una decisión, las acciones judiciales deberán ejercitarse en el EM en que esté establecida dicha autoridad de control (art. 78.3). En el caso *Schrems,* si la autoridad irlandesa, competente en virtud del mecanismo de ventanilla única, toma una decisión con la que no está conforme, el interesado deberá dirigirse a los tribunales irlandeses. Si por el contrario la autoridad de control no da curso a la reclamación o en el plazo de tres meses no informa sobre su estado o resultado, existirá derecho a la tutela judicial siempre que tal autoridad fuera competente en virtud de la aplicación del mecanismo de ventanilla única en los supuestos transfronterizos o, fuera de estos supuestos, en virtud de ser la autoridad competente en su EM (art. 78.2). En nuestro supuesto de hecho, si el señor Schrems decide plantear su reclamación ante la autoridad de control austríaca, por ser el lugar de su residencia, y esta no da curso a su reclamación o no informa en el plazo de tres meses, su tutela se ve limitada, ya que sólo si la autoridad de control era competente en virtud del mecanismo de ventanilla única será posible acudir a la vía judicial. Por lo tanto, pese a la elección que deja el legislador, ante qué autoridad se interpone la reclamación es importante a efectos de una tutela judicial efectiva posterior en el orden Contencioso-administrativo, y requiere el conocimiento de la normativa.

2. Tutela judicial civil ante la actuación de responsables y encargados

Pasando a la tutela judicial civil, es importante destacar que por esta vía se ejercitarán acciones tales como la obtención de la imposición al responsable de una limitación o prohibición de tratamiento, como alternativa a la reclamación administrativa, o acciones de indemnización –reclamación que no puede presentarse ante las autoridades de control–,

sin que nada parezca impedir la interposición de acciones relativas a un contrato, siempre que el objeto se refiera a la vulneración de normas del RPD[55].

Se han introducido importantes mejoras en la tutela civil, ya que el RPD excluye en principio la situación anterior por la que no existía paralelismo entre la ley aplicable y la jurisdicción, pues las disposiciones de la Directiva no afectan a la competencia de los órganos judiciales. Ello significa la necesaria distinción de tres supuestos distintos para poder determinar la competencia judicial, diferenciando entre aquellos en los que no existe elemento de internacionalidad por residir demandante y demandado en el mismo EM y supuestos en los que el demandado no tiene domicilio en el Estado del interesado, pudiendo estar o bien en otro EM o bien fuera de la UE. En el caso de que el domicilio del demandado se encontrara fuera del UE, debe acudirse a las normas nacionales de Derecho internacional privado (DIPr), concretamente, en el caso español, al artículo 22 de la Ley Orgánica del Poder Judicial, con las complejidades que su nueva reforma supone a la hora de aplicarlo[56]. En caso de que sí se encontrara en territorio de la Unión, la posible aplicación del Reglamento 1215/2012 relativo a la competencia judicial, Bruselas I*bis* (RBI*bis*), resultaba para la doctrina complejo y dudoso, debido a los problemas interpretativos que podían plantearse entre los conceptos de la Directiva y los del RBI*bis*[57] o cómo operan sus normas en el ámbito de la protección de datos[58]. El nuevo RPD no solo determina unas reglas claras de competencia judicial, sino que además resuelve su relación con el RBI*bis* en estas cuestiones.

---

[55] DE MIGUEL ASENSIO, P.A., «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», cit., párr. 36.

[56] Como critica DE MIGUEL ASENSIO, P.A. («La cuestionable revisión de las normas de competencia judicial internacional (LO 7/2015 de reforma de la LOPJ)», entrada de blog de 23 julio 2015. Disponible en: <http://pedrodemiguelasensio.blogspot.com.es/2015/07/la-cuestionable-revision-de-las-normas.html>. [Consultado el 22/10/2016]), la nueva reforma de la LOPJ podía perjudicar al titular de datos pues su contenido es más complejo que el anterior y agrava las carencias propias de la fragmentación y dispersión de normas, a lo que se suma la falta de coordinación del texto no sólo con instrumentos europeos e internacionales, sino también con las normas internas de competencia. Esta reforma también ha sido criticada por otros autores como GARCIMARTÍN ALFÉREZ, F.J., («La competencia judicial internacional en la reforma de la LOPJ», *Diario la Ley*, Nº8614, 28 septiembre de 2015, Ed. La Ley).

[57] Como si se podría considerarse que el término *domicilio* del RBI*bis* puede corresponderse con la noción de *establecimiento* de la Directiva. En este sentido, hay que recordar que la Directiva no recoge ninguna disposición sobre competencia judicial, por lo que no parece que la noción de *establecimiento* haya sido contemplada como un criterio de atribución de competencia (BRKAN, M., «Data protection and European Private International Law», cit., p. 11).

[58] En términos generales, encajar la protección de datos a través de la aplicación del RBI*bis* va a ser complejo, pues la relación que existe entre el responsable del tratamiento de datos y el titular de los mismos no tiene una expresión jurídica clara, ya que un tratamiento lícito de datos depende de una serie de condiciones variadas, desde el otorgamiento del consentimiento, que no queda claro que sea una materia puramente contractual o no, hasta la existencia de una relación contractual en la que el tratamiento sea necesario para la ejecución del contrato pero no para el objeto propio del mismo (art. 7.1.b) RBI*bis*). Todo ello se agrava ante la posibilidad de aplicación o no de los foros de protección o incluso una posible autonomía de la voluntad de las partes.

Así, el artículo 79 y el considerando 147 determinan que las normas sobre competencia judicial del RPD prevalecerán sobre las del RBI*bis*[59] y actuarán como fueros adicionales del mismo (art. 67 RBI*bis*), sin que en ningún caso sus reglas puedan producir como resultado el efecto de excluir al contenido del RPD[60]. Conforme al artículo 79.2 del RPD, los perjudicados pueden optar entre acudir a los tribunales de cualquier EM en el que el responsable o encargado tengan un establecimiento, o bien a los tribunales en los que el interesado tenga su residencia habitual, esto último salvo que el responsable o encargado sea una autoridad pública de un EM que actúe en el ejercicio de sus poderes públicos.

Además de aclarar no solo los tribunales competentes, sino la relación con el RBI*bis*, el RPD recoge una serie de previsiones de ámbito procesal que mejoran también la anterior regulación, como la posibilidad de que una entidad, organización o asociación sin ánimo de lucro cuyos objetivos estatutarios sean de interés público, puedan presentar reclamación en nombre de los interesados, así como ejercer sus derechos (art. 80), si bien no establece normas de competencia judicial en este sentido[61]. Por otra parte, el RPD introduce las reglas que deben seguir juzgados y tribunales de los EM en caso de pendencia del mismo proceso en dos EM (art. 81). Tal y como explica De Miguel Asensio[62], la ubicación de este artículo en el texto es confusa, pero no se refiere a procedimientos en los que se conocen acciones entre partes privadas, pues ello carecería de justificación ante el modelo más elaborado de litispendencia y conexidad del RBI*bis*. Por tanto, este artículo parece referirse a acciones judiciales ejercitadas contra la actuación de la autoridad de control. Esta argumentación se basa en los considerandos 144 y 147, que disponen la primacía del RPD sobre el RBI*bis* para las «normas específicas sobre competencia judicial», por lo que implícitamente se mantiene la supremacía del segundo sobre el primero en el resto de normas, entre ellas aquellas sobre litispendencia y conexidad, que además se vinculan con el sistema de reconocimiento y ejecución de resoluciones.

VI. ENCAJE DEL RPD EN EL MARCO JURÍDICO DE LA UNIÓN

1. Relación con normas dirigidas a la protección de datos

El RPD supone un cambio en el sistema de fuentes. Pese a que entró en vigor el 25 de mayo de 2016, no se aplicará hasta dos años después, el 25 de mayo de 2018. Ello implica

[59] DE MIGUEL ASENSIO, P.A., «Aspectos internacionales del Reglamento general de protección de datos de la UE (I): cuestiones de competencia», entrada de blog de 11 de marzo de 2016. Disponible en <http://pedrodemiguelasensio.blogspot.com.es/2016/05/aspectos-internacionales-del-reglamento.html> [Consultado el 31/10/2016].

[60] DE MIGUEL ASENSIO, P.A., «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», cit., párr. 36.

[61] De Miguel Asensio propone aquí, ante la ausencia de normas de competencia en casos de acciones colectivas en el RBI*bis*, una interpretación de las normas del art. 79.2 RPD para estas situaciones («Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», cit., párr. 37).

[62] Ídem.

que hasta dicha fecha tanto la Directiva 95/46/CE como las normas nacionales de transposición siguen siendo válidas y aplicables[63]. Tras su entrada en vigor, el efecto directo del RPD no supone per se la prohibición de adoptar por parte de los EM sus propias medidas legislativas nacionales, pero, en caso de hacerlo, ello deberá estar siempre dentro de los límites del propio Reglamento.

Es decir, nada impide que las regulaciones nacionales completen y complementen en su jurisdicción su contenido; es más, es el propio Reglamento el que hace referencias a la potestad legislativa de los EM, llegando incluso a imponer la necesidad de que sean ellos los que desarrollen las medidas específicas a contenidos de carácter general que en él se regulan, como ocurre en el Capítulo IX, donde pueden observarse ejemplos de estas imposiciones en el artículo 85, relativo a la adopción de medidas para garantizar la libertad de expresión, previsión ya contenida en la Directiva, o en el artículo 88, sobre reglas de protección de datos en el ámbito laboral[64]. Se reconoce también la facultad de los EM de mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del Reglamento para el cumplimiento de una obligación legal o de una misión realizada en interés público (considerando 10). Por tanto, no es correcto afirmar que el RPD supone la derogación total y el simple reemplazo de las legislaciones nacionales[65] sino que en realidad conforma una nueva relación entre fuentes, de tal forma que lo que sí queda sustituido es todo aquello que sea contenido del Reglamento, sin que se impida por ello la adopción de medidas legislativas adicionales y complementarias del mismo, siempre y cuando estas no vayan más allá de los poderes de actuación normativa que prevé el Reglamento.

Sin embargo, cabe plantearse entonces qué ocurrirá con aquella legislación nacional que fue más protectora que la Directiva –permitida en su considerando 22–. Kotschy[66] se decanta por considerar que esas normas nacionales no tendrán la consideración de «lex specialis» respecto del RPD, sino que estas leyes entrarán dentro del marco de la protección de datos en la medida en que supongan una forma de particularizar su aplicación sin entorpecer su efecto directo. Así, simplemente quedarán relegadas a cumplir la función de detallar las previsiones impuestas por el Reglamento, sin que puedan ser en ningún caso incompatibles con ellas.

Esta relación entre fuentes no difiere en exceso de la ya existente con la Directiva, pues, tal y como señalaba el TJUE en el asunto *Lindqvist*[67], los EM podían prever una regulación más protectora en el marco del contenido a armonizar, y ello siempre y cuando se respetara

63 AEPD, «El Reglamento de protección de datos en 12 preguntas», cit.

64 REDING, V., «The European data protection framework for the twenty-first century», cit., p. 122.

65 HUSTINX, P., «EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation», p. 30. Disponible en <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publi cations/Speeches/2014/14-09-15_Article_EUI_EN.pdf>. [Consultado el 15/09/2016].

66 KOTSCHY, W., «The proposal for a new General Data Protection Regulation – problems solved? », *International Data Privacy Law*, 2014, vol. 4, núm. 4, 2014, p. 275.

67 STJUE 6 de noviembre de 2003, asunto C-101/01, *Bodil Lindqvist*, (ECLI:EU:C:2003:596).

el objetivo de mantener un equilibrio entre la libre circulación de datos y la protección de la privacidad (párr. 96-99). Por otra parte, conviene recordar que en todo aquello que no entra dentro del ámbito de aplicación del RPD (art. 2.2) podrá ser regulado por cada una de las legislaciones nacionales[68] como ocurre por ejemplo con el tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas o con el tratamiento de datos de personas fallecidas, lo cual dificulta el objetivo de conseguir la unificación normativa.

En lo que se refiere a la relación del Reglamento con el resto de normativa europea sobre protección de datos, pese a que la Comisión defendió en un principio la interpretación de que no tuviera ningún tipo de relación legal con otros instrumentos[69], finalmente, se recoge expresamente su relación con algunos de ellos, como el Reglamento nº45/2001[70] (cdo. 17 y art. 2.3), del que dispone su adaptación a las normas y principios del RPD conforme a su artículo 98, o la Directiva 2000/31/CE de comercio electrónico, que se entenderá sin perjuicio del RPD, en particular las normas que dicha Directiva contiene en sus artículos 12 a 15[71] (cdo. 21 y art. 2.4).

2. Relación con otras normas del Derecho de la Unión

Respecto de otros actos jurídicos de la UE, más allá de la ya explicada relación con el RBI*bis* (cdo. 79 y art. 79), el RPD no se pronuncia sobre su relación con otros instrumentos normativos como el Reglamento Roma I (RRI) o Reglamento Roma II (RRII)[72] y no aduce ninguna razón por la que sí se refiere a algunos reglamentos y no a otros. Únicamente en su artículo 98 se limita a disponer que «la Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos». En este sentido, parece que la Comisión y el Parlamento pretenden terminar con la fragmentación jurídica y la multiplicidad de normativas que suponga la vuelta a la situación que se pretende mejorar.

---

[68] GABEL, D. y HICKMAN, T., «Unlocking the EU Data Protection Regulation.», 22 de julio de 2006, Disponible en: <http://www.whitecase.com/publications/article/chapter-6-data-protection-principles-unlocking-eu-general-dataprotection> [Consultado el 25/10/2016].

[69] KOTSCHY, W., «The proposal for a new General Data Protection Regulation – problems solved? », cit., p. 276.

[70] Sobre el tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión.

[71] Sobre responsabilidad de los prestadores de servicios intermediarios.

[72] Reglamentos 593/2008 sobre ley aplicable a las obligaciones contractuales, Roma I (RRI) y 864/2007 relativo a la ley aplicable a las obligaciones extracontractuales, Roma II (RRII).

Siguiendo con la relación no especificada entre el nuevo RPD y los RRI y RRII, en lo que se refiere a una posible interrelación de instrumentos, las dudas que existían en relación con la Directiva – pues había voces que consideraban que podría identificarse, por aplicación del artículo 23 de RRI y 27 de RRII, como ley especial frente a la ley general que supondrían ambos, y otras que debían excluirse de forma taxativa del ámbito de la protección de datos[73] – parecen desaparecer con el RPD, al considerarse que la unificación de normativas elimina los conflictos de leyes, y excluye en su ámbito de aplicación al resto de instrumentos normativos, por lo que solo cabría plantearse una relación entre RRI, RRII y el RPD en caso de que sean necesarias normas de conflicto para determinar la ley aplicable en aquellas cuestiones cuya regulación el RPD deja en manos de los EM. En términos generales, en el caso de RRII parece claro que la protección de datos forma parte de la exclusión del artículo 1.2.g) sobre la violación de la intimidad o privacidad, en la medida en que el TJUE[74] ha señalado que, aunque la privacidad y la protección de datos sean dos derechos reconocidos en la Carta, el primero es el núcleo del segundo[75]. Así, la relación más compleja y discutida es aquella que pueda establecerse entre RRI y la normativa de protección de datos[76].

Ello se debe a que en la protección de datos están implicadas partes civiles, pero también autoridades públicas, como son las autoridades de control, que velan por el cumplimiento de la normativa. Estamos en una zona gris, ni puramente civil ni puramente administrativa[77] que lleva a excluir la aplicación de RRI de acuerdo con su artículo 1 –lo cual es un argumento también aplicable a la exclusión del RRII conforme, también, a su art. 1–. Sin embargo, es cierto que una cosa es dirigirse contra la actuación de una autoridad pública, y otra pedir responsabilidades a aquél que, sujeto por la normativa, la ha incumplido en su perjuicio, por lo que este argumento se debilita ante esta posible separación de acciones según las partes implicadas.

Pese a ello, en cualquier caso, el derecho a la protección de datos es un derecho fundamental, lo que justifica que no pueda apartarse su tutela de las normas dirigidas a tal efecto y que pueda considerarse, a efectos del RRI, que estamos ante una norma internacionalmente imperativa en el marco del artículo 9. Brkan se apoya en dos argumentos clave para explicar esta calificación: 1) como ha reconocido la jurisprudencia del TJUE en varias ocasiones, empezando tal doctrina en el asunto *Ingmar*[78], las normas del DUE también pueden ser

[73] Identificadas por BRKAN, «Data protection and European Private International Law», cit., pp. 27-31.

[74] STJUE 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland* (ECLI:EU:C:2014:238): «La protección de datos de carácter personal, que resulta de la obligación expresa establecida en el artículo 8, apartado 1, de la Carta, tiene una importancia especial para el derecho al respeto de la vida privada, consagrado en el artículo 7 de esta» (párr. 53).

[75] KOKOTT, J. y SOBOTTA, C., "The distinction between privacy and data protection in the jurisprudence of CJEU and ECtHR", *International Data Privacy Law*, vol. 3, núm. 4, 2013, Oxford (Oxford University Press), pp. 223.

[76] BRKAN, M., «Data Protection and Conflict-of-laws: A Challenging Relationship», cit., p. 333.

[77] Expresión citada por BRKAN, «Data Protection and Conflict-of-laws: A Challenging Relationship», cit., p. 27.

[78] STJUE 9 de noviembre de 2000, Asunto C-381/98, *Ingmar GB Ltd contra Eaton Leonard Technologies Inc.,* (ECLI:EU:C:2000:605).

calificadas como «normas de policía»; 2) estamos ante una norma que verdaderamente protege el interés público, en la medida en que protege un derecho fundamental y su normativa persigue la consecución de intereses para el mercado interior[79].

Ante el silencio del RPD, siguen quedando dudas en la posible aplicación de las normas de conflicto del RRI en todo aquello que los EM decidan regular sobre protección de datos al margen de las leyes europeas. Por otra parte, en lo que se refiere a obligaciones extracontractuales, especialmente problemático es el supuesto de las acciones de indemnización en caso de tratamiento ilícito de datos, ya que con el RPD siguen existiendo muchas diferencias entre las legislaciones nacionales, por lo que en caso de que nos encontremos un supuesto transfronterizo, ante la exclusión del ámbito de Roma II, debemos acudir a las normas nacionales, en nuestro caso, al artículo 10.9 del Código Civil[80].

VII. CONCLUSIONES

La privacidad y los datos personales son consustanciales a la dignidad del ser humano y a su derecho de preservar un ámbito de intimidad resguardado del resto. No obstante, los avances tecnológicos y la globalización, junto al desarrollo de la sociedad de la información, han provocado un aumento del tratamiento automatizado de datos personales y han puesto de manifiesto las deficiencias en la protección de estos derechos[81]. Todo ello se ha visto agravado por las innovaciones de las últimas décadas en el ámbito de la tecnología e Internet, que han llevado a un cambio de percepción de la privacidad por parte de los usuarios y a un manejo de datos personales como si fueran una mercancía más que promueve el desarrollo económico y comercial.

En los problemas que se plantean en este ámbito entran en juego la regulación no solo de supuestos internacionales, sino también los mismos en un contexto que requiere importantes adaptaciones jurídicas como es Internet, cuyo carácter descentralizado y universal hace difícil un control únicamente ejercido por un determinado Estado en ciertas situaciones[82]. Así, estamos ante problemas de carácter global para los que una legislación nacional o regional resulta limitada. De ahí que el papel de la UE haya sido trascendental en la protección de los datos personales como legislador supranacional y como líder en la

[79] BRKAN, M., «Data Protection and Conflict-of-laws: A Challenging Relationship», cit., pp. 333-334.

[80] DE MIGUEL ASENSIO, P.A., «Aspectos internacionales del Reglamento general de protección de datos de la UE (II): Derecho aplicable», entrada de blog de 19 de mayo 2016. Disponible en <http://pedrodemiguelasensio.blogspot.nl/2016/05/aspectos-internacionales-del-reglamento_19.html> [Consultado el 31/10/2016].

[81] ORDOÑEZ SOLÍS, D., «La protección judicial de los derechos en Internet», Real Academia Asturiana de la Jurisprudencia, 12 de marzo de 2014, en: https://kontencioso.files.wordpress.com/2014/03/proteccic3b3n-judicial-raaj.pdf. [Consultado el 23/08/2017].

[82] MURILLO DE LA CUEVA, P.L., «Novedades sobre el derecho a la protección de datos personales», *El derecho a la protección de datos: novedades y problemas*, Aranjuez (Ed. Fundación Ciudadanía y Valores), 2010, p. 1-16.

regulación de la protección de datos, responsable de la implantación de un elevado sistema de protección[83] como fue la Directiva 95/46/CE. Sin embargo, en 1995 resultaba imposible prever la evolución del entorno digital y la importancia que ha adquirido Internet en el funcionamiento de la sociedad[84], lo cual dejó desfasada a la Directiva, obligando a la Unión Europea a plantearse una revisión de la normativa.

De tal revisión normativa nace el nuevo *Reglamento de Protección de Datos* y si bien es cierto que se ha analizado de forma breve aspectos muy concretos del mismo, pueden extraerse una serie de conclusiones:

1. El RPD supone un indudable avance en la protección de datos respecto la Directiva, pues no sólo moderniza su contenido, sino que aumenta la certidumbre y la seguridad jurídica gracias a la armonización, que elimina los problemas que surgían en el marco de la Directiva como consecuencia de la uniformización jurídica limitada. No obstante, este objetivo se ha conseguido en parte, ya que responsables y encargados deben seguir enfrentándose, a la hora de tratar datos y demostrar el cumplimiento de la regulación europea, a materias que dentro del RPD debe regular cada EM, que es precisamente lo que se pretendía evitar. Además, ello supone la existencia de diferencias en la protección de los titulares según el territorio en dichas materias.

2. Esto, por otro lado, se ve agravado por la falta de previsión de su relación con otros instrumentos y ramas del Derecho, como son los contratos o la responsabilidad extracontractual, lo que es fundamental para facilitar la tutela de los interesados. Pese a que se introduce una clara mejora en el ámbito de la determinación de la competencia judicial y su relación con el Reglamento Bruselas I*bis*, ello no tiene su reflejo en las relaciones con otros instrumentos de DIPr sobre ley aplicable, como son las normas de conflicto de los Reglamentos Roma I y Roma II. Debido a la transversalidad de la materia, una aclaración en la relación de instrumentos por parte de la UE podría facilitar la tutela de los titulares y el cumplimiento de obligaciones de responsables y encargados.

3. Si bien el RPD ha supuesto la introducción de una mayor claridad y precisión en los supuestos que determinan la aplicación territorial de la normativa europea, mejorando así el ámbito de aplicación territorial tan complejo que contemplaba la Directiva; siguen existiendo críticas ya planteadas con la Directiva como su posible aplicación extraterritorial, y se echa en falta una mayor precisión conceptual en los supuestos.

4. El RPD introduce importantes novedades en el ámbito de la determinación de la competencia judicial, con normas específicas que faltaban en la Directiva, y en la aclaración de su relación con el RBI*bis*; sin embargo, no queda del todo resuelto cómo operan las normas de competencia judicial en los casos en los que se reclama frente a la actuación

[83] SANCHO VILLA, D., «Protección de datos personales y transferencia internacional: cuestiones de ley aplicable», *Revista jurídica de Castilla y León*, núm. 16, septiembre 2008, p. 414.

[84] MINERO ALEJANDRE, G., «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», cit. p. 22.

de las autoridades de control, ya que parece que en la práctica pueden surgir problemas de tutela en casos en los que opera el mecanismo de competencia interno de ventanilla única.

Así, el RPD constituye el primer paso, absolutamente necesario, en un largo camino que lleve a una regulación en pro del fortalecimiento de una verdadera cultura de protección de datos en la que se consiga transmitir a titulares y responsables la necesidad de conseguir un adecuado equilibrio entre el desarrollo de la economía y la defensa de un derecho tan fundamental como es la protección de datos. Se trata de un instrumento que no estará exento de reformas, que deberá adaptarse a una sociedad que no deja de innovar y avanzar tecnológicamente a un ritmo al que el legislador debe necesariamente adecuarse y anticiparse para evitar situaciones irreversibles. Conseguir una protección de datos europea real y efectiva requiere todavía de trabajo en el futuro[85] y será de nuevo la práctica jurídica la que la a través de la jurisprudencia señalará y solucionará las posibles deficiencias del RPD, como ocurrió con la Directiva 95/46/CE, dando pistas al legislador para reformas posteriores que resulten necesarias para proteger y garantizar a los titulares de datos un verdadero poder de disposición sobre su propia información, que es el objetivo último de este derecho.

VIII. BIBLIOGRAFÍA

AGENCIA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA, *Manual de legislación europea en materia de protección de datos*, 1ª edición, Luxemburgo, (Oficina de Publicaciones de la Unión Europea), 2014.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, «El futuro de la protección de datos», *Monográfico de ASOCIACIÓN PROFESIONAL ESPAÑOLA DE LA PRIVACIDAD por el Día Europeo del Derecho a la Protección de Datos*, 2016. Disponible en <http://www.apep.es/aepd-el-futuro-de-la-proteccion-de-datos/> [Consultado el 25/09/2016].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, «El Reglamento de protección de datos en 12 preguntas». Disponible en <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php> [Consultado el 10/09/2017].

ALFARO ÁGUILA–REAL, J., «La sentencia Google del Tribunal Supremo: Derecho de grupos y levantamiento del velo», entrada de blog de 14 de abril 2016. Disponible en <http://almacendederecho.org/la-sentencia-google-del-tribunal-supremo-derecho-de-grupos-y-levantamiento-del-velo/> [Consultado el 30/12/2017].

[85] BLUME, P., «The myths pertaining to the proposed General Data Protection Regulation», *International Data Privacy Law*, vol. 4, núm. 4, 2014, p. 273.

BRKAN, M., «Data protection and European Private International Law», *EUI Working Paper RSCAS 2015/40,* Florence School of Regulation, Robert Schuman Centre for Advanced Studies, European University Institute, 2015, pp. 1-37.

BLUME, P., «Data Protection and Conflict-of-laws: A Challenging Relationship», *European Data Protection Law Review*, 2016, pp. 324-341.

BLUME, P., «The myths pertaining to the proposed General Data Protection Regulation», *International Data Privacy Law*, vol. 4, núm. 4, 2014, p. 273.

BYGRAVE, L.A., «Privacy and Data Protection in an International Perspective», *Stockholm Institute for Scandinavian Law*, 2010, pp. 166-198, Disponible en <http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf> [Consultado el 12/07/2017].

DE MIGUEL ASENSIO, P.A., «Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea», *Revista Española de Derecho Internacional*, vol. 69, núm. 1, enero-junio 2017. Disponible en: <http://eprints.ucm.es/41156/> [Consultado el 02/06/2017].

DE MIGUEL ASENSIO, P.A., «Aspectos internacionales del Reglamento general de protección de datos de la UE (II): Derecho aplicable», entrada de blog de 19 de mayo 2016. Disponible en <http://pedrodemiguelasensio.blogspot.nl/2016/05/aspectos-internacionales-del-reglamento_19.html> [Consultado el 31/10/2016].

DE MIGUEL ASENSIO, P.A., «Aspectos internacionales del Reglamento general de protección de datos de la UE (I): cuestiones de competencia», entrada de blog de 11 de marzo de 2016. Disponible en <http://pedrodemiguelasensio.blogspot.com.es/2016/05/aspectos-internacionales-del-reglamento.html> [Consultado el 31/10/2016].

DE MIGUEL ASENSIO, P.A., *Derecho Privado de Internet*, 5ª ed., Navarra, (Thomson Reuters), 2015.

DE MIGUEL ASENSIO, P.A., «La cuestionable revisión de las normas de competencia judicial internacional (LO 7/2015 de reforma de la LOPJ», entrada de blog de 23 julio 2015. Disponible en: <http://pedrodemiguelasensio.blogspot.com.es/2015/07/la-cuestionable-revision-de-las-normas.html> [Consultado el 22/10/2016].

DE MIGUEL ASENSIO, P.A., «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», *Revista de la Facultad de Derecho de la Universidad de Granada*, 3ª. época, núm. 7, 2004, pp. 397-417.

GABEL, D., y HICKMAN, T., «Unlocking the EU Data Protection Regulation.», 22 de julio de 2006, Disponible en: <http://www.whitecase.com/publications/

article/chapter-6-data-protection-principles-unlocking-eu-general-dataprotection> [Consultado el 25/10/2016].

GARCÍA MEXÍA, P., *Derecho Europeo de Internet,* 1ª ed., La Coruña (Netbiblio), 2009.

GARCIMARTÍN ALFÉREZ, F.J., «La competencia judicial internacional en la reforma de la LOPJ», *Diario la Ley*, Nº8614, 28 septiembre de 2015, Ed. La Ley.

GDPR PORTAL, «Frequently Asked Questions about the incoming GDPR». Disponible en: <https://www.eugdpr.org/gdpr-faqs.html> [Consultado el 17/12/2017].

GDPR PORTAL, «An overview of the main changes under GPDR and how they differ from the previous directive». Disponible en <https://www.eugdpr.org/key-changes.html> [Consultado el 17/12/2017].

GIL ANTÓN, A.M., «El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales», *Revista de Derecho UNED*, núm. 10, 2012.

GRUPO DEL ARTÍCULO 29: «Dictamen 8/2010 sobre el Derecho aplicable», 2010, pp. 1-39. Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf> [Consultado el 09/11/2016].

GRUPO DEL ARTÍCULO 29: «Dictamen 4/2007 sobre el concepto de datos personales», 2007, pp. 1-29. Disponible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf> [Consultado el 19/07/2016].

HUSTINX, P., «EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation». Disponible en <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf> [Consultado el 15/09/2016].

KOKOTT, J., y SOBOTTA, C., "The distinction between privacy and data protection in the jurisprudence of CJEU and ECtHR", *International Data Privacy Law*, vol. 3, núm. 4, 2013, pp. 222-228.

KOTSCHY, W., «The proposal for a new General Data Protection Regulation – problems solved?», *International Data Privacy Law*, vol. 4, núm. 4, 2014.

MINERO ALEJANDRE, G., «Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea», *Anuario Jurídico y Económico Escurialense,* L, 2017, pp. 13-58. Disponible en <https://dialnet.unirioja.es/servlet/articulo?codigo=5876163> [Consultado el 15/12/2017].

MURILLO DE LA CUEVA, P.L., «Novedades sobre el derecho a la protección de datos personales», *El derecho a la protección de datos: novedades y problemas*, Aranjuez (Ed. Fundación Ciudadanía y Valores), 2010.

ORDOÑEZ SOLÍS, D., «La protección judicial de los derechos en Internet», *Real Academia Asturiana de la Jurisprudencia*, 12 de marzo de 2014. Disponible en: <https://kontencioso.files.wordpress.com/2014/03/proteccic3b3n-judicial-raaj.pdf> [Consultado el 23/08/2017].

PERALES, A., «La vigencia del consentimiento en el futuro de la protección de datos personales», *Monográfico de la ASOCIACIÓN PROFESIONAL ESPAÑOLA DE LA PRIVACIDAD por el Día Europeo del Derecho a la Protección de datos,* 2016. Disponible en: <http://www.apep.es/aepd-el-futuro-de-la-proteccion-de-datos/> [Consultado el 22/09/2017].

PIÑAR MAÑAS, J.L., «Seguridad, transparencia y protección de datos», 2009, pp. 1-72. Disponible en <http://www.cepc.gob.es/docs/ley-de-transparencia/ponencia-j-luis-pi%C3%B1ar.pdf?sfvrsn=0> [Consultado el 15/07/2016].

REDING, V., «The European data protection framework for the twenty-first century», *International Data Privacy Law*, vol. 2, núm. 3, 2012, p. 121. Disponible en: <http://idpl.oxfordjournals.org/content/2/3/119.full.pdf+html> [Consultado el 6/9/2017].

SANCHO VILLA, D., «Protección de datos personales y transferencia internacional: cuestiones de ley aplicable», *Revista jurídica de Castilla y León*, núm. 16, septiembre 2008, pp. 401-445.

SVANTESSON, D., *Extraterritoriality in Data Privacy Law*, 1ª ed., Copenhague (Ex Tuto), 2013.

WALTER-ECHOLS, M., «Panopticon – Surveillance and Privacy in the Internet Age», *Worcester Polytechnic Institute*, 2009. Disponible en: <https://www.wpi.edu/Pubs/E-project/Available/E-project022709-132355/unrestricted/Panopticon.pdf> [Consultado el 25/06/2016].

IX. JURISPRUDENCIA CITADA

STJUE 9 de noviembre de 2000, asunto C-381/98, *Ingmar GB Ltd contra Eaton Leonard Technologies Inc.* (ECLI:EU:C:2000:605).

STJUE 6 de noviembre de 2003, asunto C-101/01, *Bodil Lindqvist* (ECLI:EU:C:2003:596).

STJUE 9 de marzo de 2010, asunto C-518/07, *Comisión Europea/Alemania* (ECLI:EU:C:2010:125).

STJUE 9 de noviembre 2010, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Scheche GbR (C-92/09) y Hartmut Eifert (C-93/09) contra Land Hessen* (ECLI:EU:C:2010:662).

STJUE 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd (asunto C-293/12) contra Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commisioner of the Garda Síochána, Irlanda, The Attorney General, y Kärntner Landesregierung (asunto C-594/12) contra Michael Seitlinger, Christof Tschohl y otros* (ECLI:EU:C:2014:238).

STJUE 13 de mayo de 2014, asunto C-131/12, *Google Spain SL y Google Inc. Contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (ECLI:EU:C:2014:317).

STJUE 11 de diciembre de 2014, asunto C-212/13, *František Ryneš contra* Úřad *pro ochranu osobních* údajů (ECLI:EU:C:2014:2428).

STJUE 1 de octubre de 2015, asunto C-230/14, *Weltimmo s.r.o contra Nemzeti Adatvédelmi* és *Információszabadság Hatóság* (ECLI:EU:C:2015:639).

STJUE 6 octubre 2015, asunto C-362/14, *Maximillian Schrems contra Data Protection Commisioner* (ECLI:EU:C:2015:650).

STJUE 28 de julio de 2016, asunto C-612/16, *Verein für Konsumenteninformation contra Amazon EU Sàrl* (ECLI:EU:C:2016:612).