

Máster en Abogacía por la Universidad de León

Facultad de Derecho

Universidad de León

Curso 2018 / 2019



**ANÁLISIS JURÍDICO DEL SISTEMA  
EUROPEO DE PROTECCIÓN DE DATOS Y SU  
INCIDENCIA EN LAS TRANSFERENCIAS  
INTERNACIONALES DE CARÁCTER PERSONAL  
E ILÍCITAS**

*Legal analysis of the European Data Protection system and its  
impact on personal and illicit international transfers*

Realizado por el alumno D. Luis Soto Viñas

Tutorizado por el Prof. Dr. D. Don David Carrizo Aguado

# ÍNDICE

<b>ABREVIATURAS</b> .....	4
<b>RESUMEN</b> .....	6
<b>OBJETO</b> .....	8
<b>METODOLOGÍA</b> .....	9
<b>CAPÍTULO I. COMPETENCIA Y DERECHO APLICABLE EN EL REGLAMENTO GENERAL SOBRE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA</b> .....	11
I. Determinación del régimen jurídico y delimitación de la competencia.....	11
1. Instrumentos normativos aplicables.....	11
2. Función de las normas de ámbito territorial.....	15
3. Establecimiento del responsable o encargado del tratamiento.....	18
4. Responsables o encargados no establecidos en la Unión.....	21
II. Tutela judicial civil contra un encargado o responsable.....	24
1. Acciones civiles.....	24
2. Regla especial de competencia: alcance.....	26
3. Foro del establecimiento.....	28
4. Residencia habitual del interesado.....	30
5. Interacción con las reglas de competencia del Reglamento Bruselas I <i>bis</i> .....	31
<b>CAPÍTULO II. TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL</b> .....	35
I. Concepto.....	35
II. Sujetos.....	38
III. Sistema de competencia judicial internacional.....	40
1. Regímenes normativos.....	40
2. Acciones ejercitables por la víctima.....	42
3. Elección del tribunal competente.....	43
4. Foro del domicilio del demandado.....	44
5. Foro del lugar del daño.....	46
IV. Legislación aplicable en el marco de una transferencia internacional ilícita de datos .....	48
1. El Reglamento Roma II.....	48
2. El artículo 10.9 del Código Civil.....	50

<b>CONCLUSIONES</b> .....	53
<b>BIBLIOGRAFÍA</b> .....	56
<b>ENLACES <i>WEB</i></b> .....	61
<b>TEXTOS LEGALES</b> .....	63
<b>ANEXO JURISPRUDENCIAL</b> .....	64
I. Jurisprudencia internacional .....	64
II. Jurisprudencia nacional .....	65



## ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
Art.	Artículo
BOE	Boletín Oficial del Estado
CC	Código Civil
CE	Comunidad Europea
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CL	Convenio de Lugano
Codo.	Considerando
Coord.	Coordinador
Dir.	Director
DOUE	Diario Oficial de la Unión Europea
Ed.	Editor
EE. UU	Estados Unidos
<i>EU</i>	<i>European Union</i>
EFTA	<i>European Free Trade Association</i>
GDPR	<i>General Data Protection Regulation</i>
GPD	Grupo de Protección de Datos
<i>Inc.</i>	<i>Incorporation</i>
LOPD	Ley Orgánica de Protección de Datos
LOPJ	Ley Orgánica del Poder Judicial
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
Núm.	Número
OCDE	Organización para la Cooperación y Desarrollo Económico
Pág.	Página
RBI <i>bis</i>	Reglamento Bruselas I <i>bis</i>
RGPD	Reglamento General de Protección de Datos
S. A	Sociedad Anónima
S. L	Sociedad Limitada

SSTS	Sentencias Tribunal Supremo
STC	Sentencia Tribunal Constitucional
STEDH	Sentencia Tribunal Europeo Derechos Humanos
STJCE	Sentencia Tribunal de Justicia de la Comunidad Europea
TC	Tribunal Constitucional
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea
<i>UK</i>	<i>United Kingdom</i>
<i>Vid.</i>	Véase

## RESUMEN

La entrada en vigor del nuevo Reglamento General de Protección de Datos refleja un nuevo panorama cuyo fin es consolidar un tratamiento armónico y homogéneo del derecho fundamental a la protección de datos personales en el ámbito europeo. En lo que respecta a su proyección internacional, incorpora modificaciones en los criterios que delimitan el ámbito territorial de la normativa europea, más concretamente, en el propósito de garantizar su aplicación al procesamiento de información de personas ubicadas en la UE asociados a comportamientos dirigidas a su territorio.

La presente investigación analiza la opción que integra el Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 de litigar en el propio domicilio del demandado en concordancia con la esencia protectora de esta norma. Por añadidura, la interacción con el Reglamento Bruselas I *bis* deriva en una extensión de los foros disponibles y en mejores líneas de defensa para el demandado, líneas que pueden ser ampliadas en función de lo acordado en el contrato. Por otra parte, en materia de ley aplicable, es indiscutible la ausencia de novedades que nos condicionan a mantener los criterios autónomos tradicionales.

El siguiente punto de reflexión lo debemos dedicar a las resoluciones judiciales en materia de salvaguarda de derechos de la persona y en particular de protección de datos, pues la interpretación jurisprudencial procedente del Tribunal de Justicia de la Unión Europea y del Tribunal de Derechos Humanos de Estrasburgo constituyen una garantía adicional sumada al trabajo que desarrollan los tribunales nacionales.

Como resultado, la protección de datos ha planteado diversas barreras en materia de competencia judicial y determinación de ley aplicable, sin embargo, mediante el nuevo Reglamento se persigue constituir un régimen de Derecho Internacional Privado adaptado a un entorno virtual interconectado que no podemos obviar, por lo que se hace necesario como ya hemos venido apuntando, una intervención legislativa de carácter supranacional.

**PALABRAS CLAVE:** RGPD, protección de datos, privacidad, intimidad, derecho fundamental, dato personal, encargado, responsable, transferencia internacional, usuario.

## **ABSTRACT**

The entry into force of the new General Regulation on Data Protection. As far as its international projection is concerned, the terms that define the territorial scope of European regulations are incorporated, more specifically, in the purpose of their application, the processing of information of people located in the EU territory

The present investigation analyzes the option that integrates the Regulation of litigation in the own domicile of the defendant in the concordance with the protective essence of this norm. Therefore, the interaction with the Regulation of Brussels generates an extension of the available forums and in the best lines of defense for the defendant, lines that can be extended in the function of what was agreed in the contract. On the other hand, in the matter of applicable law, the absence of novelties that allow us to maintain the traditional autonomous criteria is indisputable.

The next point of reflection, we must devote to judicial decisions on the protection of the rights of the individual and in particular of the protection of data, for the jurisprudential interpretation of the Court of Justice of the European Union and the Court of Human Rights of Strasbourg An additional guarantee.

As a result, the protection of data has raised barriers in the area of jurisdiction and determination of the applicable law, however, through the new Regulation. What is necessary as we have already pointed out, a supranational legislative intervention.

**KEYWORDS:** privacy, responsible, personal data, user, fundamental right, international transfer, responsible for data protection.

## **OBJETO**

El objeto de estudio de este trabajo es el análisis del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, haciendo especial mención a la determinación de la competencia judicial y a la ley aplicable como punto de partida para conocer el alcance del derecho a la protección de datos y el marco jurídico europeo en el que se integra el tratamiento transfronterizo de información.

Dentro de esta perspectiva, y tomando como referencia las libertades de un mercado único deslocalizado, procedemos a estudiar la evolución de las disposiciones normativas supranacionales relativas a la protección de personas físicas con el objetivo de crear un marco uniforme en un entorno de seguridad jurídica. En esta línea, abordamos el ámbito de aplicación del Reglamento en base a las actividades de un establecimiento del responsable o encargado del tratamiento. A continuación, nos centramos en el sistema de tutela civil que permitirá al individuo recibir una indemnización en concepto de reparación por haber sido víctima de una infracción del Reglamento.

Al hilo de lo expuesto en los párrafos anteriores, la segunda parte de este trabajo se focaliza en las transferencias internacionales de datos de carácter personal e ilícito. Así las cosas, trataremos de analizar la competencia judicial internacional ante una infracción extracontractual en base al Reglamento Bruselas I *bis* como sistema base europeo y a la Ley Orgánica del Poder Judicial como fuente interna de aplicación subsidiaria.

Finalmente, ante la ausencia de una normativa jurídica y convencional europea, acudiremos a nuestro Código Civil como norma de conflicto bilateral de Derecho Internacional Privado autónomo ante las eventuales conculcaciones de los derechos de la personalidad en el ámbito de aplicación material del Reglamento Roma II.

## **METODOLOGÍA**

La metodología de investigación utilizada para la realización de este trabajo podemos estructurarla de la siguiente manera:

En primer lugar, hemos realizado la elección de este tema entre la inmensidad de campos que ofrece el Derecho Internacional Privado. Centrándonos en el Reglamento General de Protección de Datos y en las transferencias internacionales de datos de carácter personal ilícitas, desde la óptica de la competencia judicial internacional y de la determinación del régimen jurídico aplicable.

En cuanto a la elección del tema objeto de análisis, consideramos que es una pieza fundamental en el Derecho Internacional Privado, ya que la tecnología ha modificado la atmósfera económico-social internacional y, en este sentido, se debe garantizar la libre transmisión de datos personales dentro de la Unión, así como en las relaciones con terceros Estados y organizaciones internacionales, protegiendo los derechos fundamentales, y en particular, el derecho a la intimidad.

En segundo lugar, hemos enfocado la temática desde una triple dimensión:

Normativa: Hemos estudiado las normas jurídicas que regulan el derecho a la protección de datos.

Fáctica: El análisis realizado se ha centrado en un ámbito geográfico determinado.

Valorativa: Hemos realizado una interpretación del ordenamiento jurídico tomando como referencia los valores que rigen actualmente en nuestra sociedad.

En tercer lugar, procedimos a elaborar un índice que hemos seguido a lo largo de todo el trabajo, reflejando mediante capítulos desarrollados por apartados, las líneas más relevantes en la materia.

Dentro de este marco, hemos partido de los siguientes métodos que nos han permitido respaldar nuestra investigación:

- Observación de la realidad.
- Aplicación sistemática de normas jurídicas tanto nacionales como comunitarias.
- Valoración de los intereses en juego: En el marco de las transferencias internacionales de información personal profundizamos en el derecho a la protección de datos sin omitir la importancia de otros derechos que debemos ponderar como la libertad de expresión, información e intimidad.

Al hilo de lo expuesto en los párrafos anteriores, localizamos las fuentes que más

se ajustaban a la elección del tema, abarcando no solamente monografías, capítulos de texto de manuales, artículos de revista, etc. sino que también fue necesario acudir a la jurisprudencia española y europea. A continuación, una vez elaborado el índice y localizadas las fuentes, comenzamos a redactar los aspectos más relevantes indicados, acudiendo con frecuencia al Área de Derecho Internacional Privado para supervisar y controlar cuanto aquello íbamos haciendo.

# CAPÍTULO I. COMPETENCIA Y DERECHO APLICABLE EN EL REGLAMENTO GENERAL SOBRE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

## I. Determinación del régimen jurídico y delimitación de la competencia

### 1. Instrumentos normativos aplicables

En primer lugar, debemos poner de relieve la amplitud de elementos normativos que constituyen el abanico legislativo en el ámbito de la protección de datos. En este sentido y, partiendo así del carácter global de Internet, la actuación de la legislación supranacional va a ser indispensable. *Internet está planteando nuevos desafíos para los derechos fundamentales hasta el punto de que precisamente la informática ha propiciado el desarrollo extraordinario de un derecho fundamental consagrado recientemente por la Carta de Derechos Fundamentales de la Unión Europea<sup>1</sup>: el derecho a la protección de los datos personales<sup>2</sup>. Conviene subrayar, por lo tanto, que el derecho aplicable<sup>3</sup> en España<sup>4</sup> será el procedente de la UE, tanto en su vertiente normativa<sup>5</sup> como*

---

<sup>1</sup> La Carta de los derechos fundamentales nace en cumplimiento del mandato de la cumbre de Colonia de junio de 1999. En dicha cumbre se acordó, en primer lugar, que en el presente estado de la Unión Europea, los derechos fundamentales aplicables en el nivel comunitario deberían consolidarse en una Carta para hacerse más evidentes (núm. 44). Además, en segundo lugar, se acordó que el citado documento debiera recoger los derechos de los ciudadanos europeos. RUIZ MIGUEL, C.: “El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea”, HERRERO DE LA FUENTE, A. A. (Coord.), *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar*, Fundación Rei Afonso Henriques, Zamora, 2003, p. 173.

<sup>2</sup> ORDÓÑEZ SOLÍS, D.: “El derecho al olvido en Internet y la sentencia Google Spain”, *Revista Aranzadi Unión Europea*, núm. 6, 2014, pág. 32.

<sup>3</sup> El Senado ha aprobado la nueva Ley Orgánica de Protección de Datos (LOPD) y de Garantía de los Derechos Digitales que adapta la normativa nacional al Reglamento General de Protección de Datos (RGPD) europeo, que empezó a aplicarse el pasado 25 de mayo. El proyecto de ley ha quedado definitivamente aprobado con 220 votos a favor y 21 en contra y ya sólo está pendiente de su publicación en el Boletín Oficial del Estado para su consiguiente entrada en vigor (fecha de consulta: 23-11-2018) <http://www.expansion.com/juridico/actualidad/tendencias/2018/11/21/5bf5b42a22601d333f8b45d1.html>.

<sup>4</sup> AEPD “Principales derechos”, (fecha de consulta 20-10-2018) <https://www.aepd.es/reglamento/derechos/index.html>

<sup>5</sup> El Consejo de Ministros ha aprobado un Real Decreto Ley con medidas urgentes para adaptar el Derecho español al Reglamento General de Protección de Datos. El Real Decreto Ley 5/2018 fue publicado en el BOE de 30 de julio y entró en vigor al día siguiente de su publicación. El Real Decreto Ley tiene por objeto establecer la regulación de determinadas materias en el ámbito de la protección de datos que no están reservadas a la ley orgánica. En concreto, regula la inspección y el régimen sancionador en materia de protección de datos y los procedimientos en caso de una posible vulneración del Reglamento (UE) 2016/679 por el que se deroga la Directiva 95/46/CE (fecha de consulta: 6-11-2018) <http://elconsultor.laley.es/content/Documento.aspx?params=H4slIAAAAAAEAMtMSbH1czUwMDA0Mzc3sjBQK0stKs7Mz7M1MjC0MDA3BgtkplW65CeHVBAk2qY15hSnqiUmFefnlJakhhZl2oYUlaYCAHSi1jZGAAAWKE>

jurisprudencial<sup>6</sup> que, junto con nuestra regulación interna<sup>7</sup> (siendo una pieza clave el art. 18 de la Constitución<sup>8</sup>), quedarán establecidos los derechos fundamentales como el honor<sup>9</sup> e intimidad<sup>10</sup> que ostenta el individuo como garantía<sup>11</sup> frente a la informática.

En lo que respecta al marco normativo europeo, *la mayor parte de los ordenamientos jurídicos de nuestro entorno otorgan a la protección de datos personales*

---

<sup>6</sup> STJUE de 9 de noviembre de 2010, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke y Hartmut Eifert* (ECLI:EU:C:2010:662). Estas sentencias han marcado una referencia en lo que concierne a la interpretación del derecho a la protección de datos personales en relación con el principio de transparencia de las instituciones europeas en el procedimiento administrativo y de las autoridades nacionales en la gestión de los fondos europeos. En ambos asuntos, el TJUE obliga a justificar la publicación o denegación de datos. Tomando como referencia este pronunciamiento *vid.* PICOD, F.: “Invalidité partielle de règlements agricoles pour incompatibilité avec la Charte des droits fondamentaux”, *La Semaine Juridique - édition générale*, núm. 50, 2010, p. 2344; OLIVER, P.: “Case C-279/09, DEB vs Germany, Judgment of the Court of Justice (Second Chamber) of 22 December 2010”, *Common Market Law Review 2011*, núm. 6, 2011, pp. 2023-2040; KRISTOFERITSCH, H.: “Transparency: Let There Be Light? Comments on the Judgment of the European Court of Justice, Joined Cases C-92/09 and C-93/09”, *European State Aid Law Quarterly 2011*, núm. 4, 2011, pp. 687-695.

<sup>7</sup> VILLAVERDE MENÉNDEZ, I.: “Protección de Datos Personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993”, *Revista Española de Derecho Constitucional*, núm. 41, 1994, p. 197.

<sup>8</sup> Art. 18 CE. 1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.* 2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.* 3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.* 4. *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.* BOE núm. 311, 29-XII-1978.

<sup>9</sup> *El derecho al honor, el derecho a la intimidad y el derecho a la propia imagen son parte del conjunto de los llamados derechos de la personalidad, reconocidos por el art. 18 de la Constitución Española, con eficacia general o erga omnes, que pertenecen a la persona por el mero hecho de serlo.* MINERO ALEJANDRE, G.: “Redes Sociales y derecho al honor, a la intimidad y a la propia imagen de personas fallecidas”, BUENO DE MATA, F. (Coord.), *Fodertics 6.0: los nuevos retos del derecho ante la era digital*, Comares, Granada, 2017, p. 43.

<sup>10</sup> STJUE de 5 de mayo de 2011, asunto C-543/09, *Deutsche Telekom AG* (ECLI:EU:C:2011:279). En esta sentencia se alude a la necesidad de ponderación del derecho a la protección de datos personales y los derechos de autor en la esfera de las empresas de telecomunicaciones. Sobre esta sentencia *vid.* IDOT, L.: “Fourniture de renseignements pour la constitution d'annuaires”, *Europe 2011 Juillet*, núm. 7, 2011, pp. 35-36.

<sup>11</sup> STC 254/93 de 20 de julio (ECLI:ES:TC:1993:254). El Tribunal Constitucional declaró que: *nuestra CE ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama “la informática”.*

la naturaleza de derecho y, en nuestro sistema jurídico<sup>12</sup>, el Tribunal Constitucional le ha reconocido rango de derecho fundamental, autónomo del derecho a la intimidad<sup>13</sup>, a partir de la expresa referencia contenida en el artículo 18.4 de la Constitución<sup>14</sup>. Aunque inicialmente el Tribunal Constitucional calificaba este derecho como una especificación del derecho a la intimidad<sup>15</sup>, pronto le otorgó la naturaleza de un derecho fundamental autónomo<sup>16</sup>. Debemos aludir a los instrumentos legales más importantes: en un primer término, debemos mencionar el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal<sup>17</sup> (en vigor desde el 1 de octubre de 1985). En segundo lugar, si bien es cierto que la Directiva de 1995<sup>18</sup> relativa al tratamiento de datos personales y su libre circulación jugaba un papel esencial, no podemos obviar la Directiva 96/66/CE (disposición derogada destinada a la protección de la intimidad en el área de las telecomunicaciones), que

---

<sup>12</sup> Se tardó mucho en desarrollar el art. 18.4 de la Constitución, publicándose la LORTAD cuando ya estaba escrita la Propuesta de Directiva y se adelantó a la misma, porque había transcurrido mucho tiempo desde el año 1978, pero también porque existía cierta litigiosidad en el Tribunal Constitucional sobre lo que más tarde se configuraría como Derecho de Acceso. NÚÑEZ LÓPEZ, M./ FERREIRO BROZ, M. M.: “Una aproximación para empresas a la Ley Orgánica de Protección de Datos”, *Derecom*, núm. 15, 2013, p. 95.

<sup>13</sup> LUCENA CID, I.V.: “La protección de la intimidad en la era tecnológica: hacia una reconceptualización”, *Revista internacional de pensamiento político*, núm. 7, 2012, versión online.

<sup>14</sup> Muestras encontramos en la jurisprudencia ordinaria de la distinción de estos derechos, entendiéndose que es el TC el que ha fijado la independencia de los derechos contemplados en el art. 18 CE, a la intimidad y a la protección de datos. RUIZ CASTILLO, M. M.: “Intimidad, protección de datos y libertad sindical: STC 11/1998, de 13 de enero”, GARCIA MURCIA, J. (Coord.), *Libertad sindical y otros derechos de acción colectiva de trabajadores y empresarios*, Aranzadi, Cizur Menor, 2015, p. 293.

<sup>15</sup> A diferencia de lo ocurrido en Estados Unidos, en España, y en el resto de las Constituciones europeas, el reconocimiento del derecho a la intimidad está plasmado en textos normativos, aunque bien es cierto que no todos los casos hay una expresa mención constitucional. VILLARINO MARZO, J.: *La privacidad en el entorno del cloud computing*, tesis doctoral dirigida por Pablo García Mexía, Universitat Abat Oliba CEU 2017, p. 34.

<sup>16</sup> LUCAS MURILLO DE LA CUEVA, P.: “La primera jurisprudencia sobre el derecho a la autodeterminación informativa”, *La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 1, 2003, p. 48.

<sup>17</sup> STEDH 25 de septiembre de 2001, P.G. y J.H. contra Reino Unido (ECLI:CE:ECHR:2001:0925JUD004478798). En el ámbito del procesamiento automatizado de información, el TEDH ha afirmado que el registro sistemático de datos puede vulnerar el derecho al respeto a la vida privada, aunque el origen sea una fuente pública.

<sup>18</sup> La consecuencia directa que trae este nuevo Reglamento 2016/679 es la derogación de la Directiva 95/46/CE Del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. ORTEGA GIMÉNEZ, A./ DOMENECH, J.J.: “Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea”, *Revista de la Facultad de Derecho*, núm. 44, 2018, p. 4.

posteriormente sería remplazada por la Directiva 2002/58 sobre la privacidad<sup>19</sup> y las comunicaciones electrónicas y la Directiva 2000/31 relativa a comercio electrónico<sup>20</sup>.

Por otra parte, y sin dejar al margen las directivas, debemos tener presente la normativa integrada en los Tratados constitutivos de la Unión Europea del 2000. Asimismo, debemos subrayar el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016<sup>21</sup> relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, en el cual la Comisión fija como objetivo la concreción de un marco uniforme<sup>22</sup> y sólido en el ámbito de la Protección de datos en la UE con el propósito reforzar la seguridad jurídica para que cualquier ciudadano pueda ejercer un control sobre sus datos, adaptándose a las exigencias que se derivan de Internet. Hay que mencionar, además, el derecho al olvido<sup>23</sup> como resultado de la aprobación de este Reglamento, así como otras disposiciones relativas a la exigencia de un consentimiento claro<sup>24</sup> del usuario para hacer un tratamiento

---

<sup>19</sup> REAL ACADEMIA ESPAÑOLA: *Diccionario panhispánico de dudas*, Santillana, Madrid, 2005, p. 524. Afirma que el término privacidad: *No es sinónimo de intimidad ("ámbito íntimo, espiritual o físico de una persona"; intimidad), aunque ambos términos están semánticamente muy próximos y son intercambiables en algunos contextos: derecho a la intimidad, derecho a la privacidad.*

<sup>20</sup> *The OCDE's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data are the cornerstone of OCDE work on information security and privacy* (fecha de consulta: 1-11-2018) <http://www.oecd.org/Internet/ieconomy/privacy-guidelines.htm>.

<sup>21</sup> *Puede afirmarse que el vigente RGPD supone un destacado hito jurídico, en tanto el Derecho de la UE se dota de un régimen común y vinculante, que pretende reforzar la tutela de este derecho, y a dicho fin, asegurar un adecuado tratamiento de los datos personales con base a la configuración de una normativa uniforme y de obligado cumplimiento.* DOPAZO FRAGUÍO, P.: “Novedades del Reglamento General de Protección de Datos”, *Revista Española de Derecho Europeo*, núm. 68, 2018, versión online.

<sup>22</sup> En este escenario, donde la Comisión subraya la necesidad de un marco jurídico uniforme donde debemos poner de relieve el art. 291, apartado 1, del Tratado de Funcionamiento de la Unión Europea, cuando señala que los Estados miembros *adoptarán todas las medidas de Derecho interno necesarias para la ejecución de los actos jurídicamente vinculantes de la Unión.*

<sup>23</sup> *Es la manifestación del derecho de supresión aplicado a los buscadores de Internet. El derecho de supresión (derecho al olvido) hace referencia al derecho a impedir la difusión de información personal a través de Internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información)* (fecha de consulta: 7-10-2018) <https://www.aepd.es/areas/Internet/derecho-al-olvido.html>.

<sup>24</sup> *Con carácter específico, el art. 7 LOPD (BOE núm. 298, 14-XII-1999). Establece para los datos de carácter personal relacionados con las creencias, ideología o religión, la necesidad de que el titular de los mismos otorgue su consentimiento expreso y por escrito para que puedan ser tratados y para los datos que hagan referencia al origen racial, a la salud y a la vida sexual la necesidad de que se otorgue un consentimiento expreso.* GUILLÉN CATALÁN, R.: “El interés legítimo: pieza clave en la excepción del consentimiento en el tratamiento de datos personales. Comentario a la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 8 de febrero de 2012”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 29, 2012, p. 435.

de sus datos<sup>25</sup> y el derecho a trasladar datos entre proveedores de servicios. *El poder de disposición que un individuo tiene sobre sus datos personales se manifiesta de modo principal en su capacidad para consentir o rechazar<sup>26</sup> un tratamiento de los mismos, decisión que sólo es posible si se le informa previamente de los caracteres definitorios de aquel, sin embargo, puede ser limitado por ley<sup>27</sup>.*

## 2. Función de las normas de ámbito territorial

Cabe decir que tanto el art. 4 de la Directiva 95/46/CE<sup>28</sup> referido al “Derecho nacional aplicable”, como el art. 3 del RGPD<sup>29</sup> titulado “Ámbito territorial” derivan en un planteamiento semejante, de tal modo que ambas confluyen en su función esencial de delimitar el ámbito espacial de la normativa europea de protección de datos. En esta línea, los encargados del tratamiento (aunque sean procedentes de terceros Estados) deben ajustarse a las exigencias marcadas, quedando supeditadas al examen jurídico-público de las autoridades de control<sup>30</sup> y afrontando un único derecho paneuropeo de protección de datos y no a veintiocho.

---

<sup>25</sup> *El consentimiento es la llave de todo tratamiento de datos personales. Salvo las excepciones legalmente previstas, el consentimiento da acceso al tratamiento de nuestros datos personales, lo legitima, y permite hablar de un mayor o menor control de los mismos.* ARENAS RAMIRO, M.: *Reforzando el ejercicio del derecho a la protección de datos personales, hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015, p. 329.

<sup>26</sup> *La obligación de información aparece estrechamente unida al aspecto clave del consentimiento del afectado, no sólo porque el consentimiento ha de ser informado, sino también porque en ocasiones la mera información, unida a la posibilidad de que el usuario manifieste su negativa, puede ser determinante de que concurra el consentimiento (cuando no haya manifestado el usuario su voluntad en contra).* DE MIGUEL ASENSIO, P. A.: *Principio de protección de datos, Derecho Privado de Internet*, Aranzadi, Cizur Menor, 2011, p. 260.

<sup>27</sup> HERNÁNDEZ CORCHETE, J.A.: “Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos”, PIÑAR MAÑAS J.L. (Coord.), *Reglamento General de Protección de Datos*, Reus, Madrid, 2016, p. 214.

<sup>28</sup> Art. 4.1 b) *Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público (disposición derogada).* DOUE L 281/31, 23-XI-1995.

<sup>29</sup> Art. 3.1 RGPD. *El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.* DOUE L 119/1, 4-V-2016.

<sup>30</sup> *Debe subrayarse el papel normativo del que dispone en nuestro sistema la Agencia Española de Protección de Datos al atribuirle el artículo 37 c) LOPD competencia para dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la ley.* MARTÍNEZ MARTÍNEZ, R.: “El derecho fundamental a la protección de datos: perspectivas”, *Revista de Internet, Derecho y Política Universitat Oberta Catalunya*, núm. 5, 2007, p. 61.

La legislación nacional aplicable de la Directiva 95/46/CE fijaba el Estado o Estados miembros<sup>31</sup> concretando qué autoridades de control tenían competencia para la supervisión, donde se partía de una correlación ley aplicable-autoridad competente propia del derecho administrativo. En esta línea, debemos tener en consideración el asunto *Weltimmo*<sup>32</sup>, donde se alude a la interpretación del art. 28.6 de la Directiva 95/46/CE. Sin embargo, el art. 3 RGPD<sup>33</sup> no comparte esta función, sino que unifica la legislación para la totalidad de la UE. Aun así, debemos poner de relieve la existencia de determinadas legislaciones no unificadas<sup>34</sup> en su totalidad, es el caso de las condiciones aplicables al consentimiento del niño<sup>35</sup> en relación con los servicios de la sociedad de la información recogidas en el apartado primero del artículo 8 RGPD<sup>36</sup>.

---

<sup>31</sup> STJUE de 29 de enero de 2008, asunto C-275/06, *Promusicae* (ECLI:EU:C:2008:54). Esta resolución fue dictada para responder a un reenvío prejudicial de un juez mercantil español. El TJUE *autoriza también a los Estados miembros a adoptar medidas que limiten la obligación de confidencialidad de los datos personales, cuando tal limitación constituya una medida necesaria para la salvaguardia de la protección de los derechos y libertades de otras personas* (apartado 53). Para mayor abundamiento *vid.* BOTANA AGRA, M.: “Infracción de derechos de autor y protección de datos personales en redes P2P (Comentario a la sentencia del Tribunal de Justicia de las Comunidades Europeas (Gran Sala), de 29 de enero de 2008, asunto C-275/06)”, *Actas de derecho industrial y derecho de autor*, 2008, pp. 801-824.

<sup>32</sup> STJUE de 1 de octubre de 2015, asunto C-230/14, *Weltimmo* (ECLI:EU:C:2015:639). En esta sentencia se concluye que no cabe imponer sanciones en base a la legislación de un Estado miembro al responsable del tratamiento de tales datos que no está establecido en dicho territorio, toma como referencia el art. 28 apartado 6 de la Directiva 95/46/CE (actualmente derogada) y afirma que ha de intervenir la autoridad de control dependiente del Estado miembro cuyo Derecho es aplicable.

<sup>33</sup> *El nuevo artículo 3 del RGPD trata este fenómeno con la obligatoriedad de la aplicación de la legislación europea cuando los datos tratados en terceros países involucren a residentes de la Unión, además de contemplar un supuesto específico dedicado al Big Data en el artículo 3.2 b), el cual no entendemos la exclusión que realiza la doctrina en cuanto a la aplicación de este supuesto a los productos o servicios diferentes a los servicios de Internet.* DOMENECH, J.J.: “La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE”, *Revista Lex Mercatoria*, núm. 6, 2017, p. 41.

<sup>34</sup> *Dicha pretendida armonización, destinada a atajar las diferencias existentes entre las legislaciones nacionales no se ha logrado.* BRU CUADRADA, E.: “La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad”, *Revista de Internet, Derecho y Política*, núm. 5, 2007, p. 90.

<sup>35</sup> *El RGPD requiere que los responsables hagan esfuerzos razonables, teniendo en cuenta la tecnología disponible, para verificar que, para los niños menores de la edad que se fije como límite, el consentimiento sea dado o sea autorizado por los padres o tutores del menor (no es una obligación en sí, sino tan sólo de medios o procedimientos razonables para establecer la intervención real de padres o tutores)* (fecha de consulta: 2-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.

<sup>36</sup> Art. 8.1 RGPD. *Cuando se aplique el art. 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.*

La función de comprobar y supervisar la correcta aplicación del RGPD (como por ejemplo en la realización de investigaciones o en la imposición de sanciones<sup>37</sup> administrativas) es ejercida por las correspondientes autoridades de control<sup>38</sup> de los Estados miembros, es decir, no existe en la actualidad una única autoridad de control europea. No obstante, cuando surgen actuaciones asociadas a una pluralidad de Estados sigue siendo esencial la designación de los Estados miembros cuyas autoridades de control<sup>39</sup> son competentes. Al mismo tiempo, sus criterios relativos al ámbito territorial de aplicación no van a ser definitivos, sino que lo será la normativa concreta sobre competencia en el ámbito administrativo.

Al margen de lo expuesto anteriormente sobre los instrumentos jurídico-públicos de supervisión, debemos destacar la aplicación de la legislación en el ámbito territorial cuando nos encontramos ante un litigio de índole civil entre dos particulares. Para ilustrar mejor esto último, en el supuesto de que un ciudadano inicie un procedimiento para obtener una indemnización como consecuencia del daño sufrido por el tratamiento incorrecto de sus datos, las acciones ejercitadas por el particular solo prosperarán si el procedimiento mencionado está comprendido en su ámbito de aplicación. Sin embargo, las reglas de conflicto<sup>40</sup> aplicables a cada caso serán las que determinen lo relativo a la

---

<sup>37</sup> *El RGPD adopta como premisa la reparación integral de los daños y perjuicios causados con la operación de tratamiento, atribuyendo responsabilidad solidaria al responsable y encargado (art. 82.1), sin dejar de imponer sanciones administrativas, cuya cuantía se eleva sustancialmente, distinguiendo dos escalones: el primero, que cuantifica hasta 10 millones de euros o una cantidad equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior; y el segundo, de hasta 20 millones de euros o de un montante equivalente al 4% como máximo del volumen de negocio total del ejercicio financiero anterior (art. 83).* RODRÍGUEZ ESCANCIANO, S.: “El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679”, *Estudios financieros. Revista de trabajo y seguridad social: Comentarios, casos prácticos: recursos humanos*, núm. 423, 2018, p. 53.

<sup>38</sup> En las dos últimas décadas, España ha sido un referente en lo que respecta a la aplicación del sistema sancionador por vulneración de la normativa de protección de datos. En efecto, se ha garantizado el efectivo cumplimiento de legislación española de protección de datos mediante un riguroso régimen sancionador enfocado principalmente en el sector privado. A modo ilustrativo, la resolución sancionadora de la AEPD 2892/2013 impuso a Google Inc. una multa de 900.000 € por la unificación de sus políticas de privacidad en 2012, mientras que en el mismo supuesto, la CNIL francesa sancionó a Google el 8 de enero de 2014 con una multa de solo 150.000 €.

<sup>39</sup> *Se afirma que el tratamiento de datos que se realice cuando los tribunales actúen en ejercicio de su función judicial no ha de estar sujeto a las autoridades de control, y ello en aras de preservar la independencia del Poder Judicial (...) el control de esas operaciones de tratamiento realizadas por los tribunales lo residencia en “organismos específicos establecidos dentro del sistema judicial”.* CREMADES LÓPEZ DE TERUEL, J./ SANCHO ALONSO, J.: “Protección de datos y poder judicial”, *Diario La Ley*, núm. 9293, 2018, p. 4.

<sup>40</sup> Art. 10.9 CC. *Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven.* BOE núm. 206, 25-VII-1889. *La gestión de negocios se regulará por la ley del*

aplicación de ley cuando nos encontremos ante situaciones ajenas al tratamiento de datos personales, es el caso del art. 10.9 CC.

### 3. Establecimiento del responsable o encargado del tratamiento

El art. 3.1 ratifica que la normativa europea será de aplicación cuando el tratamiento de datos se efectuó *en el contexto de las actividades de un establecimiento del responsable<sup>41</sup> o del encargado<sup>42</sup> en la Unión, independientemente de que el tratamiento tenga o no lugar en la Unión.*

Dicho lo anterior, la interpretación del concepto “establecimiento” ha sido discutida por el TJUE<sup>43</sup>. El codo. 22 del RGPD y el codo. 19 de la Directiva se refieren a este término como *el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades ya sea una sucursal o una filial<sup>44</sup> con personalidad jurídica, no es el factor determinante al respecto.* Es decir, el TJUE lleva a cabo la interpretación en cada caso concreto a partir del tipo de prestación que la empresa en cuestión oferte en el respectivo Estado miembro. En ocasiones, cuando el representante en otro Estado miembro preste sus servicios con el suficiente nivel de estabilidad puede bastar con un solo miembro.

---

*lugar donde el gestor realice la principal actividad. En el enriquecimiento sin causa se aplicará la ley en virtud de la cual se produjo la transferencia del valor patrimonial en favor del enriquecido.*

<sup>41</sup> El nuevo Reglamento regula esta materia bajo el principio de “responsabilidad proactiva”. Según este principio, los responsables del tratamiento deben cumplir las exigencias de la normativa europea de protección de datos y, además, ser capaces de demostrarlo. FERNÁNDEZ VILLAZÓN, L.A.: “El nuevo Reglamento Europeo de Protección de Datos”, *Foro Nueva Época*, núm. 1, 2016, versión online.

<sup>42</sup> *En determinadas materias los encargados tienen obligaciones propias que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo: deben mantener un registro de actividades de tratamiento, deben determinar las medidas de seguridad aplicables a los tratamientos que realizan. deben designar a un Delegado de Protección de Datos en los casos previstos por el RGPD (fecha de consulta: 27-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.*

<sup>43</sup> STJUE de 1 de octubre de 2015, asunto C-230/14, *Weltimmo* (ECLI:EU:C:2015:639). A raíz de esta resolución se consolida el concepto flexible de “establecimiento”: *rechaza cualquier enfoque formalista según el cual una empresa estaría establecida únicamente en el lugar en que se encontrase registrada. Por lo tanto, para determinar si una sociedad, responsable de un tratamiento de datos, dispone de un establecimiento [...] procede interpretar tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades en ese otro Estado miembro tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión* (apartado 29).

<sup>44</sup> STS 574/2016 de 14 de marzo de 2016 (ES:TS:2016:964). En esta sentencia se establece que la empresa filial no va a responder cuando ninguna de sus actividades principales esté destinada al almacenamiento o tratamiento de datos ni cuando exista una unidad de negocio. Incluso tratándose de representantes de la empresa matriz, es una sociedad con personalidad jurídica diferenciada.

Por consiguiente, el art. 4.16 a) RGPD<sup>45</sup> ha delimitado además el concepto de “establecimiento principal” de un modo preciso, concretando mediante el principio de jerarquía y especialidad elementos esenciales como puede ser la determinación de un establecimiento principal de un encargado cuando disponga de una pluralidad de establecimientos en la UE. Por consiguiente, y a tenor de lo dispuesto en sucesivas resoluciones del TJUE<sup>46</sup>, el tratamiento de los datos se ha de realizar *en el contexto de las*

---

<sup>45</sup> Art. 4.16 a) RGPD. *En lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento.*

<sup>46</sup> STJUE de 13 de mayo de 2014, asunto C-131/12, *Google Spain S.L contra Agencia Española de Protección de Datos (AEPD)* (ECLI:EU:C:2014:317). En esta sentencia el TJUE ha tratado elementos clave en el marco de la protección de datos personales y el funcionamiento de los buscadores de Internet. El antecedente de esta resolución se halla en una cuestión prejudicial remitida por la Audiencia Nacional al Tribunal de Justicia. *En efecto, en tales circunstancias, las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades* (apartado 56). Con relación a esta sentencia *vid.* TOMAN, R.: “Limited Liability of Internet Search Engine Service Providers for Data Protection of Personal Data Displayed on Source Web Pages”, *European Law Reporter*, 2013, pp. 286-289; WHITE, D.: “Private eye. Tom Morrison & David White review the world of information law”, *New Law Journal*, 2014, pp. 17-18; MUÑOZ, J.: “El llamado “derecho al olvido” y la responsabilidad de los buscadores: Comentario a la sentencia del TJUE de 13 de mayo 2014”, *Diario La Ley*, núm. 92, 2014, pp. 9-10; STEVEN, J.: “The Right to Privacy Catches Up with Search Engines: The Unforgettable Decision in Google Spain vs AEPD”, *Computer and Telecommunications Law Review*, 2014, pp. 130-133; CROWTHER, H.: “Data protection: Google vs Spain: is there now a right to be forgotten?”, *Journal of Intellectual Property Law and Practice*, 2014, pp. 892-893; HERRERO PRIETO, P.: “Search Engines: Interplay of Fundamental Rights and the Principle of Proportionality”, *Computer and Telecommunications Law Review*, 2014, pp. 213-221.

STJUE de 6 de octubre de 2015, asunto C-362/14, *Schrems* (ECLI:EU:C:2015:650). *En ese sentido es preciso observar que, dado el importante papel que cumple la protección de los datos personales en relación con el derecho fundamental al respeto de la vida privada, así como el gran número de personas cuyos derechos fundamentales pueden ser vulnerados en caso de transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, la facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda reducida, por lo que se debe ejercer un control estricto de las exigencias derivadas del artículo 25 de la Directiva 95/46, entendido a la luz de la Carta (véase por analogía la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48) (apartado 78). Vid. PADOVA, Y.: “La Cour de Justice de l’Union européenne va-t-elle invalider les accords Safe Harbour?”, *Droit de l’immatériel: informatique, médias, communication*, núm. 110, 2014, pp. 14-16.*

STJUE de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros* (ECLI:EU:C:2014:238). *En el presente asunto, debido, por una parte, al importante papel que desempeña la protección de los datos de carácter personal en lo que respecta al derecho fundamental al respeto de la vida privada y, por otra parte, a la magnitud y gravedad de la injerencia en este derecho que supone la Directiva 2006/24, la facultad de apreciación de legislador de la Unión resulta reducida, por lo que el control de dicha facultad debe ser estricto* (apartados 47 y 48).

*actividades del establecimiento.* En este sentido, el Dictamen 8/2010 del 16 de diciembre de 2010, sobre el Derecho aplicable, emitido por el Grupo de Protección de Datos del Artículo 29 Directiva 95/46/CE<sup>47</sup>, WP 179, concreta una serie de métodos para estudiar si el tratamiento en cuestión se ha llevado a cabo en tal contexto:

1. *Grado de implicación del establecimiento en las actividades en cuyo contexto se traten los datos personales. Consiste en determinar qué actividades realiza cada establecimiento.*

2. *Naturaleza de las actividades del establecimiento. La cuestión de si una actividad entraña o no un tratamiento de datos y qué tratamiento se esté efectuando en el contexto de qué actividad depende en gran medida de la naturaleza de dichas actividades.*

En definitiva, y tomando como referencia la doctrina elaborada por el TJUE en el asunto *Google Spain*<sup>48</sup>, existe la opción de que las actividades de procesamiento de datos<sup>49</sup> y las de un establecimiento local se encuentre intrínsecamente vinculadas, a pesar de que el establecimiento no ejerza ninguna función en el tratamiento de la información.

---

STS 210/2016 de 5 abril de 2016 (ES:TS:2016:1280). En relación con el espacio temporal en el que se ha de respetar los principios de la protección de datos debemos tener en consideración el apartado 13. *El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los requisitos que determinan su carácter lícito y, en concreto, con los principios de calidad de datos (adecuación, pertinencia, proporcionalidad y exactitud), no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento.*

<sup>47</sup> *El GPD es un órgano consultivo creado en virtud del art. 29 Directiva 95/46/CE e integrado básicamente por representantes de la Comisión y de las agencias nacionales de protección de datos de los Estados de la UEM.* GUERRERO PICÓ, C.: *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Civitas, Madrid, 2006, p. 341.

<sup>48</sup> *A partir de la vinculación existente entre Google Inc –gestora del buscador- y su filial en España Google S.L, el Tribunal de Justicia concluye sobre este particular que el requisito del art. 4 de la Directiva acerca de que el tratamiento de datos se lleve a cabo en el marco de las actividades de un establecimiento del responsable en territorio español se cumple cuando el gestor de un motor de búsqueda cuenta en España con una sucursal o una filial destinada a la promoción y la venta de espacios publicitarios en el buscador cuya actividad se dirige a los habitantes de España.* DE MIGUEL ASENSIO, P. A.: “El tratamiento de datos personales por buscadores de Internet tras la sentencia *Google Spain* del Tribunal de Justicia”, *La Ley Unión Europea*, núm. 17, 2014, p. 5.

<sup>49</sup> *El procesamiento de datos de carácter personal debe regirse por los principios de la legalidad, equidad y transparencia. Deben perseguir minimizar la amplitud de la intervención en el proceso de datos, ser lo más preciso posible, minimizar el almacenamiento de los mismos, primar la efectividad, la integridad y la responsabilidad ante terceros por la gestión de los mismos.* LOPEZ AGUILAR, J. F.: *Data protection package y parlamento europeo, hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Madrid, 2015, p. 58.

#### 4. Responsables o encargados no establecidos en la Unión

En virtud de lo reflejado en el codo. 14 RGPD<sup>50</sup>, la protección en las personas físicas se llevará a término independientemente de su nacionalidad o de su lugar de residencia. No obstante, cuando el procesamiento de los datos no se realiza en las actividades de un establecimiento en la Unión, dicha protección se restringe a los interesados ubicados en la UE, exigiéndose además una conexión adicional con esta, resultando imprescindible para consolidar la protección de los usuarios en el entorno global de Internet, así como para eludir una injustificada aplicación extraterritorial.

En contraste al método aplicado en la Directiva fundamentado en el recurso a medios ubicados en un Estado miembro, el art. 3.2 RGPD prevé su aplicación al tratamiento de información personal de los interesados<sup>51</sup> cuya residencia se encuentre en la UE siempre que la utilización de los datos se asocie con uno de los siguientes elementos:

*a) la oferta de bienes o servicios<sup>52</sup> a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago.*

*b) el control de su comportamiento, en la medida en que éste tenga lugar en la Unión.*

El precepto mencionado en el párrafo anterior ha de ponerse en relación con el art. 27 y el codo. 80, los cuales obligan al responsable<sup>53</sup> o encargado de nombrar a un representante establecido en la Unión en relación con las obligaciones que estipula el

---

<sup>50</sup> Codo. 14 RGPD. *La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.*

<sup>51</sup> (fecha de consulta: 7-11-2018) <https://www.aepd.es/media/estudios/informe-politicas-de-privacidad-adaptacion-RGPD.pdf>.

<sup>52</sup> STJUE de 16 de octubre de 2008, asunto C-298/07, *Bundesverband der Verbraucherzentralen und Verbraucherverbände* (ECLI:EU:C:2009:85). *El prestador de servicios ha de proporcionar a sus usuarios la información necesaria que garantice una comunicación eficiente y directa: la Directiva 2001/23 pretende garantizar la continuidad de las relaciones laborales existentes en el marco de una unidad económica, con independencia de un cambio de propietario y, de ese modo, proteger a los trabajadores en caso de que se produzca dicho cambio* (apartado 40).

<sup>53</sup> *Se añade una excepción al listado que en su momento estableció la Directiva 95/46. Se trata de la posibilidad de que el responsable pueda transferir datos a un país sin nivel adecuado de protección cuando esa transferencia sea necesaria para satisfacer intereses legítimos imperiosos del responsable y la transferencia no es repetitiva y afecta sólo a un número limitado de interesados. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los afectados y deberá comunicarse a la autoridad de protección de datos* (fecha de consulta: 3-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.

RGPD. Por consiguiente, el lugar de residencia del sujeto cuyos datos personales han sido procesados ha de ser considerado como un criterio legítimo para fijar el régimen jurídico aplicable, así como la competencia internacional. De cualquier modo, la literalidad del art. 3.2 RGPD no nos facilita su interpretación, podríamos decir que el objetivo de fondo es hacer más accesible el sometimiento a la legislación europea de aquellos individuos que no residen en la UE, pero procesan datos de personas que sí se encuentran en la Unión.

El codo. 23 RGPD<sup>54</sup> establece la necesidad de aclarar *si es evidente que el responsable*<sup>55</sup> *o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estado miembros*. Más aún, trata de evidenciar que la simple accesibilidad en la Unión *o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento*, no es suficiente para conocer dicha intención, sino que alude a otros criterios para esclarecer la pretensión del responsable<sup>56</sup>, como puede ser el idioma mediante el cual se adquieren bienes y servicios o el registro de usuarios que residen en la Unión. No obstante, podemos acudir a la jurisprudencia del TJUE<sup>57</sup> como punto de partida del criterio<sup>58</sup>, que establece que la actividad económica tenga como objetivo el Estado donde el consumidor reside habitualmente. En esta línea, El TJUE menciona otros requisitos relevantes como pueden ser la expresión de voluntad de atraer a consumidores de dicho Estado miembro, anunciar la oferta de sus bienes en ese Estado de la Unión o la

---

<sup>54</sup> El codo. 23 RGPD no contempla que la accesibilidad *Web*, el uso de un tercer idioma común o los datos de contacto sean indicios de oferta de servicios y productos en la Unión, como dicta la STJUE *Weltimmo*.

<sup>55</sup> *Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados* (fecha de consulta: 3-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.

<sup>56</sup> La doctrina establecida por el TJUE deriva de la establecida por la *Supreme Court* estadounidense *Calder vs Jones* (465 U.S. 783 (1984)), que proporciona a los jueces un método para analizar si nos encontramos ante un mercado objetivo a través de un conjunto de requisitos como la lengua utilizada, la divisa o la nacionalidad.

<sup>57</sup> STJUE de 24 de noviembre de 2011, asunto C-70/10, *Scarlet Extended* (SA ECLI:EU:C:2011:771). Litigio entre Scarlet Extended S.A y Sociétés belge des auteurs, compositeurs et éditeurs SABAM, relativo a la negativa de la primera sociedad a establecer un sistema de filtrado de las comunicaciones electrónicas mediante programas de intercambio de archivos con el fin de evitar los intercambios de archivos que vulneren los derechos de autor. *Scarlet adujo que el establecimiento de un sistema de filtrado vulnera las disposiciones del Derecho de la Unión sobre la protección de datos de carácter personal y la confidencialidad de las comunicaciones, ya que implica el tratamiento de las direcciones IP, que son datos personales* (apartado 26).

<sup>58</sup> Art. 17.1 c) del Reglamento (UE) 1215/2012. *DOUE* L 351/1, 20-XII-2012. Art. 6.1.c) del Reglamento (CE) 593/2008 (Roma I) *DOUE* L 41/7, 4-VII-2008.

difusión de sus productos mediante publicidad que sea accesible por los consumidores que residan en el Estado en cuestión<sup>59</sup>.

El art. 3.2 b) RGPD surte efectos cuando el procesamiento de los datos de los usuarios esté relacionado con el estudio de su comportamiento, se lleve a término en la UE o el responsable<sup>60</sup> no estuviera establecido en la Unión. Según el estudio de la doctrina, este suceso está dirigido exclusivamente a la utilización de archivos o programas informáticos que registran y facilitan la accesibilidad al terminal del usuario (*cookies*), sin tener en consideración el ofrecimiento de productos o servicios. Igualmente, este precepto es aplicable en la oferta de bienes y servicios a través del *Big Data* al tratarse de una monitorización de la conducta del ciudadano.

Por último, debemos poner en relación el art. 3.2 b) RGPD con el codo. 24, que se refiere al control de comportamiento como análisis del afectado en la Red. En este sentido, entiende el *Big Data* como *el uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales*<sup>61</sup>, *comportamientos y actitudes*. Esto es, el art. 3.2 b) RGPD está destinado a

---

<sup>59</sup> STJUE de 7 de diciembre de 2010, asuntos acumulados C-585/08 y C-144/09, *Pammer y Hotel Alpenhof* (ECLI:EU:C:2010:740). La resolución del TJUE enumera un conjunto de elementos para delimitar la pretensión del responsable, entre estos indicios no figura la mención en una página *Web* de la dirección electrónica o postal del vendedor ni tampoco la indicación de su número de teléfono sin prefijo internacional. Efectivamente, la mención de esta información no pone de manifiesto que el vendedor dirija su actividad a otro u otros Estados miembros, puesto que, en cualquier caso, es un tipo de información necesaria para permitir que un consumidor domiciliado en el territorio del Estado miembro en el que está establecido el vendedor se ponga en contacto con este último (apartado 77). En cambio, como se desprende del apartado 77 de la presente sentencia, la mención de la dirección electrónica o postal de la sociedad intermediaria o del vendedor no es un indicio pertinente. Lo mismo ocurre con la utilización de la lengua alemana y con la posibilidad de reservar un viaje en esa lengua, cuando es la lengua del vendedor (apartado 91).

<sup>60</sup> *El tratamiento debe contar con al menos una de las bases de legitimidad establecidas en los artículos 6, 7 y 11 de la LOPD. Dicho tratamiento debe respetar los principios enumerados en el art. 4. El responsable del tratamiento debe informar al titular de los datos, a la luz del art. 5; deberá adoptar medidas de seguridad (art. 9), notificar a la AEPD (art. 26), etc.* BARCELÓ R./ PÉREZ ASINARI, M. V.: *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD*, Tirant lo Blanch, Valencia, 2009, p. 142.

<sup>61</sup> En el tema relativo a actitudes y comportamientos personales hemos de destacar las conclusiones elaboradas por el Abogado General Paolo Mengozzi de 1 de febrero de 2018 en el asunto C-25/17, *Tietosuojavaltuutettu contra Jehovan todistajat* (ECLI:EU:C:2018:57). Establece que las actividades de los testigos de Jehová o “predicadores de puerta en puerta” trascienden el mero uso doméstico de los datos, puesto que distribuyen los predicadores por zonas y se facilitan datos sobre la situación religiosa (información sensible) a autoridades superiores en dicha comunidad. *Por consiguiente, se trata de dilucidar si la comunidad determina los fines y los medios del tratamiento de los datos recopilados por sus miembros. A tal efecto, procede recordar que se desprende de la redacción de la tercera cuestión prejudicial que la comunidad “organiza” la actividad en la que sus miembros recogen datos personales en el sentido de que reparte los radios de acción entre los distintos predicadores, realiza el seguimiento de la actividad de tales predicadores y lleva un registro de las personas que no desean recibir visitas. Dichos elementos son indicativos de que la comunidad centraliza la actividad de predicación. En estas circunstancias,*

la monitorización de las conductas reflejadas no solo en Internet sino en cualquier espacio que lo permita.

## II. Tutela judicial civil contra un encargado o responsable

### 1. Acciones civiles

La regulación de la tutela judicial contra un responsable viene reflejada en el art. 79 RGPD, siendo indispensable en el derecho a la indemnización que todo individuo ostenta como consecuencia del daño sufrido por haberse vulnerado el RGPD. En este sentido, el ejercicio de acciones judiciales es imprescindible para recibir la indemnización y es que la reclamación ante la autoridad de control no es suficiente para lograr dicha reparación. Debemos tener presente que el RGPD carece de instrumentos que coordinen el control administrativo y la tutela civil<sup>62</sup>.

Las acciones judiciales ejercitadas por los interesados, cuyos derechos han sido violados debido a un incorrecto procesamiento de sus datos personales, derivan en un litigio en el orden civil (excepto si la administración pública es la responsable o encargada del tratamiento), mientras que las reclamaciones ante las autoridades de control desembocan en recursos administrativos y ocasionalmente ante tribunales contencioso-administrativos.

Dejando a un lado el derecho de indemnización, y como alternativa a la posibilidad de reclamar ante una autoridad de control, existen otras acciones<sup>63</sup> que pueden

---

*difícilmente puede seguir sosteniéndose que dicha actividad y la eventual recogida de datos personales que la acompaña son exclusivamente individuales y totalmente ajenas a la comunidad (apartado 65).*

<sup>62</sup> SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012, pp. 190-194.

<sup>63</sup> STS de 15 de octubre de 2015 (ES:TS:2015:4132). La sentencia matiza que el “derecho al olvido” no conlleva que cada usuario pueda crear un pasado aleatoriamente, limitando la publicación de información relativa a aspectos negativos, ni supone que los que publiquen información personal puedan exigir que se diseñe un registro en base a sus pretensiones. El tribunal, tras estimar que la acción ejercitada no había caducado, atribuye la responsabilidad relativa al cumplimiento del principio de calidad de datos al editor de la *Web*. Esta Sala analiza los derechos al honor, intimidad y protección de datos personales frente al ejercicio de la libertad de información. *Ahora bien, la función que cumple la prensa en una sociedad democrática cuando informa sobre sucesos actuales y cuando ofrece al público sus hemerotecas es distinta y debe tratarse de modo diferente. Así lo ha hecho el TEDH, que ha considerado que, mientras que la actividad de los medios de comunicación cuando transmiten noticias de actualidad es la función principal de la prensa en una democracia (la de actuar como un "perro guardián", en palabras de ese tribunal), el mantenimiento y puesta a disposición del público de las hemerotecas digitales, con archivos que contienen noticias que ya se han publicado, ha de considerarse como una función secundaria, en la que el margen de apreciación de que disponen los Estados para lograr el equilibrio entre derechos es mayor puesto que el ejercicio de la libertad de información puede considerarse menos intenso (apartado 5).*

ejercitarse ante los tribunales del orden civil para lograr que se imponga una prohibición al responsable del procesamiento. La jurisprudencia del TS, en materia de derecho al olvido<sup>64</sup>, ilustra esta dualidad en la tutela público-privada en el ámbito de datos personales, donde podemos apreciar que como contraste con las sentencias del orden contencioso<sup>65</sup>, las del orden civil reflejan la eventual indemnización de los daños.

Tal como se ha visto, la jurisprudencia de la Sala de lo Civil y de la Sala de lo Contencioso del TS han enfatizado la diferencia de los criterios rectores que rigen ambas jurisdicciones, siendo el orden contencioso el encargado de conocer, tras la interposición por el perjudicado de una reclamación administrativa, las impugnaciones frente a las resoluciones de la AEPD<sup>66</sup>. En lo que respecta al término “responsable del tratamiento”, debemos poner de relieve que ambas Salas difieren en su interpretación al analizar la responsabilidad (civil o administrativa) procedente del inadecuado procesamiento de datos por la prestación de un servicio. La Sala de lo Civil<sup>67</sup> ha manifestado que *Google Spain S.L* (sede española) y *Google Inc.* son responsables del procesamiento de datos por parte del buscador, sin embargo, la Sala de lo Contencioso<sup>68</sup> del TS ha considerado a *Google Inc.* como único responsable.

---

<sup>64</sup> STS de 5 de abril de 2016 (ECLI:ES:TS:2016:1280). *La Sala realiza una ponderación entre el ejercicio de la libertad de información, consistente en que los datos sobre la concesión de indultos puedan encontrarse a través de un buscador como Google, y el respeto a los derechos al honor y a la intimidad cuando la información versa sobre el indulto por un delito que afecta negativamente a la reputación del afectado* (Tribunal Supremo Sala de lo Civil Gabinete Técnico).

<sup>65</sup> Sala de lo Contencioso del TS sobre recursos de casación contra sentencias de la Audiencia Nacional, relativas a resoluciones sancionatorias de la AEPD frente al buscador *Google*. En particular las SSTs (Sala de lo Contencioso) de 11 de marzo de 2016 (ECLI:ES:TS:2016:1057); de 14 de marzo de 2016 (ECLI:ES:TS:2016:1056 y ECLI:ES:TS:2016:964); de 15 de marzo de 2016 (ECLI:ES:TS:2016:1103); así como las ocho sentencias pronunciadas por dicha Sala el 13 de junio de 2016 (ECLI:ES:TS:2016:2696; ECLI:ES:TS:2016:2699; ECLI:ES:TS:2016:2702; ECLI:ES:TS:2016:2707; ECLI:ES:TS:2016:2722; ECLI:ES:TS:2016:2723; ECLI:ES:TS:2016:2724; ECLI:ES:TS:2016:2725). En estas últimas sentencias la Sala de lo Contencioso dedica un fundamento jurídico específicamente a abordar las implicaciones de la sentencia de la Sala de lo Civil de 5 de abril de 2016.

<sup>66</sup> *Considerando que la legislación española en materia de protección de datos es una de las más exigentes del mundo, se entiende fácilmente el recelo de la Agencia sobre las transferencias internacionales de datos. Cualquier transferencia deberá estar respaldada por las máximas garantías, con el fin de que esta transferencia no burle la legislación española ni menoscabe la protección otorgada a los afectados.* COUDERT, F.: *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, Valladolid, 2005, p. 385.

<sup>67</sup> STS de 5 de abril de 2016 (ECLI:ES:TS:2016:1280). *En las sentencias de la Sala de lo Contencioso Administrativo se está resolviendo con relación a resoluciones dictadas en un procedimiento administrativo seguido ante la AEPD, mientras que esta sentencia se dicta en un proceso civil que tiene por objeto la protección de los derechos fundamentales del demandante, en concreto los derechos al honor, a la intimidad y a la protección frente al tratamiento automatizado de sus datos de carácter personal.* (apartado 13).

<sup>68</sup> STS de 13 de junio de 2016 (ES:TS:2016:2722). *No puede compararse el planteamiento de la Sala de instancia que aprecia una corresponsabilidad de carácter genérico, sin precisar o identificar los concretos*

Desde el punto de vista de la competencia internacional, la STS (Civil) de 5 de abril de 2016 ha basado su razonamiento en el hecho de que demandar a una empresa extranjera en España evita obtener una protección eficiente del derecho a la protección de datos. *El Tribunal destaca las dificultades asociadas a tener que litigar contra un demandado domiciliado en el extranjero, como el coste de la traducción de la demanda, la dilación que implicaría el emplazamiento (con lo que se prolongaría la vulneración de los derechos fundamentales), o la eventual necesidad de solicitar la ejecución de la sentencia en EE. UU. Esta posición explica que las posteriores sentencias de 8 de abril de 2016 de la Sala de lo Contencioso incluyan una explicación del funcionamiento de la vía contencioso-administrativa, para destacar que la circunstancia de que el responsable se halle establecido en el extranjero no implica en este orden jurisdiccional que la tutela para el afectado resulte más gravosa*<sup>69</sup>.

## **2. Regla especial de competencia: alcance**

El art. 79.2 RGPD ha incorporado una novedad que afecta a la determinación de la competencia judicial internacional en el ámbito civil, otorgando a los interesados la facultad de interponer una demanda contra el responsable o el encargado del tratamiento ante los tribunales del Estado miembro *en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual*. No obstante, la aplicabilidad de este foro se encuentra condicionada por el apartado 1 del art. 79 RGPD que alude a la tutela judicial de los interesados cuando un responsable o encargado del procesamiento de sus datos ha vulnerado sus derechos. Tal y como he mencionado anteriormente, nos movemos en el marco de las acciones civiles, exceptuando el caso en el que la propia administración pública sea la encargada de dicho tratamiento, donde debemos poner de relieve la correlación entre el RBI *bis* y el art. 79.2 RGPD. De este modo, el art. 1 RBI *bis* afirma rotundamente que *el presente Reglamento se aplicará en materia civil y mercantil con independencia de la naturaleza del órgano jurisdiccional*.

---

*finés o medios del tratamiento que determina Google Spain ni cuál es el alcance de su responsabilidad y menos que forme parte de ella la obligación cuyo cumplimiento se exige por el interesado y que la AEPD declara* (fundamento jurídico séptimo).

<sup>69</sup> 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*, núm. 69, 2017, p. 27.

Ante la situación planteada, la jurisprudencia del TJUE ha excluido la aplicación del RBI *bis* cuando la tutela de los derechos afectados proceda de la actuación de una autoridad en el ejercicio de su poder público<sup>70</sup>. Dicho de otro modo, este Reglamento es aplicable cuando la *responsabilidad del Estado por acciones u omisiones* no se efectúe en el ejercicio de su autoridad (art. 1 RBI *bis*). En este sentido, el art. 78 RGPD recoge otras actuaciones excluidas, como son las originadas por las facultades propias de las autoridades de control en la realización de sus funciones públicas.

En base al art. 79 RGPD, la tutela solicitada por el interesado como consecuencia de la infracción de sus derechos puede fundamentarse en acciones de responsabilidad extracontractual con el fin de obtener una indemnización, *acciones que se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el art. 79, apartado 2* (art. 82.6 RGPD). Sin embargo, la realidad nos muestra como el interesado del tratamiento y el responsable pueden relacionarse mediante la firma de un contrato. En esta línea, el TJUE ha señalado que las acciones de responsabilidad civil ejercitadas por una de las partes deben ser entendidas en el marco del contrato siempre que se haya infringido alguna de sus obligaciones<sup>71</sup> en virtud del art. 7 RBI *bis*.

---

<sup>70</sup> STJUE de 11 de abril de 2013, asunto C-645/11, *Sapir* (ECLI:EU:C:2013:228). El litigio se origina en base a la devolución errónea de un abono excesivo en el marco de un procedimiento administrativo relativo a la indemnización de los daños producidos por la pérdida de un inmueble durante el régimen nazi. *A este respecto, es preciso hacer constar que, al igual que el del Convenio de Bruselas, el ámbito de aplicación del Reglamento 44/2001 se limita al concepto de “materia civil y mercantil”. De una jurisprudencia reiterada del Tribunal de Justicia resulta que dicho ámbito de aplicación se delimita esencialmente en atención a los elementos que caracterizan la naturaleza de las relaciones jurídicas entre las partes del litigio o el objeto de este* (apartado 32). *El Tribunal de Justicia ha considerado así que, si bien determinados litigios surgidos entre una autoridad pública y una persona de Derecho Privado pueden estar comprendidos dentro del ámbito de aplicación del Reglamento núm. 44/2001, la situación es distinta cuando la autoridad pública actúa en ejercicio del poder público* (apartado 33).

<sup>71</sup> STJUE de 13 de marzo de 2014, asunto C-548/12, *Brogssitter* (ECLI:EU:C:2014:148). *Sin embargo, la mera circunstancia de que una de las partes contratantes entable una acción de responsabilidad civil contra la otra no basta para considerar que tal acción esté comprendida en la “materia contractual” en el sentido del art. 5, punto 1, letra a), del Reglamento 44/2001. Únicamente puede considerarse que el comportamiento recriminado es un incumplimiento de las obligaciones contractuales, tal como pueden determinarse teniendo en cuenta el objeto del contrato. Este será el caso a priori, si la interpretación del contrato que une al demandado con el demandante resulta indispensable para determinar la licitud o, por el contrario, la ilicitud del comportamiento imputado al primero por el segundo* (apartados 23 a 25). Resulta también de interés la sentencia de 1 de octubre de 2002, *Karl Heinz Henkel*, asunto C-167/00 (ECLI:EU:C:2002:555). En virtud de esta resolución *vid.* JIMÉNEZ BLANCO, P.: “El tratamiento de las acciones colectivas en materia de consumidores en el Convenio de Bruselas”, *Diario La Ley*, núm. 5709, 2003, pp. 1-6; FACH GÓMEZ, K.: “Competencia judicial internacional en materia de acciones preventivas: Interpretación del Tribunal de Justicia de las Comunidades Europeas”, *Noticias de la Unión Europea*, núm. 225, 2003, pp. 83-91.

Dicho lo anterior, procedemos a analizar las acciones colectivas<sup>72</sup> llevadas a cabo cuando un conjunto de interesados ha resultado perjudicado como consecuencia del tratamiento de su información. En el ámbito europeo este tipo de acciones han quedado reflejadas en el caso *Schrems c. Facebook*<sup>73</sup>. En este contexto, el art. 80 RGPD faculta a entidades, organizaciones o asociaciones sin ánimo de lucro la posibilidad de presentar en nombre del interesado una reclamación, así como ejercer en su nombre los derechos regulados en el art. 77, 78 y 79 RGPD. Ahora bien, teniendo en cuenta que el art. 80 RGPD no hace alusión a la competencia judicial y ante la ausencia de regulación en el RBI *bis* debemos tener en consideración el art. 79.2 RGPD.

### 3. Foro del establecimiento

A diferencia de lo dispuesto en la Directiva 95/46/CE<sup>74</sup>, el término “establecimiento” no es requerido para delimitar la competencia de las autoridades nacionales de supervisión. De cualquier modo, su importancia radica como foro de competencia en este nuevo contexto, y es que el art. 79 establece que serán competentes *los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento*, por lo tanto, se ha de interpretar que existe la opción de que su presencia se de en una pluralidad de Estados miembros.

---

<sup>72</sup> STJUE de 14 de julio de 2016, asunto C-196/15, *Granarolo* (ECLI:EU:C:2016:559). Litigio entre la sociedad italiana Granarolo S.A y la sociedad francesa Ambrosi Emmi France S.A, relativo a una acción de indemnización fundada en la ruptura repentina de relaciones comerciales de larga duración. *El Tribunal de Justicia ya ha declarado que la mera circunstancia de que una de las partes contratantes entable una acción de responsabilidad civil contra la otra no basta para considerar que tal acción esté comprendida en la “materia contractual” en el sentido del art. 5, punto 1, del Reglamento Bruselas I* (apartado 21).

<sup>73</sup> STJUE de 6 de octubre de 2015, asunto C-362/14, *Schrems* (ECLI:EU:C:2015:650). Litigio entre Schrems y el *Data Protection Commissioner*, acerca de la negativa de este a instruir una reclamación presentada por Schrems, basada en que *Facebook Ireland Ltd* transfiere a Estados Unidos los datos personales de sus usuarios y los conserva en sus servidores situados en ese país. *De igual manera, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el art. 47 de la Carta. En efecto, el art. 47, párrafo primero, de esta establece que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva, respetando las condiciones establecidas en dicho artículo. En ese sentido, la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho* (apartado 95).

<sup>74</sup> *El nuevo Reglamento modifica la filosofía anterior en el sentido de que ya no se aprobará una nueva Directiva para que posteriormente los diferentes países transpongan su contenido a través de normas nacionales. En su lugar habrá una normativa única y válida en toda la UE sobre protección de datos. GUASCH PORTAS, V.: “La transferencia internacional de datos de carácter personal”, Revista de derecho Universidad Nacional Educación a Distancia, núm. 11, 2012, p. 450.*

A pesar de que la práctica nos muestra como la tendencia es que el establecimiento se corresponda con el Estado en el que se ubica el domicilio del demandado (foro general art. 4.1 RBI *bis*), nos encontramos ante dos modalidades que no derivarán en unas mismas consecuencias. Haciendo alusión al art. 4.1 del RBI *bis*, el domicilio se refiere a las personas jurídicas de forma independiente por su art. 63: *a efectos del presente Reglamento, se entenderá que una sociedad u otra persona jurídica está domiciliada en el lugar en que se encuentra: a) su sede estatutaria; b) su administración central, o c) su centro de actividad principal*. En cambio, en relación con las personas físicas, el art. 62 indica que el órgano jurisdiccional aplicará su legislación interna para afirmar si una parte *está domiciliada en el Estado miembro cuyos órganos jurisdiccionales conozcan del asunto* (art. 62.1 RBI *bis*). El art. 79.2 RGPD toma como referencia un concepto extenso de establecimiento *a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable*<sup>75</sup>.

Tomando en consideración la sentencia *Weltimmo* hemos de analizar factores como *el grado de estabilidad de la instalación, la efectividad del desarrollo de las actividades, la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión* para confirmar la presencia de una instalación en un Estado que no se corresponda con el del domicilio social. De manera análoga, en la resolución *Verein für Konsumenteninformation* el TJUE destacó la posibilidad de encontrarnos ante un establecimiento<sup>76</sup> sin que la entidad en cuestión tenga adjudicada una filial en dicho Estado miembro, en cuyo caso se ha de estudiar el nivel de eficiencia y estabilidad de la instalación (apartados 76 y 77)<sup>77</sup>.

---

<sup>75</sup> STJUE de 28 de julio de 2016, asunto C-191/15, *Verein für Konsumenteninformation* (ECLI:EU:C:2016:612). Litigio entre Verein für Konsumenteninformation (Asociación para la información de los consumidores) y Amazon EU Sàrl, con domicilio social en Luxemburgo, acerca de una acción de cesación presentada por VKI. *Por lo que se refiere, en primer lugar, al concepto de “establecimiento” en el sentido del art. 4, apartado 1, letra a), de la Directiva 95/46, el Tribunal de Justicia ha precisado que se extiende a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable* (apartado 75).

<sup>76</sup> Conclusiones elaboradas por el Abogado General Henrik Saugmandsgaard ØE presentadas el 2 de junio de 2016 en el asunto C-191/15, *Verein für Konsumenteninformation* (ECLI:EU:C:2016:388). *No excluyo que, como ha alegado VKI, un eventual servicio posventa, como un servicio de atención al cliente destinado a los clientes residentes en Austria, pueda constituir un establecimiento en dicho territorio. Sin embargo, tal apreciación no podría justificar, por sí sola, la aplicabilidad de la DSG* (apartado 121).

<sup>77</sup> STJUE de 28 de julio de 2016, asunto C-191/15, *Verein für Konsumenteninformation* (ECLI:EU:C:2016:612). *A este respecto, como ha señalado el Abogado General en el punto 119 de sus conclusiones, si bien el hecho de que la empresa responsable del tratamiento de datos no posea una filial ni una sucursal en un Estado miembro no excluye que pueda tener en su territorio un establecimiento en el sentido del art. 4, apartado 1, letra a), de la Directiva 95/46, ese establecimiento no puede existir por el*

Al hilo de lo expuesto en los párrafos anteriores, el fin de proteger y asegurar los derechos de los afectados viene directamente enlazado con la amplitud del término “establecimiento” regulado en el RGPD como foro de competencia para adjudicar competencia a tribunales de Estados miembros que no gozarían de la misma a tenor del art. 4 RBI *bis*. La flexibilidad de este término resulta clave a la hora de ejercitar acciones colectivas por interesados de múltiples Estados. En comparación con lo dispuesto en el art. 3 RGPD, donde se requiere que la acción se enfoque en un procesamiento de un establecimiento específico, el art. 79.2 RGPD considera que cualquier establecimiento del responsable o encargado puede atribuir la competencia en cuestión.

#### **4. Residencia habitual del interesado**

El art. 79 RGPD establece como elemento subsidiario de competencia la posibilidad de que el interesado ejercite las acciones ante los tribunales del Estado miembro donde resida de forma habitual. En lo que respecta al concepto de “residencia habitual”, reiterado en los Reglamentos de la UE que no se remiten de forma directa a la legislación interna de los Estados miembros, el TJUE ha manifestado que ha de interpretarse<sup>78</sup> dentro del marco en el cual se integran las demás disposiciones<sup>79</sup>.

Debemos subrayar que la “residencia habitual del interesado” no es equiparable

---

*mero hecho de que allí se pueda acceder al sitio de Internet de la empresa en cuestión. Como ya ha declarado el Tribunal de Justicia, más bien deben evaluarse tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades en el Estado miembro de que se trate (apartados 76 y 77).*

<sup>78</sup> STJUE de 16 de octubre de 2008, asunto C-298/07, *deutsche Internet versicherung* (ECLI:EU:C:2008:572). Litigio entre el Sr. Klarenberg y Ferrotron Technologies GmbH en relación con la transmisión de las relaciones laborales a esta sociedad. *En virtud de ese contrato, la sociedad que controla a Ferrotron adquirió todos los derechos sobre el software, las patentes, las solicitudes de patente y las invenciones relativas a los productos de que se trata, así como sobre las denominaciones de los mismos y los procedimientos técnicos. Ferrotron adquirió el hardware de desarrollo y los materiales de fabricación que figuraban en las existencias de ET así como una lista de proveedores y una de clientes. Asimismo, fueron transferidos a Ferrotron algunos trabajadores de ET, a saber, Neumann y tres ingenieros de la unidad “F+E/ET-Systeme” (apartado 15).* Al amparo de la jurisprudencia comunitaria, para interpretar un precepto de una norma europea debemos tener en consideración la redacción literal, en el marco en el que se ha integrado y los fines perseguidos.

<sup>79</sup> STJUE 22 de diciembre de 2010, asunto C-497/10, *Mercredi* (ECLI:EU:C:2010:829). Litigio entre Chaffe, padre de una menor, y Mercredi, madre de esa niña, sobre el derecho de custodia de la menor, que actualmente se encuentra con su madre en la isla de Reunión (Francia). *Dado que los artículos del Reglamento que mencionan el concepto de “residencia habitual” no contienen ninguna remisión expresa al Derecho de los Estados miembros para determinar el sentido y el alcance de ese concepto, su determinación debe realizarse atendiendo al contexto en el que se insertan las disposiciones del Reglamento y al objetivo pretendido por este, en especial el que resulta de su duodécimo Considerando, según el cual las normas de competencia que establece están concebidas en función del interés superior del menor, y en particular en función del criterio de proximidad (apartado 46).*

al centro de intereses de la víctima como método elaborado por la jurisprudencia del TJUE para delimitar, en los casos de vulneración de un derecho de la personalidad en la Red, donde se ha ocasionado el perjuicio en virtud del art. 7.2 RBI *bis*. En la sentencia *eDate Advertising*<sup>80</sup>, el TJUE menciona la posibilidad de que un particular desarrolle su centro de intereses en un Estado en el que no resida habitualmente, siempre que exista una previa relación o enlace con ese Estado<sup>81</sup>.

Por otro lado, debemos hacer notar que la competencia relativa a la residencia habitual del interesado se proyecta además en los perjuicios que el procesamiento de datos elaborado por el responsable o encargado haya ocasionado, es decir, no se restringe únicamente al producido en el Estado de su residencia habitual. Lo cierto es que del art. 79 RGPD no se desprende que la aplicabilidad de esta regla de competencia dependa del cumplimiento de ciertos requisitos, ahora bien, esta regla va a depender de las normas de ámbito territorial del art. 3 RGPD.

## **5. Interacción con las reglas de competencia del Reglamento Bruselas I *bis*.**

El origen de las relaciones entre el RBI *bis* y el art. 79 RGPD se enmarca en el codo. 145 y 147 RGPD, así como en el art. 67 RBI *bis*<sup>82</sup>. En esta línea, cabe subrayar como el RBI *bis* no repercute en los preceptos particulares que en materias especiales aluden a la competencia judicial en los actos de la Unión (art. 79 RGPD). En este sentido, el codo. 147 RGPD establece que *las normas generales de competencia judicial del RBI bis “deben entenderse sin perjuicio de la aplicación” de las normas específicas del*

---

<sup>80</sup> STJUE de 25 de octubre de 2011, asuntos acumulados C-509/09 y C-161/10, *eDate Advertising GmbH* (ECLI:EU:C:2011:685). *Por lo general, el lugar en el que una persona tiene su centro de intereses corresponde a su residencia habitual. Sin embargo, una persona puede tener su centro de intereses también en un Estado miembro en el que no resida habitualmente, en la medida en que otros indicios, como el ejercicio de una actividad profesional, permitan establecer la existencia de un vínculo particularmente estrecho con ese Estado miembro* (apartado 49).

<sup>81</sup> STJUE de 19 de abril de 2012, asunto C-523/10, *Wintersteiger AG* (ECLI:EU:C:2012:220). Litigio entre Wintersteiger, establecida en Austria, y Products 4U Sondermaschinenbau GmbH, establecida en Alemania, relativo a la pretensión de Wintersteiger de que se prohibiese a Products 4U utilizar la marca austriaca “Wintersteiger” como palabra clave en el sitio de Internet del prestador de un servicio remunerado de referenciación. *Dentro del contexto de Internet, el Tribunal de Justicia ha precisado asimismo que, en caso de que se alegue una lesión de los derechos de la personalidad, la persona que se considere lesionada por contenidos publicados en un sitio de Internet puede ejercitar una acción de responsabilidad por la totalidad del daño causado ante los órganos jurisdiccionales del Estado miembro en el que se encuentra su centro de intereses* (apartado 22).

<sup>82</sup> Art. 67 RBI *bis*. *El presente Reglamento no prejuzgará la aplicación de las disposiciones que, en materias particulares, regulan la competencia judicial, el reconocimiento o la ejecución de las resoluciones contenidas en los actos de la Unión o en las legislaciones nacionales armonizadas en ejecución de dichos actos.*

*RGPD*. Por consiguiente, el codo. 145 *RGPD*, en base a lo dispuesto en el art. 79.2 afirma que *por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado.*

El análisis expuesto en el párrafo anterior nos lleva a observar como el propósito de las normas de competencia del *RGPD* es ofrecer a los interesados la opción de ejercitar sus acciones en los tribunales de los Estados miembros donde el encargado acredite tener un establecimiento o la residencia habitual del perjudicado. Dicho de otro modo, el interesado puede acceder a una serie de foros adicionales sin perjuicio del sistema regulado en el *RBI bis*<sup>83</sup>. Esta alternativa también resulta factible cuando solo sean susceptibles de aplicación las leyes internas de cada Estado y no el *RBI bis* (remisión del art. 6.1 *RBI bis*).

Cabe considerar, desde el punto de vista las acciones ejercitadas, cómo los interesados disponen no sólo de los foros del *RBI bis* sino también de los recogidos en el art. 79.2 del *RGPD* que cumplimentan a los anteriores. A modo de ejemplo, son foros contenidos en el *RBI bis*: el foro general del domicilio del demandado (art. 4 *RBI bis*), la prórroga de jurisdicción (art. 25 y 26), foro especial en materia extracontractual del art. 7.2 *RBI bis*, o los foros basados en una relación de desconexión (art. 8). Sin embargo, las medidas del art. 79.2 del *RGPD* no integran determinadas opciones a las que el interesado que ejercita una acción extracontractual podría acudir en referencia al art. 7.2 *RBI bis*, teniendo en cuenta que este además de permitir demandar por la totalidad del daño a los tribunales del Estado miembro del centro de intereses de la víctima<sup>84</sup> también habilita a aquellos donde se ha reflejado las consecuencias del daño, como aquellos donde se ha difundido la información. Si bien es cierto que en materia de vulneración de derechos de

---

<sup>83</sup> 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*, núm. 69, 2017, p. 34.

<sup>84</sup> STJUE de 25 de octubre de 2011, asuntos acumulados C-509/09 y C-161/10, *eDate Advertising GmbH* (ECLI:EU:C:2011:685). *Por lo tanto, procede adaptar los criterios de conexión recordados en el apartado 42 de la presente sentencia en el sentido de que la víctima de una lesión de un derecho de la personalidad a través de Internet puede acudir, en función del lugar en el que haya producido el daño causado en la Unión Europea por dicha lesión, a un foro por la totalidad de ese daño. Habida cuenta de que la repercusión de un contenido publicado en Internet sobre los derechos de la personalidad de una persona puede ser apreciada mejor por el órgano jurisdiccional del lugar en el que la supuesta víctima tiene su centro de intereses, la atribución de competencia a dicho órgano jurisdiccional corresponde al objetivo de una buena administración de la justicia, recordado en el apartado 40 de la presente sentencia* (apartado 48).

propiedad intelectual<sup>85</sup> nos encontramos ante un criterio consolidado por la jurisprudencia del TJUE<sup>86</sup>, en el marco de los derechos de la personalidad.

En lo que se refiere a la tutela privada de la protección de datos personales, la UE ha desarrollado instrumentos de acción colectiva dirigidos a los perjudicados de los distintos Estados miembros por un mismo procesamiento de su información. Si bien cabe decir que el art. 81 RGPD no incorpora ningún criterio de competencia específica en esta materia, las reglas contenidas en el art. 79.2 permiten el ejercicio de estas acciones ante los tribunales de un Estado miembro: *las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento*. De igual modo, y en virtud del art. 8.1 RBI *bis*, debemos mencionar el foro relativo a una pluralidad de demandados: *una persona domiciliada en un Estado miembro también podrá ser demandada: 1) si hay varios demandados, ante el órgano jurisdiccional del domicilio de cualquiera de ellos, siempre que las demandas estén vinculadas entre sí por una relación tan estrecha que resulte oportuno tramitarlas y juzgarlas al mismo tiempo a fin de evitar resoluciones que podrían ser contradictorias si se juzgasen los asuntos separadamente*.

La redacción del art. 79 RGPD parece no especificar la competencia para conocer de las acciones que el encargado o responsable del tratamiento pueden ejercitar frente a

---

<sup>85</sup> STJUE de 3 de octubre de 2013, asunto C-170/12, *Peter Pinckney* (ECLI:EU:C:2013:635). Litigio entre el Pinckney, residente en Francia, y KDG Mediatech AG, sociedad domiciliada en Austria, por una demanda de indemnización de daños y perjuicios debido a la vulneración por parte de dicha sociedad de los derechos patrimoniales de autor del Pinckney. *En efecto, si dicho órgano jurisdiccional fuera también competente para conocer del daño causado en el territorio de otros Estados miembros, sustituiría a los tribunales de dichos Estados, mientras que éstos son, en principio, competentes, en virtud del art. 5, punto 3, del Reglamento y del principio de territorialidad, para conocer del daño causado en el territorio de su respectivo Estado miembro y están en mejores condiciones de valorar, por una parte, si efectivamente se han vulnerado los derechos patrimoniales de autor garantizados por el Estado miembro de que se trate y, por otra parte, para determinar la naturaleza del daño causado* (apartado 46).

<sup>86</sup> STJUE de 17 de octubre de 2017, asunto C-194/16, *Bolagsupplysningen OÜ y Ingrid Ilsjan* (ECLI:EU:C:2017:766). Litigio entre Bolagsupplysningen OÜ e Ingrid Ilsjan, por un lado, y Svensk Handel AB, por otro, en relación con determinadas pretensiones de rectificación de información supuestamente inexacta publicada en el sitio de Internet de esta última, de supresión de comentarios relativos a esta información en un foro de discusión del mencionado sitio y de indemnización del perjuicio presuntamente sufrido. *El art. 7, punto 2, del Reglamento 1215/2012 debe interpretarse en el sentido de que una persona que alega que la publicación de información inexacta en Internet y la no supresión de comentarios que la afectan han vulnerado sus derechos de la personalidad no puede presentar una demanda al objeto de obtener la rectificación de esa información y la supresión de esos comentarios ante los tribunales de cada Estado miembro en cuyo territorio la información publicada en Internet sea o haya sido accesible* (apartado 50).

los interesados. En consecuencia, cuando los responsables o encargados ostentan la posición de actores, el RGPD no incorpora foros adicionales debido a que sus reglas de competencia se constituyen en torno a la protección de los interesados. En consecuencia, las acciones ejercitadas por el responsable frente a los interesados se basarán en el contenido de su relación contractual y no en lo dispuesto en el RGPD.

Debemos destacar que las reglas del RBI *bis* en ningún caso pueden afectar a lo dispuesto en el art. 79.2 RGPD, y esto es para controlar la eficacia de los acuerdos atributivos de jurisdicción entre el responsable y el interesado, cuando el verdadero fin sea la oposición a la demanda por un interesado ante el tribunal competente.

En último lugar, debemos subrayar que en ningún caso cabe descartar *el ejercicio por un responsable frente a un interesado de acciones de carácter extracontractual, por ejemplo de acciones declarativas de no infracción, que en el sistema del RBI bis pueden ejercitar ante los tribunales del lugar de origen del daño, que típicamente coincidirá con su propio domicilio, lo que en el marco del RBI bis llevaría normalmente a apreciar litispendencia con respecto a una posterior acción de indemnización fundada en la infracción*<sup>87</sup>. *En tales circunstancias, la eventual repercusión del RGPD en materia de litispendencia presenta particular relevancia*<sup>88</sup>.

---

<sup>87</sup> STJUE de 19 de diciembre de 2013, asunto C-452/12, *Nipponkoa* (ECLI:EU:C:2013:858). *A este respecto, hay que recordar que, de acuerdo con la jurisprudencia del Tribunal de Justicia acerca de la interpretación del art. 27 del Reglamento 44/2001, una demanda por la que se solicita que se declare que el demandado es responsable de un perjuicio y que se le condene a pagar una indemnización por daños y perjuicios –como la acción de repetición en el procedimiento principal– tiene la misma causa y el mismo objeto que una demanda anterior mediante la que se solicita que se declare que el demandante no es responsable de tal perjuicio* (apartado 42). A tenor de lo dispuesto en el presente pronunciamiento *vid.* TREPPOZ, E.: “La résolution perturbatrice européenne des conflits de conventions en matière de contrats de transport”, *Revue des contrats*, 2014, pp. 251-254.

<sup>88</sup> 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*, núm. 69, 2017, p. 37.

## CAPÍTULO II. TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

### I. Concepto

Si bien es cierto que en la actualidad no existe un término legal que defina el concepto de “transferencia internacional de datos”<sup>89</sup> a nivel global, debemos de estudiar esta expresión desde una óptica jurídica y socioeconómica por parte de las legislaciones relativas al tratamiento de datos de nuestro entorno. En consecuencia, este término<sup>90</sup> se refiere a todo intercambio de información a través de las fronteras, al margen del soporte técnico empleado para ello o la modalidad de tratamiento<sup>91</sup>.

Desde la perspectiva jurídica española se hace referencia al tratamiento de datos como *operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación*<sup>92</sup>, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias art. 3 c) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal<sup>93</sup>. Sin embargo, estrictamente el RGPD no

---

<sup>89</sup> El documento denominado *Frequently asked questions relating to transfers of personal data from the EU/EEA to third countries*, redactado por la Comisión Europea, afirma que el concepto de transferencia de datos personales ha de vincularse con el acto de enviar documentos, vía papel o electrónica, que contiene información personal, a través de correo o por e-mail. Además, hace referencia a los supuestos en los que un responsable de tratamiento toma acciones con el fin de que los datos personales se encuentren disponibles por otra parte situada en un país tercero (fecha de consulta: 7-08-2018) [http://ec.europa.eu/justice/policies/privacy/docs/international\\_transfers\\_faq/international\\_transfers\\_faq.pdf](http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

<sup>90</sup> La profesora Matus Arenas define “transferencia internacional” como *un tratamiento que consiste en la transmisión o transporte de datos, fuera de un Estado, realizado por el responsable del tratamiento directamente a una persona natural (física) o jurídica, que los recibirá en un tercer país, para someterlos a un nuevo tratamiento de datos, bien sea por cuenta propia o por cuenta del transmitente de los datos*. MATUS ARENAS, J.: “Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos”, *Seminario Regional de Protección de Datos*, núm. 97, 2010, versión online.

<sup>91</sup> BLAS, F.: “Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales”, *Revista Derecho del Estado*, núm. 23, 2009, p. 52.

<sup>92</sup> Comunicación de la Comisión Europea de 4 de noviembre de 2010 sobre “un enfoque global de la protección de datos personales en la Unión Europea: el olvido como ‘cancelación’ de datos personales” (fecha de consulta: 9-10-2018) <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009>.

<sup>93</sup> Finalmente, para trasponer dicha Directiva, se aprobó la Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal (LOPD), que derogó la LORTAD y cuyo objeto se extendió a garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal. LESMES SERRANO, C.: *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008, p. 258.

define el término “transferencia internacional de datos personales”<sup>94</sup> sino más bien establece que debemos entender por “tratamiento transfronterizo”<sup>95</sup>.

En relación con lo expuesto en los párrafos anteriores, para esclarecer esta idea de “transferencia internacional de datos de carácter personal”<sup>96</sup> debemos concretar los siguientes elementos:

- El tratamiento de información debe ser relativo a datos de carácter personal, es decir, toda información sobre una persona física identificada o identificable.
- El procesamiento de datos personales<sup>97</sup> puede efectuarse de forma automatizada (vía informatizada), o no automatizada (vía convencional).
- El objetivo del destinatario en esta transferencia internacional<sup>98</sup> de información personal es el tratamiento de esta, bien mediante cesión o comunicación a otro responsable o como prestación de un servicio propio del encargado del tratamiento.
- Transmisión física efectiva de datos de carácter personal<sup>99</sup> a través de las

---

<sup>94</sup> STEDH de 10 de julio de 2014, asunto C-212/13, *Amann vs Suiza* (ECLI:EU:C:2014:2072). En esta paradigmática sentencia se define “dato personal” como cualquier información relativa a un individuo identificado o identificable.

<sup>95</sup> Art. 4.23 RGPD tratamiento transfronterizo: *a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.*

<sup>96</sup> AEPD, “Transferencias internacionales de datos” (fecha de consulta: 7-07-2018) <https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html>.

<sup>97</sup> *En la era del Internet de las cosas, en todo momento generaremos información relacionada con aspectos de nuestra vida que, combinada y segmentada de acuerdo con determinadas correlaciones más o menos afortunadas en su capacidad “predictiva” pueden pre-determinar sin más que una persona, por la categoría a la que pertenece por la “estadística”, pueda acceder o no, a un determinado tipo de producto o servicio. La reflexión es, por tanto, mucho más profunda y está en el origen del por qué (y respecto de qué) son necesarias las normas de protección de datos.* ÁLVAREZ RIGAUDIAS, C.: *El poder del usuario digital, hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Madrid, 2015, p. 305.

<sup>98</sup> *En el Considerando 78 de la Propuesta de Reglamento se reconoce que los flujos transfronterizos de datos personales son necesarios para la expansión del comercio y la cooperación internacional.* GUASCH PORTAS, V.: “La transferencia internacional de datos de carácter personal”, *Revista de derecho Universidad Nacional Educación a Distancia*, núm. 11, 2012, p. 450.

<sup>99</sup> STC 292/2000 de 30 de noviembre de 2000 (ECLI:ES:TC:2000:292). *El hecho de que se hable de datos de carácter personal no significa que sólo se protejan los relativos a la vida privada o íntima de la persona. Se deben proteger todos aquellos datos que identifiquen o permitan identificar la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otro índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo y cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 de la Constitución Española otorga, sino los datos de carácter personal (apartado 6).*

fronteras nacionales, bien en el territorio de la UE o respecto a terceros Estados.

- El destino de los datos personales ha de localizarse en un territorio diferente al de origen de estos.

A fin de continuar profundizando en este concepto, procedemos a estudiar la perspectiva que la jurisprudencia del TJUE<sup>100</sup> ha aportado en la materia. Más concretamente, tomaremos como punto de referencia la sentencia *Lindqvist*, de 6 de noviembre de 2003, asunto C-101/01, *Bodil Lindqvist* relativa a la publicación de datos personales en Internet. El TJUE consideró en esta sentencia que no se produce una transferencia de datos a un país tercero cuando un sujeto ubicado en un Estado miembro publica información en una *Web*, almacenada por su proveedor de servicios cuyo domicilio se encuentra en cualquier Estado miembro, de tal forma que estos datos son accesibles<sup>101</sup> a cualquier usuario de la Red (incluso si se localiza en Estados extracomunitarios<sup>102</sup>), aunque sí se trata de un tratamiento de datos conforme a la

---

<sup>100</sup> En este contexto debemos destacar resoluciones como la STJUE de 18 de octubre de 2012, asunto C-173/11, *Football Dataco Ltd* (ECLI:EU:C:2012:642). Football Dataco y otros son responsables de la organización de los campeonatos inglés o escocés de fútbol. Football Dataco Ltd tiene a su cargo la creación y explotación de los datos y derechos de propiedad intelectual relativos a esos campeonatos. Football Dataco y otros alegan que ostentan, en virtud del Derecho del Reino Unido, *un derecho sui generis sobre la base de datos denominada “Football Live” que debe interpretarse en el sentido de que el envío por una persona, a través de un servidor Web situado en un Estado miembro A, de datos previamente obtenidos por esta persona a partir de una base de datos protegida por el derecho sui generis con arreglo a esta misma Directiva al ordenador de otra persona establecida en un Estado miembro B, a solicitud de esta última, para ser almacenados en la memoria de este ordenador y ser visualizados en su pantalla, constituye un acto de “reutilización” de dichos datos por parte de la persona que ha realizado tal envío. Debe considerarse que este acto ha tenido lugar, al menos, en el Estado miembro B cuando existan indicios que permitan concluir que tal acto pone de manifiesto la intención de su autor de dirigirse a los miembros del público establecidos en este último Estado miembro, extremo este que corresponde verificar al órgano jurisdiccional nacional* (apartado 47 de la cuestión prejudicial).

<sup>101</sup> El derecho de acceso es una pieza fundamental del derecho a la protección de datos, debido a que si un sujeto no puede acceder a la información que administra un responsable sobre ella, se va a imposibilitar la oportunidad de ejercitar los derechos para la defensa de sus datos. En este sentido se pronunció el TJUE en la STJUE de 7 de mayo de 2009, asunto C-553/07, *College van burgemeester en wethouders van Rotterdam* (ECLI:EU:C:2009:293). *El citado derecho de acceso es indispensable para que el interesado pueda ejercer los derechos que se contemplan en el art. 12, letras b) y c), de la Directiva, a saber, en su caso, cuando el tratamiento no se ajuste a las disposiciones de la misma, obtener del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de los datos (letra b), o que proceda a notificar a los terceros a quienes se hayan comunicado los datos, toda rectificación, supresión o bloqueo efectuado, si no resulta imposible o supone un esfuerzo desproporcionado (letra c)* (apartado 51). Sobre este pronunciamiento *vid.* CORTÉS MARTÍN, J. M.: “Jurisprudencia del TJCE, Mayo-Agosto 2009”, *Revista de Derecho Comunitario Europeo*, 2009, pp. 1109-1178.

<sup>102</sup> STJUE de 12 de julio de 2011, asunto C-324/09, *L’Oréal SA* (ECLI:EU:C:2011:474). Litigio entre, por un lado, L’Oréal SA y sus filiales Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie y L’Oréal (UK) Ltd y, por otro lado, tres filiales de eBay Inc. eBay International AG, eBay Europe SARL y eBay (UK) Ltd, el Sr. Potts, la Sra. Ratchford, la Sra. Ormsby, el Sr. Clarke, la Sra. Clarke, el Sr. Fox y la Sra. Bi, en relación con la comercialización, sin el consentimiento de L’Oréal, de productos de esta a través del mercado electrónico gestionado por eBay. *La simple posibilidad de acceder, en un determinado territorio nacional, al sitio de Internet en el que se encuentran los datos en cuestión no basta para concluir*

Directiva 95/46/CE<sup>103</sup> (actualmente derogada por el RGPD).

Dicho de otro modo, en una transferencia internacional de datos resulta esencial la existencia de un traslado o movimiento de datos personales, se requiere por lo tanto un comportamiento activo<sup>104</sup> por parte del emisor al transferir los mismos, excluyendo de esta idea el supuesto en el que desde una posición pasiva en un tercer Estado<sup>105</sup> se acceda a información publicada en una *Web*.

## II. Sujetos

Una vez detallado el concepto de transferencia internacional de datos, procedemos a estudiar, desde una óptica subjetiva, cuáles son los sujetos que participan en una transferencia internacional de datos, teniendo en consideración si existe una situación de desamparo jurídico en alguno de ellos:

---

*que la persona que explota este sitio lleva a cabo un acto de reutilización al que resulta de aplicación el Derecho nacional que rige en este territorio en materia de protección a través del derecho sui generis (apartado 64).*

<sup>103</sup> Una vez más, el TJUE actúa como instrumento de integración europeo, resaltando, en el presente caso, el carácter de normación completa de la Directiva, y no mínima, que puede ser desarrollada por los Estados miembros. Éstos podrán internamente regular aquellas situaciones no comprendidas en el ámbito de aplicación de esta última y cuando ninguna otra norma de Derecho comunitario se oponga a ello. PULIDO QUECEDO, M.: “La catequista y los riesgos de Internet”, *Actualidad Jurídica Aranzadi*, núm. 602, 2003, p. 15.

<sup>104</sup> STJUE 6 de noviembre de 2003, asunto C-101/01, *Bodil Lindqvist* (ECLI:EU:C:2003:596). Estas cuestiones se suscitaron en el marco de un proceso penal seguido ante dicho órgano jurisdiccional contra la Sra. Lindqvist, acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio Internet diversos datos de carácter personal sobre varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia. *De los autos se desprende que, para obtener la información que figura en las páginas Web en las que la Sra. Lindqvist había introducido datos relativos a sus compañeros, un usuario de Internet debía no sólo conectarse sino también realizar, a iniciativa propia, las acciones necesarias para consultar dichas páginas. En otras palabras, las páginas Web de la Sra. Lindqvist no contenían los mecanismos técnicos que permiten el envío automático de la información a personas que no hayan buscado deliberadamente acceder a dichas páginas* (apartado 60). Con relación a esta sentencia *vid.* DE MIGUEL ASENSIO, P. A.: “Avances en la interpretación de la normativa comunitaria sobre protección de datos personales”, *Diario La Ley*, núm. 5964, 2004, pp. 1-8; PARDOLESI, R.: “Il codice in materia di protezione dei dati personali e l'intangibilità della "privacy" comunitaria”, *Il Foro italiano*, núm. 4, 2004, pp. 59-64.

<sup>105</sup> ZABÍA DE LA MATA, J.: *Protección de datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008, pp. 581-582.

Titular de los datos: Es el afectado<sup>106</sup>, es decir, la persona física titular<sup>107</sup> de la información que es susceptible de una transmisión de datos personal e ilícita. En este sentido, es el titular del derecho fundamental a la protección de datos recogido en el art. 8 de la Carta de los Derechos Fundamentales de la UE<sup>108</sup>. Ciertamente, la privacidad<sup>109</sup> está consolidada como derecho humano puesto que garantiza otros derechos como el de acceder a un trabajo, servicios o créditos.

Exportador: Es el promotor, puede tratarse de una persona física o jurídica, pública o privada o incluso un órgano administrativo que envíe los datos personales a otro Estado.

Importador: Es el receptor, por lo tanto, admite la misma diversidad de posibilidades que el exportador.

Ambos (exportador e importador<sup>110</sup>) son empresarios cuya actividad consiste en la captación, tratamiento y procesamiento de la información que administran en ficheros de datos con el propósito de promover una transferencia de datos de carácter personal. Como consecuencia, *se crea un subconcepto para referirse con mayor precisión al empresario responsable establecido en la UE que promueve una transferencia internacional a un tercer Estado (que se denomina exportador) dirigida a un empresario*

---

<sup>106</sup> *La potencial pluralidad de ordenamientos jurídicos implicados en la protección de la correcta circulación internacional de datos de naturaleza personal y la existencia en sí de transferencias internacionales de tales datos, consecuencia del creciente carácter internacional de las relaciones personales y comerciales, exige la intervención del Derecho Internacional Privado.* ORTEGA GIMÉNEZ, A.: “La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en Derecho Internacional Privado español”, *Diario La Ley*, núm. 8661, 2015, versión online.

<sup>107</sup> STC 292/2000 de 30 de noviembre (ECLI:ES:TC:2000:292). Establece que el derecho fundamental a la protección de datos atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la ley (apartado 5).

<sup>108</sup> Art. 8.1 Carta de los Derechos Fundamentales de la UE (2016/C 202/02): *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.* DOUE C 83/389, 30-III-2010.

<sup>109</sup> STC 292/2000 de 30 de noviembre (ECLI:ES:TC:2000:292). Detalla la naturaleza del derecho a la privacidad. Blinda determinada información de carácter personal que, debido a su naturaleza de poder ser procesados por medios informáticos, exponen información del individuo pudiendo vulnerar sus derechos. *El que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo* (apartado 6).

<sup>110</sup> El art. 3 de Decisión de la Comisión de 5 de febrero de 2010, atribuye una definición a cada uno de estos sujetos, siendo el exportador de datos *el responsable del tratamiento que transfiera los datos personales*; y el importador *el encargado del tratamiento establecido en un tercer país que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de este, de conformidad con sus instrucciones y los términos de la presente decisión* (fecha de consulta: 18-10-2018) <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32010D0087>.

*receptor establecido en ese lugar (que denominamos importador), con independencia de que este último vaya a actuar como responsable o un encargado*<sup>111</sup>.

En suma, resulta clara la posición de desamparo o desprotección del titular del derecho a la protección de datos en un contexto en el que ha sufrido un tratamiento ilícito internacional de sus datos respecto al exportador e importador puesto que dispone de instrumentos menos eficientes frente a su actuación.

### **III. Sistema de competencia judicial internacional.**

#### **1. Regímenes normativos**

En el ámbito de los daños a los derechos de la personalidad no existen normas internacionales específicas que regulen la competencia judicial internacional, en contraste con otros campos del sector de obligaciones extracontractuales (hechos lesivos en el medio ambiente<sup>112</sup>). *Esta ausencia también es patente en el régimen de la UE y en la mayoría de los sistemas nacionales de Derecho Internacional Privado, este es el caso del sistema español, pues el régimen interno de competencia judicial internacional recogido en la LOPJ (art. 22 para el orden jurisdiccional civil) no prevé regla específica para este tipo de litigios*<sup>113</sup>.

En consecuencia con lo expuesto en el párrafo anterior, procedemos a analizar las reglas de competencia ante un supuesto de lesión internacional de estos derechos: a) El sistema Bruselas (RBI *bis*/ RBI) y el Convenio de Lugano (CL)<sup>114</sup> como sistema básico europeo de competencia judicial internacional y reconocimiento de decisiones en materia civil y mercantil y b) el sistema español de fuente interna de competencia judicial internacional (LOPJ)<sup>115</sup> caracterizado por su aplicabilidad subsidiaria en ausencia de mecanismo europeo y convencional.

---

<sup>111</sup> SANCHO VILLA, D.: *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor, 2010, p. 27.

<sup>112</sup> CRESPO HERNÁNDEZ, A.: *La responsabilidad civil derivada de la contaminación transfronteriza ante la jurisdicción estatal*, Eurolex, Madrid, 1999, p. 88.

<sup>113</sup> CORDERO ÁLVAREZ, C. I.: *Litigios internacionales sobre difamación y derechos de la personalidad*, Dykinson, Madrid, 2015, p. 81.

<sup>114</sup> El nuevo Convenio de Lugano fue firmado el 30 de octubre de 2007 en Lugano, entre los Estados de la Comunidad Europea y los países EFTA. Hace alusión a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil. *DOUE L 337/68, 21-XII-2007*.

<sup>115</sup> Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *BOE* núm. 157, 02-VII-1985.

#### A) RBI *bis*

El sistema de competencia judicial internacional del RBI *bis* está dirigido a las demandas interpuestas con posterioridad al 10 de enero de 2015. Este Reglamento mantiene la misma línea que la versión anterior, sin modificar el ámbito material en procedimientos que versen sobre violación de los derechos de la personalidad. En relación con el criterio de aplicación espacial, y a diferencia de lo previsto en el RBI<sup>116</sup>, los criterios de competencia judicial internacional se van a extender a los domiciliados en terceros Estados (Art. 6.1 RBI *bis*<sup>117</sup>) en las siguientes materias: contratos individuales de trabajo, contratos de consumo y los casos en los que las partes están facultadas para elegir un tribunal de un Estado miembro. En particular, la aplicación del art. 6 RBI *bis* es viable cuando el daño sobre un derecho de la personalidad esté vinculado con la prestación de servicios *online* en un contrato de consumo<sup>118</sup>.

Los criterios de competencia no exclusivos regulados en el sistema RBI/RBI *bis* por los que los tribunales europeos se van a pronunciar en estos procedimientos son: el foro general del domicilio del demandado (art. 4 RBI *bis*/ art. 2 RBI/CL), autonomía de voluntad de las partes o foros de sumisión expresa o tácita (arts. 25 y 26 RBI *bis*, arts. 23 y 24 RBI/CL) y el lugar donde se ha producido o pudiera producirse el daño (art. 7.2 RBI *bis*, art. 5.3 RBI/CL). Además, debemos mencionar el posible recurso a los foros por conexidad procesal del art. 8 RBI *bis* (art. 6 RBI/CL).

#### B) Sistema de fuente interna (LOPJ).

El sistema interno de competencia judicial internacional de los tribunales españoles se regula en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Ahora bien, debemos poner de relieve que su aplicación es subsidiaria ya que la legislación europea y los Convenios internacionales son de aplicación preferente<sup>119</sup> sobre la LOPJ.

---

<sup>116</sup> A diferencia de lo dispuesto en la nueva versión del Reglamento, en el art. 4 RBI los instrumentos de competencia judicial internacional de fuente interna solo podrán aplicarse cuando el demandado tenga su domicilio fuera de la UE: *Si el demandado no estuviere domiciliado en un Estado miembro, la competencia judicial se regirá, en cada Estado miembro, por la ley de este Estado miembro, sin perjuicio de la aplicación de lo dispuesto en los artículos 22 y 23. DOUE L 12/1, 16-I-2001.*

<sup>117</sup> Art. 6.1 RBI *bis*: *Si el demandado no está domiciliado en un Estado miembro, la competencia judicial se regirá, en cada Estado miembro, por la legislación de ese Estado miembro, sin perjuicio de lo dispuesto en el artículo 18, apartado 1, el artículo 21, apartado 2, y los artículos 24 y 25.*

<sup>118</sup> AÑOVEROS TERRADAS, B.: “Extensión de los foros de protección del consumidor a demandados domiciliados en terceros Estados”, *Agencia Española de Derecho Internacional Privado*, tomo IX, 2009, pp. 285-306.

<sup>119</sup> Art. 96.1 CE. *Los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno. Sus disposiciones sólo podrán ser derogadas,*

En este caso, la opción de acudir a la LOPJ por los tribunales españoles se restringe a los casos en los que la parte demandada tenga su domicilio fuera de la UE, excepto que nos encontremos ante un contrato de consumo y no resulte viable ningún instrumento convencional.

Los foros de competencia en el ámbito civil relativo a litigios sobre derechos de la personalidad (materia contractual y extracontractual) se detallan en el art. 22 LOPJ. La regla de competencia judicial internacional más representativa en este tipo de procedimientos judiciales es la reflejada en el art. 22.3 LOPJ de obligaciones extracontractuales. En los mismos términos que el sistema europeo, el punto de referencia es el lugar del daño, atribuyendo la competencia a los órganos españoles cuando la obligación se haya originado en España. No obstante, también se regula la opción de atribuir competencia judicial a la jurisdicción nacional de la residencia habitual común de la víctima y autor del daño.

## 2. Acciones ejercitables por la víctima

El sujeto que ha sido víctima<sup>120</sup> de una vulneración de sus derechos de la personalidad tiene a su disposición una serie de acciones<sup>121</sup> en virtud del Derecho material aplicable. La acción de reparación o resarcitoria es la acción más representativa en los sistemas jurídicos nacionales y está enfocada a obtener una reparación del daño. Más concretamente, se trata de la condena consistente en el pago de una indemnización.

---

*modificadas o suspendidas en la forma prevista en los propios tratados o de acuerdo con las normas generales del Derecho internacional.*

Art. 21.1 LOPJ. *Los Tribunales civiles españoles conocerán de las pretensiones que se susciten en territorio español con arreglo a lo establecido en los tratados y convenios internacionales en los que España sea parte, en las normas de la Unión Europea y en las leyes españolas.*

<sup>120</sup> *La prestación de servicios tecnológicos en la nube, sobre la base de la existencia o no de una vinculación jurídica entre el causante del daño y el afectado, puede dar lugar a la exigencia de responsabilidad civil contractual (cuando entre el autor y la víctima hubiere existido una previa relación contractual y se hubiere producido un incumplimiento de lo pactado –responsabilidad derivada de un contrato de prestación de servicios en la nube–), o extracontractual (exigencia de una indemnización por los daños y perjuicios ocasionados –responsabilidad no contractual por vulneración del derecho a la protección de datos personales derivada de la computación en nube–).* ORTEGA GIMÉNEZ, A.: “Cloud computing, protección de datos y Derecho Internacional Privado (resolución de controversias y determinación de la ley aplicable)”, MARTÍNEZ MARTÍNEZ, R. (Dir.), *Derecho y cloud computing*, Aranzadi, Cizur Menor, 2012, p. 271.

<sup>121</sup> *En materia de transferencias internacionales de datos: se amplía la lista de posibles instrumentos para ofrecer garantías, incluyéndose expresamente, entre otros, las Normas Corporativas Vinculantes para responsables y encargados, los códigos de conducta y esquemas de certificación, así como los cláusulas contractuales modelo que puedan aprobar las autoridades de protección de datos (fecha de consulta: 27-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.*

Otra opción consiste en ejercitar acciones cuyo propósito es eliminar un comportamiento lesivo (acción de cesación) o solicitar medidas preventivas para evitar posibles perjuicios en un futuro (acción de prohibición). La cuestión aquí es que estas dos acciones<sup>122</sup> se pueden iniciar de forma independiente o de un modo coetáneo a la acción de reparación de daños. Consecuentemente, debemos diferenciar las medidas provisionales y/o cautelares de las de cesación. Mientras que las primeras son accesorias y dependen directamente de un procedimiento principal sobre el fondo, las de cesación o prohibición son autónomas, si bien como he mencionado anteriormente cabe el ejercicio coetáneo.

### 3. Elección del tribunal competente

Tomando como punto de partida el sistema jerárquico de foros regulado en el RBI-RBI *bis*/CL, analizaremos la sumisión tácita y expresa debido a su aplicabilidad preferente respecto del foro general del domicilio del demandado y foro especial por razón de la materia. Sin embargo, en la práctica, la autonomía jurisdiccional (voluntad de las partes) como medio de atribución de competencia se limita a casos muy restringidos en el ámbito de la responsabilidad extracontractual. El motivo se debe a la complejidad de pactar la jurisdicción competente por las partes, independientemente de que el acuerdo se constituya antes o después de que se origine la controversia. Es claro pues, que las obligaciones extracontractuales nacen en ausencia de previa relación entre las partes por lo que no ha existido opción de pacto previo en la mayoría de los casos.

La autonomía de la voluntad (sumisión expresa y tácita) como criterio de competencia resulta viable en el marco del RBI *bis*/ CL, cuando no nos encontremos ante contratos en los que una de las partes figure en una posición de inferioridad<sup>123</sup> o una materia de competencia exclusiva de un Estado miembro. En este sentido, las partes deben encontrarse en la misma posición sin prevalencia de la una sobre la otra por la seguridad

---

<sup>122</sup> *Conviene señalar los dos condicionantes cumulativos que han sido objeto de introducción en el Reglamento, esto es, en un primer término, la necesidad de ofrecer garantías adecuadas, y, en un segundo término, la imperiosa obligación de que los interesados dispongan de “derechos exigibles” y “acciones legales efectivas”, traduciéndose ello en un intento de reforzar las garantías de las que disponen los afectados sobre el control de sus datos personales.* CASTELLANOS RODRÍGUEZ, A.: “El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield”, *Institut de Ciències Polítiques i Socials*, núm. 350, 2017, p. 10.

<sup>123</sup> Contrato de consumo, art. 19 RBI *bis*. *Únicamente prevalecerán sobre las disposiciones de la presente sección los acuerdos: que permitan al consumidor formular demandas ante órganos jurisdiccionales distintos de los indicados en la presente sección.*

jurídica que esto supone.

#### 4. Foro del domicilio del demandado

El foro general del domicilio del demandado está consolidado como instrumento base de atribución de competencia judicial internacional en la UE (art. 4 RBI *bis*<sup>124</sup>, art. 2 RBI/CL) y en la mayoría de las legislaciones internas de los Estados miembros (art. 22.2 LOPJ-22 *ter*, versión revisada). Desde esta perspectiva, en la práctica este foro se presenta como una solución más viable que la sumisión en el ámbito de la responsabilidad civil extracontractual. De esta manera, se facilita la competencia a los tribunales del domicilio del demandado<sup>125</sup>, al margen del medio empleado para la comisión del daño y del lugar donde se originó o materializó el perjuicio. De hecho, facilita la concentración de acciones en una única jurisdicción frente a un mismo sujeto, siendo especialmente llamativo cuando el medio empleado es de carácter global (Internet) y va a derivar en una difusión masiva de contenidos lesivos.

Desde la óptica del alcance de la competencia, el domicilio del demandado atribuye al tribunal competencia ilimitada para pronunciarse sobre la totalidad de daños sufridos por el perjudicado, al margen de donde se hayan materializado, o donde se haya producido la actuación originaria (que a veces no se corresponde con el domicilio del demandado). Al amparo del art. 7.2 RBI *bis*<sup>126</sup>, el Estado donde se ha materializado el daño ostenta una facultad limitada para pronunciarse sobre los sucesos que han tenido

---

<sup>124</sup> STJCE de 17 de noviembre de 2011, asunto C-327/10, *Hypoteční banka a.s* (ECLI:EU:C:2011:745). Litigio entre Hypoteční banka a.s. y el Sr. Lindner, con domicilio actual desconocido, dirigido a obtener el pago de una cantidad de aproximadamente 4,4 millones de coronas checas correspondiente a cuotas impagadas de un crédito hipotecario que la primera había concedido al segundo. *En una situación como la controvertida en el litigio principal, en la que un consumidor que ha firmado un contrato de préstamo inmobiliario de larga duración, el cual establece la obligación de informar a la otra parte contratante de todo cambio de domicilio, renuncia a su domicilio antes de la interposición de una acción en su contra por incumplimiento de sus obligaciones contractuales, los tribunales del Estado miembro en el que se encuentre el último domicilio conocido del consumidor son competentes* (apartado 57). En relación con la presente resolución *vid.* AÑOVEROS TERRADAS, B.: “Consumidor con domicilio desconocido. ¿Hasta dónde llega la protección? A propósito de la sentencia del TJCE (Sala Primera) de 17 de noviembre de 2011, (C-327/10, Hypoteční banka a.s. contra Udo Mike Lindner)”, *Diario La Ley*, núm. 7870, 2012, pp. 4-8.

<sup>125</sup> STJCE de 15 de marzo de 2012, asunto C-292/10, *Cornelius de Visser* (ECLI:EU:C:2012:142). Para mayor abundamiento *vid.* COSLIN, C.: “Récents éclairages sur la compétence des tribunaux en matière de délits prétendument commis sur Internet”, *Droit de l’immatériel: informatique, médias, communication*, núm. 90, 2013, pp. 33-35.

<sup>126</sup> Art. 7.2 RBI *bis*. *Una persona domiciliada en un Estado miembro podrá ser demandada en otro Estado miembro: 2) en materia delictual o cuasidelictual, ante el órgano jurisdiccional del lugar donde se haya producido o pueda producirse el hecho dañoso.*

lugar en su jurisdicción. Así, *el foro del domicilio del demandado se presenta como una opción más adecuada para la víctima, pues para llegar al mismo resultado: el resarcimiento/compensación por todos los daños y perjuicios sufridos, en el primero de los casos debería de litigar en cada uno de los Estados donde el daño se hubiera manifestado, mientras que dirigiéndose al lugar del domicilio del demandado le sirve con el ejercicio de una única acción global*<sup>127</sup>. Sin embargo, debemos diferenciar el lugar de origen del daño (7.2 RBI *bis*), vinculado con el establecimiento del emisor de contenidos y el centro principal de intereses de la víctima, caracterizado por disponer de una competencia general. Si bien, el sujeto perjudicado ha de analizar estas dos alternativas (lugar de origen del daño/domicilio del demandado), partiendo de la base de que ambas son foros de competencia universal y debiendo valorar, por tanto, cuál de ellas se ajusta más a sus expectativas.

Una vez reflejados los beneficios asociados al foro del domicilio del demandado, debemos matizar que su aplicabilidad es más bien excepcional, y es que pasan a ser muy puntuales los litigios que versen sobre vulneraciones de los derechos de la personalidad en Internet tramitados por el tribunal del domicilio del demandado. En primer lugar, esto se debe al elevado coste de la internacionalidad del litigio, coste que la víctima va a asumir en su totalidad. Esta situación se acentúa cuando el daño se ha efectuado mediante un medio masivo, apto para producir una lesión en una pluralidad de puntos geográficos distantes entre sí.

Acerca de los perjuicios ocasionados vía *online*, es frecuente que el servidor donde se integra la *Web* con los datos lesivos se localice en un Estado miembro que no sea el del domicilio, pudiendo afectar al ejercicio de las acciones de cesación y/o prohibición en comportamientos transfronterizos emitidos en un medio virtual. En este contexto, a pesar del alcance, en teoría ilimitado, del tribunal del domicilio del demandado, podemos encontrarnos con obstáculos en el momento de materializar la medida (cesación o prohibición) en un tribunal que no sea el de la jurisdicción del foro. En este escenario, debemos acudir al foro del art. 35 RBI *bis*<sup>128</sup>, que atribuye competencia judicial internacional concreta a los Estados miembros para ejecutar las medidas judiciales

---

<sup>127</sup> CORDERO ÁLVAREZ, C. I.: *Litigios internacionales sobre difamación y derechos de la personalidad*, Dykinson, Madrid, 2015, p. 101.

<sup>128</sup> Art. 35 RBI *bis*. *Podrán solicitarse a los órganos jurisdiccionales de un Estado miembro medidas provisionales o cautelares previstas por la ley de dicho Estado miembro, incluso si un órgano jurisdiccional de otro Estado miembro es competente para conocer del fondo del asunto.*

cautelares con independencia del Estado miembro en el que se siga la causa principal. A diferencia de las medidas judiciales cautelares, cuando la medida pretendida sea una acción de fondo, es preferible acudir al foro especial del lugar del daño siempre que se corresponda con la ubicación donde ha de materializarse la medida.

## 5. Foro del lugar del daño

El *forum delicti commissi* (foro del lugar del daño) como instrumento de selección del tribunal competente europeo en el ámbito delictual (art. 7.2 RBI *bis*), refleja una serie de problemas a la hora de localizar el hecho lesivo. Conviene subrayar que Internet, como vía masiva de comunicación, contribuye a deslocalizar el lugar donde se ha producido el daño y esto se debe a la diferencia espacial entre el punto geográfico de actuación originaria y el lugar de consecución. Se debe agregar las limitaciones vigentes en el entorno virtual características de los otros mecanismos de competencia generales como es el foro del domicilio del demandado.

Por otra parte, para la correcta aplicación de este foro, debemos hacer alusión al principio de proximidad<sup>129</sup>, como conexión entre el litigio y la jurisdicción y como medio habilitante para desplazar la regla general de competencia del domicilio del demandado y facilitar a la víctima el lugar donde ejercitar su acción. Al mismo tiempo, debemos referirnos al principio de previsibilidad del tribunal competente para el eventual responsable, que se traduce en la consagración de determinados principios procesales convencionales como es el art. 6 CEDH<sup>130</sup>.

En relación con la delimitación y alcance de esta regla (art. 7.2 RBI *bis*), la jurisprudencia del TJUE ha destacado su naturaleza residual, y es que solo se va a aplicar

---

<sup>129</sup> STJCE de 11 de septiembre de 1995, asunto C-364/93, *Marinari* (ECLI:EU:C:1995:289). A tenor de lo dispuesto en el presente pronunciamiento *vid.* BRIGGS, A.: “The Uncertainty of Special Jurisdiction”, *Lloyd's Maritime and Commercial Law Quarterly*, 1996, pp. 27-29; HARTLEY, TREVOR: “Article 5: Place Where the Harmful Event Occurs”, *European Law Review*, 1996, pp. 164-166; BORRÁS RODRÍGUEZ, A.: “Jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, *Revista Jurídica de Catalunya*, 1996, pp. 613-615; SARAVALLE, A.: “Evento dannoso e sue conseguenze patrimoniali: giurisprudenza italiana e comunitaria a confronto”, *Il Foro italiano*, núm. 4, 1996, pp. 341-348.

<sup>130</sup> Art. 6.1 CEDH. *Toda persona tiene derecho a que su causa sea oída equitativa, públicamente y dentro de un plazo razonable, por un Tribunal independiente e imparcial, establecido por la Ley, que decidirá los litigios sobre sus derechos y obligaciones de carácter civil o sobre el fundamento de cualquier acusación en materia penal dirigida contra ella.* BOE núm. 243, 10-X-1979. Este precepto refleja la consolidación de un conjunto de principios procesales que vienen a garantizar el derecho de acceso a la justicia a través de un equilibrio entre las partes así como un foro de competencia justo para el demandado.

a obligaciones no integradas en el art. 5.1 RBI<sup>131</sup>/ 7.1 RBI bis referido a obligaciones contractuales<sup>132</sup>. *La regla de competencia del art. 5.3 RBI/7.2 RBI bis comprende no solo las acciones resarcitorias relativas a daños y perjuicios ya materializados sino también el ejercicio de acciones preventivas de prohibición o cesación de actividades para la tutela de estos derechos, esto es, medidas de carácter previo a la materialización del daño*<sup>133</sup>. *La cuestión aquí es concretar ese lugar del riesgo con carácter previo (ya sea del acto de origen o de materialización del daño) dada la multiplicidad de posibles jurisdicciones en las que podrían potencialmente manifestarse el riesgo del daño*<sup>134</sup>.

---

<sup>131</sup> STJUE de 5 de febrero de 2004, asunto C-18/02, *DFDS Torline A/S* (ECLI:EU:C:2004:74). Litigio entre Danmarks Rederiforening (asociación de armadores daneses), que actúa en nombre de DFDS Torline A/S, que es un armador, y la LO Landsorganisationen i Sverige (Confederación General del Trabajo sueca), que actúa en nombre de SEKO, que es un sindicato, en relación con la legalidad de una acción colectiva cuyo preaviso fue notificado por este último contra DFDS. *El Tribunal de Justicia ha declarado ya que no puede acogerse la interpretación del art. 5, núm. 3, del Convenio de Bruselas según la cual la aplicación de dicha disposición está subordinada a que se produzca efectivamente el daño y que la afirmación de que el órgano jurisdiccional del lugar donde se ha producido el hecho dañoso es normalmente el más adecuado para conocer del asunto, sobre todo por motivos de proximidad del litigio y de facilidad para la práctica de la prueba, es igualmente válida tanto si el litigio tiene por objeto la reparación de un perjuicio que ya se ha producido como si el objeto de la acción se dirige a impedir que se produzca el daño* (apartado 27).

<sup>132</sup> STJUE 17 de junio de 1992, asunto C-26/91, *Jakob Handte et Cie GmbH* (ECLI:EU:C:1992:268). Litigio entre la empresa Jakob Handte et Cie GmbH, con domicilio social en Tuttlingen (Alemania) y la sociedad anónima Traitements mécanochimiques des surfaces, con domicilio social en Bonneville. *En efecto, además de la circunstancia de que el fabricante no tiene relación contractual alguna con el comprador y no asume ninguna obligación contractual respecto de este comprador, cuyos domicilio e identidad puede ignorar legítimamente, resulta que, en la mayor parte de los Estados contratantes, la responsabilidad del fabricante frente al comprador por vicios de la cosa vendida no está considerada como de naturaleza contractual* (apartado 20). Sobre este pronunciamiento *vid.* BORRÁS RODRÍGUEZ, A.: “Jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, *Revista Jurídica de Catalunya*, 1993, pp. 259-262; DECKER, M.: “Contract or Tort: A Conflict of Characterisation”, *International and Comparative Law Quarterly*, 1993, pp. 366-369.

<sup>133</sup> STJCE de 1 de octubre de 2002, asunto C-167/00, *Karl Heinz Henkel* (ECLI:EU:C:2002:555). Litigio entre el Verein für Konsumenteninformation, asociación austriaca con domicilio social en Austria, y el Sr. Henkel, nacional alemán domiciliado en Alemania, relativo al uso por este último, en contratos celebrados con consumidores austríacos, de cláusulas que el VKI considera abusivas. *La regla de competencia especial contenida en el art. 5, núm. 3, del Convenio de Bruselas se basa en la existencia de una conexión particularmente estrecha entre la controversia y el órgano jurisdiccional del lugar en que se ha producido el hecho dañoso, que justifica una atribución de competencia a dicho órgano jurisdiccional por razones de buena administración de la justicia y de sustanciación adecuada del proceso* (apartado 46).

<sup>134</sup> CORDERO ÁLVAREZ, C. I.: *Litigios internacionales sobre difamación y derechos de la personalidad*, Dykinson, Madrid, 2015, p. 132.

## IV. Legislación aplicable en el marco de una transferencia internacional ilícita de datos

### 1. El Reglamento Roma II

El Reglamento (CE) núm. 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007 (Roma II), relativo a la ley aplicable a las obligaciones extracontractuales dispone de un criterio amplio: la vinculación con el Estado en el que se ha ocasionado el perjuicio, de otros mecanismos más específicos y en concreto de una cláusula de escape, que nos permite desvincularnos de estas reglas más concretas cuando el daño se haya manifestado en otro país<sup>135</sup>.

Puede interpretarse que nos encontramos ante una norma de carácter universal, que podemos integrar en el objetivo de asegurar un funcionamiento adecuado del mercado europeo, en la importancia de proporcionar una solución única para el conjunto de jueces nacionales y en la posible proyección intracomunitaria de todas las relaciones internacionales. En consecuencia, debido a este componente universal se ha consolidado la determinación uniforme de la ley aplicable a las obligaciones extracontractuales<sup>136</sup>, al margen del tribunal nacional que haya tramitado el litigio. En este contexto, se ha derivado en un aumento en la previsibilidad jurídica de las partes, puesto que pueden conocer con cierta probabilidad la legislación que será de aplicación en su litigio.

El problema se plantea, precisamente, porque el ilícito internacional de datos<sup>137</sup> personales no se ha incorporado en la aplicación del Roma II: art. 1.2. *Se excluirán del ámbito de aplicación del presente Reglamento: g) las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación*, es por ello por lo que la alternativa se refleja en el art. 10.9 CC, que consolida como punto de conexión *la ley del lugar donde hubiere ocurrido el hecho de que deriven*<sup>138</sup>. Sin embargo, el art. 30 del Reglamento Roma II no

---

<sup>135</sup> CALVO CARAVACA, A. L./ AREAL LUDEÑA, S.: *Cuestiones actuales del derecho mercantil internacional*, Colex, Madrid, 2005, p. 531.

<sup>136</sup> PALAO MORENO, G.: *Responsabilidad civil extracontractual en el derecho europeo*, Tirant lo Blanch, Valencia, 2008, p. 32.

<sup>137</sup> *Resulta aquí relevante lo ya señalado en relación con la responsabilidad derivada de los daños a la personalidad, en particular los supuestos de difamación, en Internet, incluido el hecho de que no es aplicable el Reglamento Roma II, en virtud de lo dispuesto en su art. 1.2 g) que excluye su aplicación a las "las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad", por lo que todavía resulta de aplicación el art. 10.9 CC.* DE MIGUEL ASENSIO, P.: *Derecho Privado de Internet*, Civitas, Madrid, 2015, p. 65.

<sup>138</sup> El criterio de base es que la ley aplicable es la del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado, típicamente su residencia habitual, sin perjuicio de que en la medida en que pueda

descarta la opción de que la Comisión europea recoja nuevas propuestas en este ámbito.

La polémica STJUE *eDate Advertising* derivó en la creación de una iniciativa: *Working Document on the amendment of Regulation (EC) núm. 864/2007 on the law applicable to non-contractual obligations Rome II*<sup>139</sup>, en el marco del Parlamento europeo que integraba la adopción de una concreta propuesta de reforma legislativa del Reglamento Roma II. Esta propuesta tiene su origen en la ausencia de un adecuado sistema de protección frente al atentado contra los derechos que afectan a la personalidad (derecho a la intimidad y a la protección de datos), así como en el propósito de suplir este vacío legal mediante un precepto 5 a) en el Reglamento Roma II<sup>140</sup>. Con todo, este propósito de adquirir una unificación<sup>141</sup> en la legislación europea aplicable se explica desde el aumento en las acciones que involucran a un conjunto de Estados en materia de difusión de datos vía Internet. Aun así, ello no obsta a que esta iniciativa haya planteado serios interrogantes relativos al lugar de materialización del daño como punto de conexión.

Sin dejar al margen las consideraciones anteriores, hemos de resaltar dos puntos que merecen una especial consideración en esta propuesta. En primer lugar, se ha incluido una “cláusula de escape” dirigida a potenciales responsables en estos procedimientos con la que se habilita la posibilidad de aplicar a sus posibles responsabilidades la legislación de su residencia habitual. En segundo término, debemos señalar la facultad atribuida a los

---

operar un criterio de alternatividad, como en ocasiones se admite en la interpretación del art. 10.9 CC, en determinadas situaciones podrá el demandante optar por invocar como lugar del daño alternativamente el del establecimiento del responsable del tratamiento en el marco del cual se desarrolle este. DE MIGUEL ASENSIO, P.: *Derecho Privado de Internet*, Civitas, Madrid, 2015, p. 65.

<sup>139</sup> Documento de Trabajo del Comité de Asuntos Legales del Parlamento Europeo. DT/836983EN.doc, de 23/05/2011.

<sup>140</sup> Art. 5 a) *Privacy and rights relating to personality: 1. The law applicable to a non-contractual obligation arising out of a violation of privacy or rights relating to the personality, including defamation, shall be the law of the country in which the most significant element or elements of the loss or damage occur or are likely to occur. 2. However, the law applicable shall be the law of the country in which the defendant is habitually resident if he or she could not reasonably have foreseen substantial consequences of his or her act occurring in the country designated by paragraph 1. DOUE L 199/1, 31-VII-2007.*

<sup>141</sup> En relación con la necesidad de unificar la legislación aplicable: *El 11 de abril de 1985 los ministros de la OCDE adoptaron la Declaración sobre flujos de datos transfronterizos. Esta declaración abordaba las cuestiones políticas que surgían del flujo de datos personales más allá de las fronteras nacionales como flujos de datos e información sobre actividades comerciales, flujos intraempresariales, servicios de información informatizada, e intercambios científicos y tecnológicos. Al adoptar esta declaración, los gobiernos de la OCDE reafirmaron su compromiso por desarrollar enfoques comunes ante las cuestiones de flujos de datos transfronterizos y, si se presenta la ocasión, desarrollar soluciones armonizadas* (fecha de consulta: 5-11-2018) <https://www.oecd.org/sti/ieconomy/15590267.pdf>.

litigantes<sup>142</sup> de elegir el ordenamiento jurídico que va a sustentar su vínculo extracontractual. Gracias a estos dos elementos se aporta previsibilidad para las partes y equilibrio en el procedimiento.

El art. 14 Reglamento Roma II<sup>143</sup> habilita al afectado y al autor del perjuicio la opción de elegir la ley aplicable, en base al principio de autonomía conflictual. No obstante, esta posibilidad de elección por las partes carece de aplicabilidad práctica debido a que solo opera con posterioridad al nacimiento del litigio y por ello es inusual que se evite una situación de desprotección del perjudicado mediante una tutela adaptada y eficiente.

En conclusión, la ausencia de una reglamentación normativa europea y convencional ha desembocado en la necesidad de acudir a vías legislativas más clásicas, en nuestro caso al art. 10.9 CC.

## 2. El artículo 10.9 del Código Civil

Cuando los órganos judiciales españoles confirmen su competencia para resolver una pretensión relativa a la violación del derecho a la protección de datos en el contexto de una transferencia internacional de datos ilícita y, ante una ausencia de reglamentación normativa eficiente de la UE, solo cabe acudir a la regulación prevista en el ámbito de obligaciones extracontractuales del art. 10.9 CC<sup>144</sup> (norma de conflicto bilateral de Derecho Internacional Privado Autónomo).

Así las cosas, la estructura del art. 10.9 CC opera en base a dos alternativas:

A) *Lex loci actus*: Aplicación de la ley de aquel Estado donde se ha manifestado el hecho del que procede la responsabilidad. Ahora bien, para localizar este Estado debemos tener presente un conjunto de ilícitos que han desembocado en un daño a ese

---

<sup>142</sup> El contenido del art. 45 RGPD se puede comparar con el que se recoge en el art. 2.1 del protocolo adicional al Convenio 108 del Consejo de Europa (BOE núm. 274, 15-XI-1985): *cada parte dispondrá que la transferencia de datos de carácter personal hacia un destinatario sometido a la jurisdicción de un Estado u organización que no sea Parte en el Convenio sólo podrá efectuarse si dicho Estado u organización garantiza un nivel de protección adecuado a la transferencia de datos prevista*. GUASCH PORTAS, V.: “La computación en nube y las transferencias internacionales de datos en el nuevo Reglamento de la UE”, *Revista de derecho Universidad Nacional Educación a Distancia*, núm. 20, Madrid, 2017, p. 338.

<sup>143</sup> Art. 14. *Libertad de elección I. Las partes podrán convenir someter la obligación extracontractual a la ley que elijan: a) mediante un acuerdo posterior al hecho generador del daño, o bien b) cuando todas las partes desarrollen una actividad comercial, también mediante un acuerdo negociado libremente antes del hecho generador del daño. La elección deberá manifestarse expresamente o resultar de manera inequívoca de las circunstancias del caso y no perjudicará los derechos de tercero.*

<sup>144</sup> ESLAVA RODRÍGUEZ, M.: “El Locus Delicti Commssi en los ilícitos contra la vida privada cometidos a través de Internet”, *Revista Iberoamericana de Derecho Informático*, núm. 34, 2002, p. 33.

derecho fundamental: *cada acto de agresión contra el derecho a la protección de datos debe considerarse verificado en el Estado donde realmente tiene lugar, que es donde despliega su resultado lesivo; esto es, el tratamiento automatizado de datos personales se rige por la ley del Estado en cuyo territorio tiene lugar dicho tratamiento de datos que ha provocado el daño. Es en este Estado donde se produce el ilícito el locus delicti (lugar del evento causal)*<sup>145</sup>.

Es de mencionar la importancia de conocer la localización de los ficheros de datos a la hora emplear la regla recogida en el párrafo anterior. En este sentido, es común que se ubiquen en un Estado distinto al del establecimiento del responsable. Además, debemos subrayar que la actividad de un tercero en otro Estado que provoca el daño no nos permite *per se* averiguar el origen del daño en el Estado de su establecimiento.

En definitiva, el objetivo de esta regla es *restaurar el equilibrio roto por el acto dañoso, imponiendo la obligación de reparar el daño causado. Así la obligación está ligada al hecho que la ha causado, el cual se localiza en el lugar donde se ha producido*<sup>146</sup>. Dicho de otro modo, el usuario afectado va a ser protegido por la legislación local y, a tenor de lo dispuesto en el art. 10.9 CC, será de aplicación la normativa española<sup>147</sup> cuando el responsable del fichero esté domiciliado en un tercer Estado (fuera de la UE) y cuando el tratamiento de datos se hubiera realizado en España

B) *Lex loci damni*: Aplicación de la ley de aquel Estado en el que se materializa el daño para las víctimas. Nos encontramos ante una regla de conexión especial y eficaz para conocer donde se ha producido la vulneración del derecho a la protección de datos. En términos generales, este lugar puede ser además su residencia habitual.

Desde esta perspectiva, la residencia habitual del perjudicado es con frecuencia el centro de las relaciones económicas y sociales sobre las cuales puede ocasionarse un atentado contra los derechos de la personalidad. En principio, la residencia habitual del perjudicado va a constituir un enlace con ciertas garantías para el autor del daño, por controlar los detalles personales de la víctima, como para el perjudicado, debido a la

---

<sup>145</sup> ORTEGA GIMÉNEZ, A.: *Transferencia internacional de datos de carácter personal ilícita*, Aranzadi, Cizur Menor, 2016, p. 154.

<sup>146</sup> FELIU ÁLVAREZ DE SOTOMAYOR, S.: “Competencia judicial internacional y ley aplicable a los supuestos de responsabilidad extracontractual de los intermediarios básicos de Internet”/ CAVANILLAS MÚGICA, S. (Coord.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Comares, Granada, 2005, p. 226.

<sup>147</sup> ROVIRA SUEIRO, M.E.: “Daños a los derechos de la personalidad”/ REGLERO CAMPOS, L. F. (Coord.), *Lecciones de responsabilidad Civil*, Cizur Menor, 2002, p. 557.

confianza que le brinda la protección del Estado donde reside. Así, nos va a facilitar la posibilidad de aplicar una sola ley en los casos en los que el perjuicio se haya sufrido en un conjunto de Estados. Para ilustrar mejor este supuesto, si se ha difundido información falsa relativa a la liquidez de un consumidor residente en España y que solicita un crédito en otro Estado, el *locus damni* se va a encontrar en ese tercer Estado.

En cualquier caso, en el ámbito de aplicación del art. 10.9 CC, la ley donde se efectúa el daño directo para el perjudicado es la ley de la residencia habitual del afectado, excepto que otra ley evidencie donde se ha producido el daño. Si el daño se manifiesta en una pluralidad de Estados, aplicaríamos cada legislación en función del alcance del daño en cada lugar.

Finalmente, es posible destacar que el art. 10.9 CC<sup>148</sup> ha generado un posicionamiento doctrinal abiertamente disconforme, no solo por manejar un supuesto de hecho excesivamente vago y ambiguo, sino que además se estructura en torno a una consecuencia jurídica que goza de aparente neutralidad pero que claramente evidencia una situación de inferioridad jurídica del interesado<sup>149</sup>. *La mayor crítica que se puede realizar al art. 10.9 del Código Civil es su tradicional ceguera material o neutralidad. Cuando se parte de una situación en la que una de las partes está en manifiesta inferioridad, la neutralidad, lejos de ser una virtud, se convierte en una potencial fuente de injusticia*<sup>150</sup>.

---

<sup>148</sup> Art. 10.9 CC. *Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven. La gestión de negocios se regulará por la ley del lugar donde el gestor realice la principal actividad. En el enriquecimiento sin causa se aplicará la ley en virtud de la cual se produjo la transferencia del valor patrimonial en favor del enriquecido.*

<sup>149</sup> REQUEJO ISIDRO, M.: *Artículo 10.9, Comentarios al Código Civil*, Lex Nova, Valladolid, 2010, pp. 91-92.

<sup>150</sup> ORTEGA GIMÉNEZ, A.: *Transferencia internacional de datos de carácter personal ilícita*, Aranzadi, Cizur Menor, 2016, p. 157.

## CONCLUSIONES

**PRIMERA.** El Reglamento regula la tutela civil del derecho a la protección de datos, es decir, incorpora un sistema paralelo a las reclamaciones ante las autoridades de control, elemento clave para hacer efectivo el derecho a una indemnización como consecuencia del perjuicio ocasionado por el responsable o encargado del tratamiento. Acorde con esta protección jurisdiccional, se han desarrollado reglas especiales de competencia judicial internacional que van a gozar de una aplicación preferente respecto del Reglamento Bruselas I *bis* y el ordenamiento jurídico interno de cada Estado. Aunque el ámbito territorial del RGPD deriva de la aplicación de sus preceptos por los tribunales nacionales, no obsta para que sea necesario fijar, en virtud de las reglas de conflicto, la ley aplicable a los ilícitos que generen responsabilidad civil.

**SEGUNDA.** El Reglamento contiene como foro principal el lugar donde el demandado haya fijado un establecimiento. Los artículos referidos a la delimitación del ámbito territorial, así como los tribunales del lugar de residencia del perjudicado, parten de un concepto extenso y flexible del término “establecimiento”. Se prevé una serie de preceptos especiales relativos a la conexión entre procedimientos judiciales que cuentan con una aplicabilidad limitada, que se reducen a los supuestos en los que se inicien acciones frente a las resoluciones que procedan de autoridades de control.

**TERCERA.** En el ámbito de las transferencias internacionales de datos, la normativa actual de competencia judicial internacional es insuficiente para velar por los intereses del perjudicado en un procesamiento internacional ilícito de su información personal. Por lo que se refiere a la autonomía de la voluntad y a la sumisión expresa, se trata de un sistema ineficiente cuando una de las partes se encuentra en una posición de inferioridad. Con respecto a la sumisión tácita, su viabilidad real es poco probable, y es que el demandante tiende a iniciar sus acciones legales ante los órganos del lugar donde reside. Además, el autor del hecho lesivo ante esta sumisión tácita trataría de impedir ser procesado por los tribunales del demandante, impugnando su competencia.

**CUARTA.** En ausencia de sumisión a la hora de optar por un tribunal competente, la alternativa entre foro general y especial no aporta a la víctima una defensa óptima de sus derechos. Esto es, el foro general del domicilio del demandado no va a favorecer al perjudicado ante una transferencia internacional de sus datos, no solo por el elevado coste

de litigación transfronteriza que deberá asumir en su totalidad, sino también por la distancia geográfica que separa al demandante del centro de intereses del autor de la lesión, distancia que se da en el intercambio masivo de información *online*.

**QUINTA.** El *fórum delicti commissi* (foro especial) es la vía más común en nuestro derecho nacional y en el comparado para elegir el órgano judicial competente en cuestiones de responsabilidad civil extracontractual. En cambio, deriva en los ya mencionados problemas relacionados con la deslocalización y desconcentración del perjuicio originado que obliga a la víctima de la transferencia ilícita a seguir un procedimiento al margen de su centro de intereses. Dicho lo anterior, la obtención de una protección eficiente va a exigir la interpretación del foro especial en beneficio del perjudicado partiendo de su residencia habitual, que ha de ser entendida como el punto de referencia global de la actuación originaria de la responsabilidad civil extracontractual.

**SEXTA.** La aplicación del art. 10.9 del CC genera un contexto de inseguridad jurídica por no aportar a la víctima de una transferencia ilícita de datos una protección eficaz, siendo el tribunal el órgano responsable de interpretar la ley del lugar donde se ha cometido el ilícito. De hecho, la generalidad del precepto en un contexto de responsabilidad civil extracontractual desvía la atención que requiere la desprotección del sujeto perjudicado. En segundo lugar, este artículo adolece de una excesiva neutralidad, que va a desembocar en un procedimiento injusto cuando una de las partes litiga desde una posición de inferioridad. Por consiguiente, el art. 10.9 CC se fundamenta en una estructura rígida en la que el juez únicamente va a poder optar entre aplicar el ordenamiento del Estado donde se ha efectuado el hecho causal o la normativa del país donde se ha materializado el daño.

**SÉPTIMA.** El ordenamiento jurídico aplicable es claramente insuficiente para asegurar el derecho a la protección de datos, esto se debe a su dispersión y división entre los ordenamientos internos de los Estados miembros respaldados a su vez por las correspondientes autoridades de protección independientes. En síntesis, el titular de los datos susceptibles de un tratamiento transfronterizo internacional se va a posicionar en una situación de desprotección frente al sujeto exportador cuyo potencial económico y profesional es claramente más avanzado.

**OCTAVA.** En definitiva, consideramos que a pesar de los avances legislativos que integra el RGPD, todavía no se han abordado con éxito aquellas cuestiones relacionadas con su aplicación práctica, y es que a menudo los operadores jurídicos se van a ver superados por un escenario internacional, donde la confluencia de innovaciones tecnológicas crean un clima de inseguridad jurídica causado principalmente por la deslocalización empresarial en la prestación de sus servicios y por la diversidad de operadores y responsables. Ahora bien, puede que este Reglamento sea el primer paso para optimizar el nivel de protección de los datos personales de los ciudadanos en la UE y así construir una sociedad en la que los derechos fundamentales no se vean minorados por el inminente impacto de las nuevas tecnologías que han llegado para quedarse.

## BIBLIOGRAFÍA

- ÁLVAREZ RIGAUDIAS, C.: *El poder del usuario digital, hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Madrid, 2015.
- AÑOVEROS TERRADAS, B.: “Extensión de los foros de protección del consumidor a demandados domiciliados en terceros Estados”, *Agencia Española de Derecho Internacional Privado*, tomo IX, 2009, pp. 285-306.
- : “Consumidor con domicilio desconocido. ¿Hasta dónde llega la protección? A propósito de la sentencia del TJCE (Sala Primera) de 17 de noviembre de 2011, [C-327/10, Hypoteční banka a.s. contra Udo Mike Lindner]”, *Diario La Ley*, núm. 7870, 2012, pp. 4-8.
- ARENAS RAMIRO, M.: *Reforzando el ejercicio del derecho a la protección de datos personales, hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.
- BARCELÓ R./ PÉREZ ASINARI, M. V.: *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD*, Tirant lo Blanch, Valencia, 2009.
- BLAS, F.: “Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales”, *Revista Derecho del Estado*, núm. 23, 2009, pp. 37-66.
- BORRÁS RODRÍGUEZ, A.: “Jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, *Revista Jurídica de Catalunya*, 1993, pp. 259-262.
- : “Jurisprudencia del Tribunal de Justicia de las Comunidades Europeas”, *Revista Jurídica de Catalunya*, 1996, pp. 613-615.
- BOTANA AGRA, M.: “Infracción de derechos de autor y protección de datos personales en redes P2P (Comentario a la sentencia del Tribunal de Justicia de las Comunidades Europeas (Gran Sala), de 29 de enero de 2008, asunto C-275/06)”, *Actas de derecho industrial y derecho de autor*, 2008, pp. 801-824.
- BRIGGS, A.: “The Uncertainty of Special Jurisdiction”, *Lloyd's Maritime and Commercial Law Quarterly*, 1996, pp. 27-29.
- BRU CUADRADA, E.: “La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad”, *Revista de Internet, Derecho y Política*, núm. 5, 2007, pp. 78-92.
- CALVO CARAVACA, A. L./ AREAL LUDEÑA, S.: *Cuestiones actuales del derecho mercantil internacional*, Colex, Madrid, 2005.
- CASTELLANOS RODRÍGUEZ, A.: “El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield”, *Institut de Ciències Polítiques i Socials*, núm. 350, 2017, pp. 5-34.
- CORDERO ÁLVAREZ, C. I.: *Litigios internacionales sobre difamación y derechos de la personalidad*, Dykinson, Madrid, 2015.
- CORTÉS MARTÍN, J. M.: “Jurisprudencia del TJCE, Mayo-Agosto 2009”, *Revista de Derecho Comunitario Europeo*, 2009, pp. 1109-1178.

- COSLIN, C.: “Récents éclairages sur la compétence des tribunaux en matière de délits prétendument commis sur Internet”, *Droit de l’immatériel: informatique, médias, communication*, núm. 90, 2013, pp. 33-35.
- COUDERT, F.: *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, Valladolid, 2005.
- CREMADES LÓPEZ DE TERUEL, J./ SANCHO ALONSO, J.: “Protección de datos y poder judicial”, *Diario La Ley*, núm. 9293, 2018, pp. 1-20.
- CRESPO HERNÁNDEZ, A.: *La responsabilidad civil derivada de la contaminación transfronteriza ante la jurisdicción estatal*, Eurolex, Madrid, 1999.
- CROWTHER, H.: “Data protection: Google vs Spain: is there now a right to be forgotten?”, *Journal of Intellectual Property Law and Practice*, 2014, pp. 892-893.
- DECKER, M.: “Contract or Tort: A Conflict of Characterisation”, *International and Comparative Law Quarterly*, 1993, pp. 366-369.
- DE MIGUEL ASENSIO, P. A.: “Avances en la interpretación de la normativa comunitaria sobre protección de datos personales”, *Diario La Ley*, núm. 5964, 2004, pp. 1-8.
- : *Principio de protección de datos, Derecho Privado de Internet*, Aranzadi, Navarra, 2011.
- : “El tratamiento de datos personales por buscadores de Internet tras la sentencia Google Spain del Tribunal de Justicia”, *La Ley Unión Europea*, núm. 17, 2014, pp. 5-11.
- : *Derecho Privado de Internet*, Civitas, Madrid, 2015.
- : “Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea”, *Revista Española de Derecho Internacional*, núm. 69, 2017, pp. 75-108.
- DOMENECH, J.J.: “La aplicación del nuevo RGPD en el contexto del tratamiento de datos en la UE”, *Revista Lex Mercatoria*, núm. 6, 2017, pp. 37-42.
- DOPAZO FRAGUÍO, P.: “Novedades del Reglamento General de Protección de Datos”, *Revista Española de Derecho Europeo*, núm. 68, 2018, versión *online*.
- ESLAVA RODRÍGUEZ, M.: “El Locus Delicti Commssi en los ilícitos contra la vida privada cometidos a través de Internet”, *Revista Iberoamericana de Derecho Informático*, núm. 34, 2002, pp. 25-35.
- FELIU ÁLVAREZ DE SOTOMAYOR, S.: “Competencia judicial internacional y ley aplicable a los supuestos de responsabilidad extracontractual de los intermediarios básicos de Internet”/ CAVANILLAS MÚGICA, S. (Coord.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Comares, Granada, 2005, pp. 203-226.
- FERNÁNDEZ VILLAZÓN, L. A.: “El nuevo Reglamento Europeo de Protección de Datos”, *Foro Nueva Época*, núm. 1, 2016, versión *online*.
- GUERRERO PICÓ, C.: *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Civitas, Madrid, 2006.

- GUILLÉN CATALÁN, R.: “El interés legítimo: pieza clave en la excepción del consentimiento en el tratamiento de datos personales. Comentario a la Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 8 de febrero de 2012”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 29, 2012, pp. 431-438.
- GUASCH PORTAS, V.: “La transferencia internacional de datos de carácter personal”, *Revista de derecho Universidad Nacional Educación a Distancia*, núm. 11, 2012, pp. 413-454.
- : “La computación en nube y las transferencias internacionales de datos en el nuevo Reglamento de la UE”, *Revista de derecho Universidad Nacional Educación a Distancia*, núm. 20, 2017, pp. 333-349.
- HARTLEY, TREVOR: “Article 5: Place Where the Harmful Event Occurs”, *European Law Review*, 1996, pp. 164-166.
- HERNÁNDEZ CORCHETE, J.A.: “Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos”, PIÑAR MAÑAS J.L (Coord.), *Reglamento General de Protección de Datos*, Reus, Madrid, 2016, pp. 205-226.
- HERRERO PRIETO, P.: “Search Engines: Interplay of Fundamental Rights and the Principle of Proportionality”, *Computer and Telecommunications Law Review*, 2014, pp. 213-221.
- IDOT, L.: “Fourniture de renseignements pour la constitution d'annuaires”, *Europe 2011 Juillet*, núm. 7, 2011, pp. 35-36.
- JIMÉNEZ BLANCO, P.: “El tratamiento de las acciones colectivas en materia de consumidores en el Convenio de Bruselas”, *Diario La Ley*, núm. 5709, 2003, pp. 1-6.
- KRISTOFERITSCH, H.: “Transparency: Let There Be Light? Comments on the Judgment of the European Court of Justice, Joined Cases C-92/09 and C-93/09”, *European State Aid Law Quarterly 2011*, núm. 4, 2011, pp. 687-695.
- LESMES SERRANO, C.: *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia*, Lex Nova, Valladolid, 2008.
- LOPEZ AGUILAR, J. F.: *Data protection package y Parlamento europeo, hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Madrid, 2015.
- LUCENA CID, I.V.: “La protección de la intimidad en la era tecnológica: hacia una reconceptualización”, *Revista internacional de pensamiento político*, núm. 7, 2012, versión *online*.
- MATUS ARENAS, J.: “Transferencias internacionales a países con niveles adecuados y no adecuados de protección. Aspectos prácticos”, *Seminario Regional de Protección de Datos*, núm. 97, 2010, versión *online*.
- MINERO ALEJANDRE, G.: “Redes Sociales y derecho al honor, a la intimidad y a la propia imagen de personas fallecidas”, BUENO DE MATA, F. (Coord.), *Fodertics 6.0: los nuevos retos del derecho ante la era digital*, Comares, Granada, 2017, pp. 41-51.

- MUÑOZ, J.: “El llamado "derecho al olvido" y la responsabilidad de los buscadores: Comentario a la sentencia del TJUE de 13 de mayo 2014”, *Diario La Ley*, núm. 92, 2014, pp. 3-18.
- MURILLO DE LA CUEVA, P. L.: “La primera jurisprudencia sobre el derecho a la autodeterminación informativa”, *La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 1, 2003, pp. 43-58.
- NÚÑEZ LÓPEZ, M./ FERREIRO BROZ, M. M.: “Una aproximación para empresas a la Ley Orgánica de Protección de Datos”, *Derecom*, núm. 15, 2013, versión *online*.
- OLIVER, P.: “Case C-279/09, DEB vs Germany, Judgment of the Court of Justice (Second Chamber) of 22 December 2010”, *Common Market Law Review 2011*, núm. 6, 2011, pp. 2023-2040.
- ORDÓÑEZ SOLÍS, D.: “El derecho al olvido en Internet y la sentencia Google Spain”, *Revista Aranzadi Unión Europea*, núm. 6, 2014, pp. 27-50.
- ORTEGA GIMÉNEZ, A. / DOMENECH, J.J.: “Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea”, *Revista de la Facultad de Derecho*, núm. 44, 2018, pp. 1-35.
- ORTEGA GIMÉNEZ, A.: “Cloud computing, protección de datos y Derecho Internacional Privado (resolución de controversias y determinación de la ley aplicable)”, MARTÍNEZ MARTÍNEZ, R. (Dir.), *Derecho y cloud computing*, Aranzadi, Cizur Menor (Navarra), 2012, pp. 255-287.
- : “La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en Derecho Internacional Privado español”, *Diario La Ley*, núm. 8661, 2015, versión *online*.
- : *Transferencia internacional de datos de carácter personal ilícitas*, Aranzadi, Cizur Menor (Navarra), 2016.
- PADOVA, Y.: “La Cour de justice de l'Union européenne va-t-elle invalider les accords Safe Harbour?”, *Droit de l'immatériel: informatique, médias, communication*, núm. 110, 2014, pp. 14-16.
- PALAO MORENO, G.: *Responsabilidad civil extracontractual en el derecho europeo*, Tirant lo Blanch, Valencia, 2008.
- PARDOLESI, R.: “Il codice in materia di protezione dei dati personali e l'intangibilità della "privacy" comunitaria”, *Il Foro italiano*, núm. 4, 2004, pp. 59-64.
- PICOD, F.: “Invalidité partielle de règlements agricoles pour incompatibilité avec la Charte des droits fondamentaux”, *La Semaine Juridique - édition générale*, núm. 50, 2010, pp. 2340-2375.
- PULIDO QUECEDO, M.: “La catequista y los riesgos de Internet”, *Actualidad Jurídica Aranzadi*, núm. 602, 2003, pp. 14-15.
- REQUEJO ISIDRO, M.: *Artículo 10.9, Comentarios al Código Civil*, Lex Nova, Valladolid, 2010.
- RODRÍGUEZ ESCANCIANO, S.: “El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679”, *Estudios financieros. Revista de trabajo y seguridad social: Comentarios, casos prácticos: recursos humanos*, núm. 423, 2018, pp. 19-62.

- ROVIRA SUEIRO, M.E.: “Daños a los derechos de la personalidad”/ REGLERO CAMPOS, L. F. (Coord.), *Lecciones de responsabilidad Civil*, Cizur Menor (Navarra), 2002.
- RUIZ CASTILLO, M. M.: “Intimidación, protección de datos y libertad sindical: STC 11/1998, de 13 de enero”, GARCIA MURCIA, J. (Coord.), *Libertad sindical y otros derechos de acción colectiva de trabajadores y empresarios*, Aranzadi, Cizur Menor, 2015.
- RUIZ MIGUEL, C.: “El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea”, HERRERO DE LA FUENTE, A. A. (Coord.), *La Carta de Derechos Fundamentales de la Unión Europea: una perspectiva pluridisciplinar*, Fundación Rei Afonso Henriques, Zamora, 2003.
- SANCHO VILLA, D.: *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor, 2010.
- SARAVALLE, A.: “Evento dannoso e sue conseguenze patrimoniali: giurisprudenza italiana e comunitaria a confronto”, *Il Foro italiano*, núm. 4, 1996, pp. 341-348.
- SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012.
- STEVEN, J.: “The Right to Privacy Catches Up with Search Engines: The Unforgettable Decision in Google Spain vs AEPD”, *Computer and Telecommunications Law Review*, 2014, pp. 130-133.
- TOMAN, R.: “Limited Liability of Internet Search Engine Service Providers for Data Protection of Personal Data Displayed on Source Web Pages”, *European Law Reporter*, 2013, pp. 286-289.
- TREPPOZ, E.: “La résolution perturbatrice européenne des conflits de conventions en matière de contrats de transport”, *Revue des contrats*, 2014, pp. 251-254.
- VILLARINO MARZO, J.: *La privacidad en el entorno del cloud computing*, tesis doctoral dirigida por Pablo García Mexía, Universitat Abat Oliba CEU 2017.
- VILLAVERDE MENÉNDEZ, I.: “Protección de Datos Personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993”, *Revista Española de Derecho Constitucional*, núm. 41, 1994, pp. 187-224.
- WHITE, D.: “Private eye. Tom Morrison & David White review the world of information law”, *New Law Journal*, 2014, pp. 15-28.
- ZABÍA DE LA MATA, J.: *Protección de datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008.

## **ENLACES WEB**

(fecha de consulta: 7-07-2018)  
<https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html>.

(fecha de consulta: 7-08-2018)  
[http://ec.europa.eu/justice/policies/privacy/docs/international\\_transfers\\_faq/international\\_transfers\\_faq.pdf](http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

(fecha de consulta: 2-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.

(fecha de consulta: 3-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.

(fecha de consulta: 3-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.

(fecha de consulta: 7-10-2018) <https://www.aepd.es/areas/internet/derecho-al-olvido.html>.

(fecha de consulta: 9-10-2018) <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009>.

(fecha de consulta: 18-10-2018) <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32010D0087>.

(fecha de consulta: 27-10-2018) <https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf>.

(fecha de consulta: 1-11-2018) <http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm>.

(fecha de consulta: 5-11-2018)  
<https://www.oecd.org/sti/ieconomy/15590267.pdf>.

(fecha de consulta: 6-11-2018)  
<http://elconsultor.laley.es/content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMS>

bH1czUwMDA0Mzc3sjBQK0stKs7Mz7M1MjC0MDA3BgtkplW65CeHVBak2qY15h  
SnqiUmFefnlJakhhZl2oYUlaYCAHSi1jZGAAAAWKE.

(fecha de consulta: 7-11-2018) <https://www.aepd.es/media/estudios/informe-politicas-de-privacidad-adaptacion-RGPD.pdf>.

(fecha de consulta: 23-11-2018) <http://www.expansion.com/juridico/actualidad/tendencias/2018/11/21/5bf5b42a22601d333f8b45d1.html>.

## TEXTOS LEGALES

Código Civil	<i>BOE</i> núm. 206	25-VII-1889
Constitución española	<i>BOE</i> núm. 311	29-XII-1978
Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales	<i>BOE</i> núm. 243	10-X-1979
Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.	<i>BOE</i> núm. 157	02-VII-1985
Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal	<i>BOE</i> núm. 274	15-XI-1985
Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	<i>DOUE</i> L 281/31	23-XI-1995
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal	<i>BOE</i> núm. 298	14-XII-1999
Reglamento (CE) núm. 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil	<i>DOUE</i> L 12/1	16-I-2001
Reglamento (CE) núm. 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales (Roma II)	<i>DOUE</i> L 199/1	31-VII-2007
Decisión del Consejo, de 15 de octubre de 2007, relativa a la firma, en nombre de la Comunidad, del Convenio relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil	<i>DOUE</i> L 337/68	21-XII-2007
Reglamento (CE) núm. 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I)	<i>DOUE</i> L 41/7	4-VII-2008
Carta de los Derechos Fundamentales de la Unión Europea	<i>DOUE</i> C 83/389	30-III-2010
Reglamento (UE) núm. 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil	<i>DOUE</i> L 351/1	20-XII-2012
Reglamento (UE) 2016/679 del Parlamento Europeo y de Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos	<i>DOUE</i> L 119/1	4-V-2016

## ANEXO JURISPRUDENCIAL

### I. Jurisprudencia internacional

TRIBUNAL	ASUNTO	PARTES	ECLI
STJUE 17 junio 1992	C-26/91	<i>Handte et Cie GmbH</i>	EU:C:1992:268
STJCE 11 septiembre 1995	C-364/93	<i>Marinari</i>	EU:C:1995:289
STEDH 25 septiembre 2001		<i>P.G. y J.H. contra Reino Unido</i>	CE:ECHR:2001:0925JUD004478798
STJCE 1 octubre 2002	C-167/00	<i>Karl Heinz Henkel</i>	EU:C:2002:555
STJUE 6 noviembre 2003	C-101/01	<i>Bodil Lindqvist</i>	EU:C:2003:596
STJUE 5 febrero 2004	C-18/02	<i>DFDS Torline A/S</i>	EU:C:2004:74
STJUE 29 enero 2008	C-275/06	<i>Promusicae</i>	EU:C:2008:54
STJUE 16 octubre 2008	C-298/07	<i>deutsche internet versicherung</i>	EU:C:2008:572
STJUE 7 mayo 2009	C-553/07	<i>College van burgemeester en wethouders van Rotterdam</i>	EU:C:2009:293
STJUE 9 noviembre 2010	C-92/09 y C-93/09	<i>Volker und Markus Schecke y Hartmut Eifert</i>	EU:C:2010:662
STJUE 7 diciembre 2010	C-585/08 y C-144/09	<i>Pammer y Hotel Alpenhof</i>	EU:C:2010:740
STJUE 22 diciembre 2010	C-497/10	<i>Mercredi</i>	EU:C:2010:829
STJUE 5 mayo 2011	C-543/09	<i>Deutsche Telekom AG</i>	EU:C:2011:279
STJUE 12 julio 2011	C-324/09	<i>L'Oréal SA</i>	EU:C:2011:474
STJUE 25 octubre 2011	C-509/09 y C-161/10	<i>eDate Advertising GmbH</i>	EU:C:2011:685
STJCE 17 noviembre 2011	C-327/10	<i>Hypoteční banka a.s</i>	EU:C:2011:745
STJUE 24 noviembre 2011	C-70/10	<i>Scarlet Extended</i>	EU:C:2011:771
STJCE 15 marzo 2012	C-292/10	<i>Cornelius de Visser</i>	EU:C:2012:142
STJUE 19 abril 2012	C-523/10	<i>Wintersteiger AG</i>	EU:C:2012:220
STJUE 18 octubre 2012	C-173/11	<i>Football Dataco Ltd</i>	EU:C:2012:642
STJUE 11 abril 2013	C-645/11	<i>Sapir</i>	EU:C:2013:228

STJUE 3 octubre 2013	C-170/12	<i>Peter Pinckney</i>	EU:C:2013:635
STJUE 19 diciembre 2013	C-452/12	<i>Nipponkoa</i>	EU:C:2013:858
STJUE 13 marzo 2014	C-548/12	<i>Brogstetter</i>	EU:C:2014:148
STJUE 8 abril 2014	C-293/12 y C-594/12	<i>Digital Rights Ireland y Seitlinger y otros</i>	EU:C:2014:238
STJUE 13 mayo 2014	C-131/12	<i>Google Spain S.L contra Agencia Española de Protección de Datos</i>	EU:C:2014:317
STEDH 10 julio 2014	C-212/13	<i>Amann vs Suiza</i>	EU:C:2014:2072
STJUE 1 octubre 2015	C-230/14	<i>Weltimmo</i>	EU:C:2015:639
STJUE 6 octubre 2015	C-362/14	<i>Schrems</i>	EU:C:2015:650
STJUE 14 julio 2016	C-196/15	<i>Granarolo</i>	EU:C:2016:559
STJUE 28 julio 2016	C-191/15	<i>Verein für Konsumenteninformation</i>	EU:C:2016:612
STJUE 17 octubre 2017	C-194/16	<i>Bolagsupplysningen OÜ y Ingrid Ilsjan</i>	EU:C:2017:766

Conclusiones elaboradas por el Abogado General Henrik Saugmandsgaard ØE presentadas el 2 de junio de 2016 en el asunto C-191/15, <i>Verein für Konsumenteninformation</i> (ECLI:EU:C:2016:388)
Conclusiones elaboradas por el Abogado General Paolo Mengozzi de 1 de febrero de 2018 en el asunto C-25/17, <i>Tietosuojavaltuutettu contra Jehovan todistajat</i> (ECLI:EU:C:2018:57)
<i>Supreme Court</i> estadounidense <i>Calder vs Jones</i> (465 U.S. 783, 1984)

## II. Jurisprudencia nacional

STC de 20 de julio de 1993	ECLI:ES:TC:1993:254
STC de 30 de noviembre de 2000	ECLI:ES:TC:2000:292
STS de 15 de octubre de 2015	ES:TS:2015:4132
STS de 11 de marzo de 2016	ECLI:ES:TS:2016:1057
STS de 14 de marzo de 2016	ES:TS:2016:964
STS de 15 de marzo de 2016	ECLI:ES:TS:2016:1103
STS de 5 abril de 2016	ES:TS:2016:1280
STS de 13 de junio de 2016	ECLI:ES:TS:2016:2696

STS de 13 de junio de 2016	ECLI:ES:TS:2016:2699
STS de 13 de junio de 2016	ECLI:ES:TS:2016:2702
STS de 13 de junio de 2016	ECLI:ES:TS:2016:2707
STS de 13 de junio de 2016	ECLI:ES:TS:2016:2722
STS de 13 de junio de 2016	ECLI:ES:TS:2016:2723
STS de 13 de junio de 2016	ECLI:ES:TS:2016:2724
STS de 13 de junio de 2016	ECLI:ES:TS:2016:2725