universidad de león

FACULTAD DE DERECHO

UNIVERSIDAD DE LEÓN

CURSO 2018 / 2019

EL MARCO LEGAL DE LA PROTECCIÓN DE DATOS EN EL SENO DE LA UE: DEBATE ENTORNO A LAS «TRANSFERENCIAS INTERNACIONALES DE DATOS»

The legal framework of data protection regulation within the EU: The debate around «international data transfers»

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR: D. RUBÉN RODRÍGUEZ GONZÁLEZ

TUTOR: DR. D. DAVID CARRIZO AGUADO

ÍNDICE

ABREVIATURAS

EEE	Espacio Económico Europeo
RGPD	Reglamento General de protección de Datos
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales
GTPD	Grupo de Trabajo sobre Protección de Datos del artículo 29
UE	Unión Europea
AEPD	Agencia Española de Protección de Datos
BOE	Boletín Oficial del Estado
CC	Código Civil
CE	Constitución Española
CJI	Competencia Judicial Internacional
Coord.	Coordinador
Aut.	Autor
DIPr	Derecho Internacional Privado
DOUE / DOCE	Diario Oficial de la Unión Europea / Diario Oficial de la Comunidad Europea
EM	Estado miembro
LOPJ	Ley Orgánica del Poder Judicial
Núm.	Número
p. / pp.	Página / páginas
Vol.	Volumen
RBIbis	Reglamento "Bruselas I Bis"
RR II	Reglamento "Roma II"
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
TEDH	Tribunal Europeo de Derechos Humanos
Vid.	Véase
Ibídem	"En el mismo lugar"
TFUE	Tratado de Funcionamiento de la Unión Europea

RESUMEN

El ámbito de aplicación territorial del nuevo Reglamento General de Protección de Datos traspasa las fronteras de la UE para convertirse en una norma con vocación de "aplicación universal". La libre circulación de datos tiene que estar garantizada por el respeto al derecho fundamental a la protección de datos personales, de tal manera, que los ciudadanos cuenten con garantías adecuadas para velar, y en su caso reclamar, por un tratamiento de sus datos ajustado a los preceptos del Reglamento. Autoridades de control independientes y el derecho a la tutela judicial efectiva, constituyen la base de esta protección. La coexistencia con las actuales normas de Derecho Internacional Privado resulta, en este sentido, fundamental. Mismas garantías ofrece el Reglamento para las «transferencias internacionales de datos», es decir, las realizadas fuera del EEE, mediante un sistema de "garantías adecuadas", que implica el compromiso de los sujetos responsables del tratamiento, de cumplir con lo establecido en la normativa europea, para la primera y sucesivas transferencias internacionales de datos. El marco normativo integral para la libre circulación de los datos, se completa con un Reglamento para la circulación de los datos no personales, que conforman la política de la UE dentro del Mercado Único Digital.

PALABRAS CLAVE: RGPD, ámbito territorial, autoridades de control, derechos, competencia judicial, ley aplicable, transferencias internacionales de datos, datos no personales, *Privacy Shield*.

ABSTRACT

The territorial scope of the new General Data Protection Regulation crosses the European Union borders to become an "universal law", potentially applicable out of the EU. The free movement of data must be guaranteed by the respect of the Fundamental Right to Data Protection. In order to achieve this, the law has to provide efficient legal instruments to the citizens for claiming against an illegal treatment of their data, wherever the data have been treated. Independent national authorities and the right to legal protection are the two measures prescribed by the law to effectively guarantee this fundamental right. The interaction with the current rules of Private International Law results a key aspect, inspired by the Principle of Specialty. The new legal framework for international data transfers aims to equalise the rights and guarantees established by the GDPR for cross-border transfers to all transfers of data that take place outside the European Economic Area, not being limited to the first movement but also to the subsequent moves. Together with a new Regulation for non-personal data transfers, constitutes the integral regulatory framework designed by the European Union to strengthen and consolidate the Digital Single Market.

KEY WORDS: General Data Protection Regulation, GDPR, national authorities, International jurisdiction, applicable law, forum of jurisdiction, international data transfers, Privacy-Shield, non-personal data transfers.

OBJETO

El carácter extraterritorial de la nueva normativa europea de protección de datos personales es, sin duda, una de sus principales características. A ello se dedica el primer capítulo del presente trabajo, el cual tiene por objeto el estudio de su ámbito aplicación. Con especial énfasis a las novedades introducidas en cuanto a su ámbito espacial, comparándolo con el régimen anterior y mencionando los precedentes jurisprudenciales emanados del TJUE, que han definido en gran medida el texto del RGPD. Una interpretación flexible del concepto de "establecimiento", junto con la obligación para todas aquellas empresas u organizaciones, que a pesar de no estar establecidas en la UE, ofrezcan bienes o servicios u observen el comportamiento de personas ubicadas en la UE, principalmente a través de internet, de cumplir con la normativa europea de protección de datos, constituyen el núcleo principal de la exposición.

El segundo capítulo, se dedica al análisis de las dos vías a través de las cuales los interesados pueden hacer valer su derecho fundamental a la protección de datos personales, tanto desde el punto de vista administrativo como judicial. En el primer caso, las autoridades nacionales de control juegan un papel fundamental, como órganos públicos independientes encargados de supervisar la aplicación del RGPD, con competencias específicas para conocer de las reclamaciones presentadas por los ciudadanos, realizar las investigaciones pertinentes y si procede, imponer las sanciones previstas por la ley a los sujetos responsable del tratamiento. La nueva distinción entre "autoridad de control principal" e "interesadas", unido al principio de colaboración y cooperación entre ellas, son las principales novedades introducidas por el Reglamento.

Por otro lado, el derecho a una indemnización, expresamente reconocido por el Reglamento en favor de los interesados, como consecuencia de un tratamiento ilícito de datos, se ejercita en el orden jurisdiccional civil. Para la garantía de la tutela judicial efectiva, la nueva ley establece foros de competencia expresos que prevalecen sobre las normas generales preexistentes de DIPr en materia de CJI. En cuanto a la Ley Aplicable y cuestiones de Litispendencia, se precisa observar lo dispuesto por las normas internacionales que lo regulan, puesto que lo previsto en el RGPD sobre estas cuestiones, resulta insuficiente o no regulado. Por lo tanto, la interacción entre la normativa de protección de datos y las normas generales del DIPr reviste un particular interés. A su análisis, se dedica el capítulo tercero del trabajo.

El último capítulo se dedica a las transferencias internacionales de datos, un nuevo marco normativo inspirado en el principio de "garantías adecuadas", es un claro reflejo del "carácter universal" de la ley. En este sentido, en un mundo interconectado y globalizado, las transferencias de datos a terceros países se producen de manera cotidiana. Para garantizar que estas transferencias no pierdan las garantías que establece la ley para los movimientos de datos dentro de los Estados miembros, se han establecido diferentes mecanismo de "adhesión", que permiten a terceros países u organizaciones internacionales llevar a cabo transferencias datos dentro del marco legal establecido por el Reglamento, con los mismos derechos y garantías establecidos en la ley para las transferencias transfronterizas dentro de la UE, siempre y cuando entren dentro de su ámbito de aplicación, es decir, constituyan un tratamiento de datos personales de personas ubicadas en la UE. Un apartado específico se dedica al mecanismo de intercambio de datos entre la UE y los EE.UU, conocido como Escudo de Privacidad EU-EE.UU ó *Privacy Shield*.

Finalmente, se hace una especial mención del nuevo y muy reciente marco normativo para la circulación de los datos no personales dentro de la UE, como instrumento legal que viene a complementar al RGPD, y que juntos constituyen, el marco normativo integral diseñado por la UE para la libre circulación de los datos, como parte de su política de Mercado Único Digital clave en la nueva "economía digital".

METODOLOGÍA

La metodología de investigación utilizada para la realización de este trabajo tiene una estructura diferenciada.

Primera parte: elección del tema

En primer lugar, fruto de un interés personal por la protección de datos personales y por los conocimientos adquiridos durante el Máster, entre los que se encuentran las sesiones dedicadas a aspectos relevantes del DIPr, y haber sido oyente de una conferencia del señor José Luis Piñar Mañas sobre las transferencias internacionales de datos, han sido determinantes para la elección del tema. A pesar de ello, no fue fácil esta elección debido al gran potencial que tiene otras cuestiones ligadas al mundo de la Ciberseguridad y Derecho Digital. La elección del tutor y las conversaciones mantenidas con él sobre el objeto del trabajo, fueron clave para decidirme.

Segunda parte: desarrollo de la exposición

Una vez elegido el tema del trabajo, comenzó una labor de recopilación de información por medio de diversas fuentes tanto doctrinales, jurisprudenciales como legislativas.

Para una correcta distribución del trabajó, se acordó con el tutor dividirlo en cuatro capítulos, todos ellos vinculados por el componente transfronterizo que caracteriza a la nueva legislación en materia de protección de datos personales. En primer lugar, se analiza el ámbito de aplicación de la normativa, tanto material como territorial, desgranando cada uno de los artículos y Considerandos dedicados en la norma a estos aspectos, además, se hace una comparación con el régimen anterior y se citan algunos precedentes jurisprudenciales al respecto. El segundo capítulo está dedicado a las vías de reclamación de los interesados ante un tratamiento ilícito de sus datos. Las cuales se dividen en: vía administrativa ante las autoridades de control nacionales, y la judicial, ante los Tribunales del orden administrativo (y contencioso-administrativo), por lo que se refiere a las resoluciones dictadas por las autoridades de control, y la civil, para las reclamaciones ejercidas en virtud del derecho a una indemnización por los posibles daños y perjuicios causados al interesado. Vinculado a esto, se analiza la interacción entre las distintas autoridades de control nacionales para conocer y resolver de las reclamaciones ante ellos presentas, y con respecto a la tutela judicial efectiva, se dedica el siguiente

capítulo, con especial relevancia sobre las cuestiones de determinación de la CJI, Ley Aplicable y Litispendencia. El último y cuarto capítulo, está dedicado a las transferencias internacionales de datos tanto personales como no personales, que tiene por objeto garantizar la libre circulación de datos dentro de la UE.

Tercer parte: fuentes utilizadas

Entre los recursos utilizados para la recopilación de información, se han utilizado artículos de revistas jurídicas, libros, jurisprudencia del TJUE y TS, y la consulta de los sitios web de la Comisión Europea, AEPD, BOE, Curia, como fuentes principales. Destaco la consulta de manuales de DIPr para repasar y tener presente la legislación vigente en la materia.

Todos los recursos utilizados se complementan con tutorías que han sido de gran ayuda, en especial en lo referente al enfoque del trabajo, el correcto formato a utilizar, consejos sobre recursos bibliográficos, fuentes donde consultar y el cálculo de los tiempos para una correcta organización del trabajo. Desde un punto de vista personal, quiero destacar los ánimos dados desde el inicio, y su voluntad para darle el mejor enfoque posible al trabajo. Todo ello, ha resultado imprescindible para el resultado final conseguido.

INTRODUCCIÓN

Desde el pasado 25 de mayo de 2018, es directamente aplicable para todos los Estados miembros de la UE, el Reglamento (UE) 2016/679[1] de protección de datos personales. Reglamento que deroga a la Directiva 95/46/CE[2] y desplaza en la medida que resulte incompatible con él, a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre[3]. El RGPD reconoce el carácter de derecho fundamental[4] a la protección de las personas físicas frente al tratamiento de datos personales. Así se reconoce también en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea[5], y el artículo 16, apartado 1 del TFUE[6], que establecen que *"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*.

El reconocimiento de este derecho como fundamental, unido a la rápida evolución tecnológica y globalización, han planteado nuevos retos para la protección de datos personales[7]. Uno de ellos es su ámbito espacial de aplicación, pues a falta de otras legislaciones a nivel mundial sobre esta materia, el RGPD se configura como una norma con vocación de "aplicación universal", y ello es debido principalmente al impacto del mundo digital en nuestra sociedad, y a la posibilidad de dirigir u ofertar bienes o servicios a través de internet, a personas ubicadas en un país o zona geográfica distinta a donde se localiza el establecimiento físico o sede de la compañía, Este factor, ha supuesto una auténtica revolución comercial, y las leyes necesitan adaptarse a esta nueva realidad. El caso de la protección de datos, es un claro reflejo de este nuevo paradigma, puesto que en pocos años se ha convertido de un derecho casi inexistente a tener el carácter de derecho fundamental[8] con una regulación y jurisprudencia muy relevantes. En los siguientes

---

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *DOUE* 119/1, 4-V-2016.

[2] 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos. *DOCE* L 281, 23-XI-1995.

[3] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *BOE* núm. 298, 14-XII-1999.

[4] Considerando 1 del RGPD.

[5] *DOUE* C 83, 30-III-2010.

[6] Tratado de Funcionamiento de la Unión Europea. *DOUE* C 326, 26-X-2012.

[7] Considerando 6 del RGPD.

[8] Derivado de los arts. 10 y 14 de la CE. Y definido como autónomo e independiente por la STC de 30 de noviembre de 2000 (ECLI:ES:TC:2000:292).

capítulos, se analiza la legislación vigente en materia de protección de datos poniendo el acento en su carácter de norma extraterritorial y analizando algunas de sus principales implicaciones, sobre todo en materia de autoridades de control competentes y cuestiones relevantes del DIPr como la determinación de la CJI, ley aplicable y litispendencia. Mención especial, merece el nuevo régimen de transferencias internacionales de datos personales y no personales, que configuran el marco normativo diseñado por la UE para favorecer el Mercado Único Digital conectado, creando "unas condiciones de competencia equitativas en las que todas las empresas que ofrezcan sus productos o sus servicios digitales en la UE estén sujetas a unas mismas normas en materia de protección de datos"[9]. Favoreciendo a su vez, la libre circulación de datos dentro de la UE y evitando las injustificadas restricciones a la ubicación de los datos para su almacenamiento o tratamiento.

[9] COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia para el Mercado Único Digital de Europa. COM (2015) 192 final (fecha de consulta: 02-07-2019). https://eur-lex.europa.eu/.

La estrategia para el Mercado Único Digital se basa en tres ámbitos políticos o "pilares": Mejor acceso a los consumidores y a las empresas a los bienes en línea. Un entorno en el que puedan prosperar las redes y los servicios digitales. Y el sector digital como motor del crecimiento.

CAPÍTULO I. PANORAMA JURÍDICO EN MATERIA DE PROTECCIÓN DE DATOS

1. Observaciones iniciales

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, es la norma que regula el tratamiento que realizan personas, empresas u organizaciones de los datos personales relacionados con personas en la UE[10]. Queda fuera de su ámbito de aplicación el tratamiento de datos de personas fallecidas[11] y personas jurídicas[12]. Además, no se aplica a los datos que trate una persona en el marco de una actividad doméstica, siempre que no guarden relación con una actividad comercial o profesional[13].

El RGPD nace con la intención de unificar criterios y la legislación en materia de protección de datos en los Estados miembros, ya que la previa Directiva (derogada por este Reglamento) no logró armonizar las diferentes leyes estatales[14]. Esta evolución normativa se traduce en una mayor seguridad jurídica en el sentido de que los sujetos obligados a cumplir con la legislación[15] (responsable del tratamiento y encargado) deben asumir que la norma de referencia es el RGPD y no las normas nacionales[16]. No obstante, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[17] (LOPDGDD), que viene a concretar y desarrollar lo dispuesto

[10] Art. 4.1 del RGPD: "datos personales": toda información sobre una persona física identificada o identificable ("el interesado").

[11] El Considerando 27 del RGPD deja claro que no se aplica a la protección de datos personales de personas fallecidas, aunque deja a discreción de cada Estado la posibilidad de aprobar normas que regulen el tratamiento de estos datos. En el caso del derecho español, esta habilitación se traduce en lo dispuesto en el art. 3 de la LOPDGDD sobre la regulación de los datos de las personas fallecidas. A pesar de que queda excluido de su ámbito de aplicación el tratamiento de los mismos, se permite a las personas vinculadas al fallecido (por razones familiares, de hecho o herederos) la posibilidad de solicitar acceso a sus datos, así como ejercitar los derecho de supresión o rectificación, en su caso conforme las instrucciones del fallecido.

[12] Considerando 14 del RGPD.

[13] Artículos 1, 2 y considerandos 1, 2, 14, 18 y 27 del RGPD.

[14] DOPAZO FRAGUÍO, P.: "La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente. (Novedades del Reglamento General de Protección de Datos)". *Revista Europea de Derecho Europeo*, núm. 68, 2018, pp. 2-3.

[15] Considerando 22 del RGPD.

[16] Guía del Reglamento General de Protección de Datos para responsables de tratamiento. AEPD. (fecha de consulta: 19-05-2019) https://www.aepd.es.

[17] *BOE* núm. 294, 06-XII-2018.

en el RGPD, en vigor desde el 6 de diciembre de 2018, si incluye algunas precisiones o desarrollos que deja a discreción de cada Estado el RGPD.

Como punto de partida, es posible afirmar que el objeto del RGPD es doble: por una parte, regular un derecho (protección de datos) y garantizar una libertad (la libre circulación de los datos)[18].

2. Ámbito de aplicación material y territorial del RGPD

El objetivo de este capítulo es analizar y desarrollar los preceptos dedicados al alcance material y territorial del RGPD. Destacando las diferencias con la ya derogada Directiva 95/46/CE, y citando algunos precedentes jurisprudenciales emanados del TJUE, que han ayudado en gran medida a completar y aclarar lo establecido en la ley. Todo ello, permitirá entender mejor la evolución normativa de este derecho, sirviendo también como base para el estudio en los siguientes capítulos de las vías de reclamación de los interesados ante un tratamiento ilícito de sus datos, cuestiones relativas a la interacción entre la normativa de protección de datos y el Derecho Internacional Privado, y las novedades sobre transferencias internacionales de datos contenidas en el RGPD.

2.1. Ámbito de aplicación material

En cuanto al ámbito de aplicación material, se regula en el art. 2 y Considerandos 14 a 21 y 27 del RGPD. Y se complementa con lo dispuesto en el art. 2 de la LOPDGDD. El art. 2 del RGPD comienza, en su apartado primero, estableciendo que el Reglamento se aplica a todas aquellas actividades relacionadas con el tratamiento de datos personales por medios automatizados, total o parcialmente, o no automatizados de personas físicas en la Unión Europea, siendo indiferente su nacionalidad o residencia habitual, destinados o potencialmente destinados a ser incluidos en un fichero.

Partiendo de la definición de "tratamiento" realizada por el RGPD en su art. 4. b), definido como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no. Se entiende que el "tratamiento" se refiere a la recogida y posterior inclusión de datos personales en una base de datos o fichero, entendido éste, como un conjunto organizado

[18] Considerando 166 del RGPD: "*A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión*".

de datos. Lo que conlleva que la práctica totalidad de actividades que impliquen la utilización de datos de carácter personal, tienen una alta probabilidad de que exista en ellas un "tratamiento de datos" a efectos del RGPD[19]. Sin embargo, conviene resaltar el hecho de que la mera presencia de datos personales no es suficiente para hacer valer el derecho a la protección de datos personales, sino que tienen que haber sido objeto de tratamiento[20].

El apartado segundo del art. 2, enumera una serie de excepciones (*numerus clausus*) a las que no se aplica el RGPD, que son: los tratamientos de datos personales en el ejercicio de una actividad no comprendida entre las competencias atribuidas expresamente a la Unión Europea (letra a); las actividades relacionadas con la política exterior y de seguridad común de los Estados miembros (letra b); el tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia o la llevanza de un repertorio de direcciones[21] (letra c); y el tratamiento por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales incluida la de protección frente a amenazas a la seguridad pública y su prevención (letra d) que se regirá por lo dispuesto en la Directiva 2016/680[22].

A modo de ejemplo, materias como la protección y la prevención frente a las amenazas para la seguridad pública, los controles fronterizos o las actividades relacionadas con la protección internacional se regirán en la medida en que estén comprendidas en el ámbito de aplicación del derecho de la UE por el RGPD[23].

Por lo tanto, si de acuerdo a los tratados constitutivos, la Unión no tiene competencias para abordar una materia determinada, a los tratamientos de datos que se

---

[19] ERDOZÁIN LÓPEZ, J. C.: "La protección de los datos de carácter personal en las telecomunicaciones", *Revista Doctrinal Aranzadi Civil-Mercantil*, núm. 1, 2007, pp. 2-3.

[20] TRANCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Madrid, 2010, pp.732-733.

[21] Considerando 18 RGPD.

[22] Directiva 2016/680/UE, de 27 de abril. Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos. *DOUE* L núm. 119, 4-V-2016.

[23] DÍAZ MARTÍN, C.: "El Reglamento General de Protección de Datos, su implementación y la transición para el responsable público". *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 47, 2018, p. 1.

puedan desarrollar para la realización de esa materia no les puede ser de aplicación el RGPD[24].

En el derecho español el ámbito de aplicación de la normativa en materia de protección de datos personales comprende: la política exterior, la seguridad nacional[25] y también las actividades policiales de las fuerzas y cuerpos de seguridad distinguiendo entre tratamientos de datos personales con fines administrativos y policiales. Quedan exceptuadas las actividades de tratamiento relacionadas con materias clasificadas[26] (art. 2.2.c LOPDGDD). Sobre las materias clasificadas existe un debate en torno a cuándo se encuentran excluidas del ámbito de aplicación, desde que son declaradas materias clasificadas o desde la recogida de los datos con fines específicos relacionados con la protección de la seguridad del Estado, en la medida en que la finalidad perseguida prevalezca sobre el derecho fundamental a la protección de datos personales de los interesados debe entenderse que quedaría excluida la aplicación desde la recogida de los datos[27].

Por su parte, el art. 2.3 de la LOPDGDD viene a completar lo dispuesto en el RGPD, incorporado el principio de especialidad normativa "ley especial deroga ley general", es decir, cuando no exista una regulación específica establece la aplicación del RGPD como normativa de referencia general y la de su articulado de forma supletoria. Se encuentran en esta situación los tratamientos realizados al amparo de la legislación del régimen electoral general, en el ámbito de instituciones penitenciarias y aquellos derivados del Registro Civil, los Registros de la Propiedad y los Mercantiles. La finalidad de este precepto es fijar una coherencia jurídica estableciendo una jerarquía normativa en materia de protección de datos tanto a nivel europeo como nacional. Además, conviene destacar lo declarado por el Consejo de Estado en su Dictamen sobre el Anteproyecto de Ley Orgánica de Protección de Datos[28] "esa aplicabilidad supletoria del RGPD, en los casos

[24] URIARTE LANDA, I.: "Ámbito de aplicación material", PIÑAR MAÑAS J.L. (Dir.) / ÁLVAREZ CARO, M.; RECIO GAYO, M. (Coords.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Barcelona, 2016, pp. 64-66.

[25] Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. *BOE* núm. 233, 29-09-2015.

[26] De acuerdo con la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales (*BOE* núm. 84, 06-IV-1968) por materias clasificadas, cabe entender "asunto, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado".

[27] DÍAZ MARTÍN, C.: "El Reglamento General de Protección de Datos, su implementación y la transición para el responsable público". *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 47, 2018, p. 3.

[28] Consejo de Estado. "Dictamen sobre el «Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal". Núm. de expediente 757/2017. Aprobado el 26 de octubre de 2017 (fecha de consulta: 24-05-2019) https://www.boe.es/.

en principio no sometidos al Derecho de la Unión, lleva consigo la de la jurisprudencia interpretativa del mismo, así como la competencia prejudicial del Tribunal de Justicia de la Unión Europea".

2.2. Ámbito de aplicación territorial

El ámbito de aplicación territorial, está regulado en el art. 3 y Considerandos 22 a 25 del RGPD. A diferencia del artículo 4 de la Directiva 95/46/CE, titulado "Derecho nacional aplicable", el artículo 3 del RGPD se denomina "Ámbito territorial". Aunque ambos tienen como finalidad la concreción del ámbito de aplicación espacial de la legislación europea, el espíritu del Reglamento tiene por objeto unificar la normativa en Europa, más que concretar la ley del Estado miembro que se debe aplicar como preveía la Directiva, con alguna excepción[29]. La Directiva no sólo preveía la determinación de la ley aplicable sino también la autoridad de control competente, habida cuenta de la estricta correlación entre ambas en el derecho administrativo[30].

Lo que si resulta coincidente en ambas leyes, es que parten de una clasificación tripartita[31], y prevén como primer criterio determinante el sometimiento a la legislación europea el que el tratamiento de datos tenga lugar en el contexto (marco) de las actividades de un establecimiento del responsable o del encargado en la Unión (un Estado miembro), independientemente del lugar de tratamiento de los datos[32].

Si lo sujetos responsables, se encuentra establecidos en un lugar distinto, el RGPD introduce como novedad que será de aplicación la legislación europea cuando el responsable o encargado a pesar de no estar establecidos en la UE, realiza actividades de tratamiento de datos relacionadas, bien con la oferta de bienes o servicios (de pago o gratuitos) a interesados en la Unión, u observen el comportamiento de personas ubicadas en la Unión Europea.[33]

---

[29] Como la determinación de la edad mínima del menor para otorgar su consentimiento (art. 8 del RGPD).

[30] 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 (REDI)*, núm. 1, 2017, p. 6.

[31] Art. 4.2 RGPD: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no*".

[32] Art. 3.1 del RGPD.

[33] Art. 3.2 del RGPD.

Por último, y al igual que recogía la Directiva 95/46/CE, el RGPD será de aplicación para el tratamiento de datos personales realizados por un responsable no establecido en la UE, sino en un lugar en que el Derecho de los Estados miembros se aplica en virtud del Derecho Internacional Público[34], como es el caso de una misión diplomática u oficina consular de un Estado miembro (art. 25 RGPD)"[35].

A. *Actividades de un establecimiento del responsable o del encargado en la UE*

Como se ha señalado, el primero de los criterios referidos al ámbito territorial del art. 3 del RGPD establece que será de aplicación el RGPD cuando el tratamiento de datos se lleve a cabo en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la Unión. Si bien no resulta algo novedoso con respecto a la Directiva, se introducen algunos cambios.

Una de las novedades que introduce el Reglamento con respecto a la Directiva es que incluye no sólo al responsable del tratamiento sino también al encargado del tratamiento, entendiendo éste como "la *persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento"*.

Por otra parte, se sustituye el término "marco" por "contexto".

De este primer supuesto, la cuestión más controvertida es la definición de "establecimiento". Cuestión que ya venía siendo discutida con la Directiva y sobre la que se pronunció el TJUE en varias ocasiones. Destacan las sentencias *Weltimmo*[36] y *Google Spain*[37]. Si bien ambas presentan como denominador común el de establecer un concepto

[34] Art. 3.3 RGPD.

[35] 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 (REDI)*, núm. 1, 2017, pp. 7-8.

[36] STJUE de 1 de octubre de 2015, asunto C-230/14, *Weltimmo*, ECLI:EU:C:2015:639. A mayor abundamiento, víd. JERKER SVANTESSON, D.: "The CJEU's Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, Yet So Very Important", *Maastricht Journal of European and Comparative Law*, núm. 1, 2016, pp. 332-341.

[37] STJUE de 13 de mayo de 2014, asunto C-131/12, *Google Spain y Google*, ECLI:EU:C:2014:317. A mayor abundamiento, vid. 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. ORDÓÑEZ SOLÍS, D.: "El derecho al olvido en Internet y la sentencia Google Spain", *Revista Aranzadi Unión Europea*, núm. 6, 2014, pp. 27-50.

flexible de "establecimiento"[38], la sentencia *Weltimmo* pone el acento en la concurrencia de varios Estados a efectos de ley aplicable y autoridad de control competente[39], mientras que la segunda (caso *Google Spain*) tiene su origen en una petición de tutela por parte de un ciudadano con respecto al Derecho al Olvido de la información localizada en internet y accesible a través de motores de búsqueda. Su relevancia en cuanto al alcance territorial reside en que establece que será de aplicación la legislación europea en aquellos casos en los que exista una "vinculación inextricable" entre las actividades de un establecimiento en la Unión y el procesamiento de datos, independientemente de que el tratamiento se lleve a cabo o no en la Unión[40]. Es decir, en el presente caso se probó que la compañía Google contaba con una sociedad establecida en España, Google Spain, S.L., y pese a que esta sucursal no se dedica a tareas de motor de búsqueda y tratamiento de datos personales, se concluyó que su actividad está inevitablemente enlazada con tareas de recogida y uso de datos que posteriormente la compañía utiliza y trata, pese a que el tratamiento se realiza en su sede central Google Inc. localizada fuera de la Unión.

Para ayudar en la interpretación, el RGPD aclara que "*un establecimiento implica 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 con personalidad jurídica, no es el factor determinante al respecto*"[41].

Esta interpretación amplia del concepto de "establecimiento" que hace el RGPD a efectos de determinar el ámbito territorial de aplicación, no es sino la concreción en una norma de cómo lo venía interpretando el TJUE hasta ahora. En la ya mencionada sentencia *Weltimmo*, el Tribunal se pronuncia sobre si la realización de actividades de tratamiento de un responsable en otro Estado miembro distinto de aquel donde tiene su establecimiento, puede ser considerado como un tratamiento dentro del marco de las

[38] DE MIGUEL ASENSIO, P.A.: "Protección de datos y Derecho aplicable: nuevos desarrollos". http://pedrodemiguelasensio.blogspot.com/ (fecha de entrada 05-02-2016).

[39] "La sentencia *Weltimmo* refuerza la posibilidad de actuación por parte de las diversas autoridades nacionales de control (así como facilita el acceso por los afectados a la de su propio Estado) en situaciones en las que prestadores de servicios en principio establecidos en un único Estado miembro (o en un tercer Estado, como EEUU) tienen un gran número de usuarios en diversos Estados miembros en los que además cuentan con algún tipo de presencia, como una mera oficina de representación, de modo que a efectos de la aplicación de la legislación de protección de datos (y de la determinación de la autoridad de control) se les puede considerar establecidos en más de un Estado miembro". Vid. DE MIGUEL ASENSIO, P. A.: "Aspectos internacionales de la protección de datos: las sentencias *Schrems* y *Weltimmo* del Tribunal de Justicia", *La Ley Unión Europea*, núm. 31, 2015, p. 8.

[40] GONZALO DOMÉNECH, J.J.*:* "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana. de Derecho*, núm. 26, 2018, pp. 410-411.

[41] Considerando 22 del RGPD.

actividades en ese otro Estado[42]. Sobre esta cuestión, el TJUE afirma que "basta con un solo representante en otro Estado miembro si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación de los servicios en la Unión"[43]. De manera similar, el TJUE, en el asunto *Verein für Konsumenteninformation vs Amazon EU Sàrl*[44], determina que es posible considerar la existencia de un establecimiento en un Estado miembro cuando no exista ni una filial o sucursal, siendo necesario valorar el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado[45], siendo posible considerar como "establecimiento" un representante de la sociedad si actúa con un grado de estabilidad suficiente.

Además, el artículo 4. 16) del RGPD ha considerado en su definición el concepto de "establecimiento principal", que ha permitido aclarar y delimitar cuestiones altamente relevantes como la concreción de un establecimiento principal del responsable o de un encargado con varios establecimientos en la Unión mediante reglas marcadas por el principio de especialidad y jerarquía[46]:

1º) En el supuesto de un responsable con varios establecimientos, como norma general se considerará principal el establecimiento donde se lleve a cabo la administración central en la UE. Pero como norma especial, si las decisiones sobre los fines y los medios del tratamiento se toman en otro establecimiento, y tiene el poder para hacerlas efectivas, se considerará como principal este último.

2º) En cuanto al supuesto de un encargado con varios establecimientos, se considerará principal el establecimiento en el que se lleve a cabo la administración central en la Unión. Si careciera de ella, como norma supletoria, será el establecimiento del encargado en la UE en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado.

---

[42] DE MIGUEL ASENSIO, P. A.: "Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia", *La Ley Unión Europea*, núm. 31, 2015, pp. 9-10.

[43] Apartados 29 y 30 de la STJUE de 1 de octubre de 2015, *Weltimmo*.

[44] STJUE de 28 de julio de 2016, asunto C-191/15, *Verein für Konsumenteninformation vs Amazon EU Sàrl*. ECLI:EU: C:2016:612. A mayor abundamiento, vid. ZANFIR FORTUNA, G.: "A Missed Opportunity: The Amazon Case That Almost Made Data Subjects Into Consumers", *European Data Protection Law Review*, núm. 2, 2016, pp. 585-589.

[45] Apartados 76 y 77 de la STJUE *Verein für Konsumenteninformation vs Amazon EU Sàrl*.

[46] GONZALO DOMÉNECH, J.J.: "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, núm. 26, 2018, pp. 410-411.

B. *Actividades relacionadas con la oferta de bienes o servicios*

Sin embargo, donde destaca el Reglamento como novedad es en el carácter extraterritorial de sus disposiciones para proteger los datos personales de los interesados que residan en la UE frente a actividades comerciales o de control. Y es que varios son los elementos que permiten entender la trascendencia internacional alcanzada por la legislación europea en materia de protección de datos personales[47]. El hecho de que se configure como un derecho fundamental[48], la falta de legislación a nivel global sobre la materia y la creciente utilización de información sobre personas físicas como componente esencial de actividades ofertadas o prestadas a través de internet[49], favorecen la llamada "aplicación universal" del Reglamento.

El art. 3.2 del RGPD establece que el Reglamento es aplicable al tratamiento de datos personales de interesados que residan en la Unión, por parte de un responsable o encargado no establecido en la Unión, si las actividades de tratamiento están relacionadas con un objeto determinado, que puede ser: a) la oferta de bienes o servicios a dichos interesados en la Unión, de pago o gratuitos. b) El control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Pese a que la versión española de la norma habla de tratamiento de datos de interesados "*que residan en la Unión*", existe consenso en que debe ser entendido y sustituido por el concepto de "interesados que se encuentren en la Unión", en consonancia así con el planteamiento de que la protección *"debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia"*[50].

Para entender el alcance de lo establecido en el art. 3.2 inciso a), es necesario tener en cuenta lo dispuesto en el considerando 23, donde se dice que "*para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión*" (*targeting-*

[47] 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 (REDI)*, núm. 1, 2017, pp. 1-2.

[48] Tal y como define el TC, en la Sentencia 290/2000 de 30 de noviembre (ECLI:ES:TC:2000:290), se trata del derecho de todo ciudadano a disponer de sus datos personales y conocer el tratamiento de los mismos que realicen otras personas. Esto es, se trata de proteger y garantizar el control de todo sujeto de derecho de los datos de los que sea titular.

[49] Caso de la utilización de la información en las redes sociales.

[50] Considerando 14 RGPD.

based analysis)[51]. Conforme al Considerando 23, se descarta que la mera accesibilidad del sitio web del responsable, encargado o un intermediario en la Unión, una dirección de correo electrónico u otro dato de contacto el uso de un tercer idioma común, no son suficientes para probar la intención de ofertar bienes o servicios en la Unión. Sin embargo, si considera el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros, o la mención de clientes o usuarios que residen en la Unión, como indicios suficientes para probar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

Este criterio se pone en consonancia, salvando las distancias con las particularidades de cada caso, con la doctrina del TJUE relativa al criterio de que la actividad comercial vaya dirigida al Estado de la residencia habitual del consumidor, que tienen su reflejo en los criterios de vinculación establecidos con carácter indicativo – que no exhaustivo - por el TJUE en los asuntos *Pammer* y *Hotel Alpenhof* [52].

Entre los indicios relevantes según el Tribunal se encuentran "*todas las expresiones manifiestas de la voluntad de atraer a los consumidores de dicho Estado miembro*"[53], como la mención de que ofrece sus servicios o sus bienes en ese Estado miembro o la publicidad en medios que facilitan el conocimiento de su sitio por consumidores domiciliados en ese Estado. Ahora bien, la conclusión de que un sitio va dirigido al Estado miembro del domicilio del consumidor también puede alcanzarse en situaciones en las que no cabe apreciar expresiones manifiestas de la voluntad de atraer a los consumidores de ese país. Como otros indicios que pueden ser relevantes, los apartados. 83 y 84 y el fallo de la Sentencia enumeran los siguientes aspectos: 1) el carácter internacional de la actividad; 2) la indicación del prefijo internacional en los números de teléfono; 3) utilización de un nombre de dominio de primer nivel geográfico distinto al del Estado del vendedor; 4) descripción de un itinerario de envío desde un Estado miembro al lugar de la prestación del servicio; 5) la mención de una clientela internacional formada por clientes domiciliados en un Estado miembro, y 6) el empleo de lenguas o divisas que no se corresponden con las habituales en el Estado a partir del cual ejerce su actividad el empresario.

---

[51] GEIST, M.: "Is There a There There? Toward Greater Certainty for Internet Jurisdiction", *Berkeley Technology Law Journal*, núm. 3, 2001, pp. 1345-1406.

[52] STJUE de 7 de diciembre de 2010, *Pammer y Hotel Alpenhof*, asuntos acumulados C-585/08 y C-144/09, ECLI:EU:C:2010:740.

[53] Apartado 80 STJUE de 7 de diciembre de 2010, *Pammer y Hotel Alpenhof*.

C. *Actividades que observen el comportamiento de personas en la UE*

Este supuesto parece ideado básicamente para aquellas situaciones en las que ese control, en particular al hilo del empleo de archivos o programas informáticos que almacenan y permiten el acceso a información en el equipo de un usuario, como cookies, no tiene lugar en el marco del ofrecimiento al interesado de productos o servicios[54]. El objetivo principal de este tipo de programas es monitorizar el comportamiento humano.

También parecería englobarse dentro de este precepto los tratamientos realizados por *Big Data*[55] a la luz de lo establecido en el Considerando 24. Donde se dice que "*para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial 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, comportamientos y actitudes*".

[54] 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 (REDI)*, núm. 1, 2017, p. 16.

[55] COMISIÓN EUROPEA. Digital Single Market. Big data. Big data (en español, grandes datos o grandes volúmenes de datos) es un término que se refiere a grandes cantidades de datos generados rápidamente y procedentes de diversas fuentes. Pudiendo ser generados por personas o de manera automatizada. (fecha de consulta: 02-06-2019) (en línea), https://ec.europa.eu/.

CAPÍTULO II. VÍAS DE RECLAMACIÓN QUE LOS INTERESADOS DISPONEN ANTE UN TRATAMIENTO ILÍCITO DE DATOS PERSONALES

1. Observaciones iniciales

Frente a un tratamiento ilícito de datos, el RGPD contempla dos vías a través de las cuales los interesados pueden hacer valer sus derechos: desde el punto de vista administrativo, a través de una reclamación ante una autoridad de control y en segundo lugar, el ejercicio acciones judiciales contra los sujetos responsables del tratamiento.

Ambas reclamaciones no son excluyentes, es decir, pueden ejercitarse una o ambas a la vez o de manera consecutiva. Una reclamación presentada ante una autoridad de control tiene como finalidad la imposición de una sanción económica contra el responsable o encargado del tratamiento por el incumplimiento de las disposiciones del Reglamento. Mientras que la segunda, tiene como objetivo principal que el afectado pueda reclamar una indemnización como consecuencia de los daños y perjuicios sufridos, derivados del incumplimiento de las obligaciones del RGPD por parte del responsable o encargado del tratamiento.

Otra diferencia entre ambas, es que una reclamación ante una autoridad de control constituye una reclamación por la vía administrativa (recurrible en última instancia ante los tribunales contencioso-administrativos), mientras que las acciones judiciales para reclamar una indemnización se ejercitan en el orden civil (salvo que el responsable o encargado sea una administración pública)[56].

En los siguientes apartados se analiza el marco normativo y jurisprudencial de estas dos vías de reclamación que constituyen la principal garantía de los ciudadanos para hacer valer sus derechos ante cualquier tratamiento ilícito de sus datos, y el reconocimiento a la tutela judicial efectiva como derecho fundamental[57] reconocido por la CE[58].

---

[56] GONZALO DOMÉNECH, J.J.: "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, núm. 26, 2018, pp. 415-416.

[57] RECIO GAYO, M.: "Los derechos a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva", PIÑAR MAÑAS J.L. (Dir.) / ÁLVAREZ CARO, M.; RECIO GAYO, M. (Coords.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Barcelona, 2016, pp. 550-551.

[58] Art. 24.1 CE (*BOE*, núm. 311, 29-XII-1978). "Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión".

2. Reclamaciones ante las autoridades control

2.1. Introducción

Conforme al art. 77 del RGPD, los interesados podrán presentar una reclamación ante una autoridad de control si consideran que sus datos de carácter personal están siendo objeto de un tratamiento que no respeta los preceptos del Reglamento.

Este derecho de defensa, se ejercitará cuando se vulnere alguno de los derechos reconocidos a los interesados en el RGPD, esto es, el derecho de información, derecho de acceso, derecho de rectificación, derecho al olvido, derecho a la limitación del tratamiento, derecho a la portabilidad de los datos y derechos sobre decisiones individuales automatizadas[59].

2.2. Autoridades de control nacionales

En el Capítulo VI del RGPD se regulan las autoridades de control. Configuradas como organismos públicos independientes "encargados de supervisar la aplicación del Reglamento"[60]. Cada Estado miembro puede contar con más de una autoridad de control conforme lo establecido en el art. 51.1 del RGPD[61]. Por su parte, en la LOPDGDD se regulan en el Título VII.

Dos de las principales funciones asignadas a las autoridades de control nacionales, son las de control de la aplicación del RGPD y demás normativa interna en materia de protección de datos y, la gestión y resolución de las reclamaciones presentadas por los interesados o por un organismo, organización o asociación de conformidad con el artículo 80 del RGPD e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control[62]. Por lo que aquí interesa, el análisis se centrará en las reclamaciones.

---

[59] Título III, Capítulo II, arts. 12, 13, 14, 15, 16, 17 y 18 LOPDGDD.

[60] Art. 51.1 del RGPD.

[61] Caso de España, que cuenta con la Agencia de Protección de Datos como órgano nacional encargado de la supervisión y cumplimiento del RGPD. Y respecto a nivel autonómico se han creado la Autoridad Catalana de Protección de Datos, la Agencia Vasca de protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía, reguladas en las disposiciones 57 y 58 de la LOPDGDD.

[62] Funciones y control. AEPD. (Fecha de consulta: 09-06-2019). https://www.aepd.es.

A. *Alcance territorial de competencia*

En cuanto al alcance territorial de su competencia, de conformidad con el art. 55 del RGPD, cada autoridad es competente en el territorio de su Estado. De esta manera, el alcance de su competencia se extiende a aquellos tratamientos realizados en el contexto de las actividades de un establecimiento en su Estado miembro, los realizados por autoridades públicas de ese Estado, los que afecten a interesados en su territorio, así como los realizados por quienes no están establecidos en la Unión, cuando sus destinatarios son interesados residentes en su territorio (considerando 122 del RGPD)[63].

Si bien se establece el criterio de la territorialidad, se pueden dar situaciones en las que varios Estados estén involucrados (casos de tratamiento transfronterizos de datos), lo que es susceptible de generar una situación de confusión en torno a qué autoridad de control sería la competente para conocer de una reclamación. De hecho, no es algo excepcional teniendo en cuenta el concepto amplio de "establecimiento" previsto por el RGPD, como se analizó en el capítulo correspondiente al ámbito territorial. Y también a la posibilidad de que un servicio esté destinado a interesados de varios países de la Unión Europea, principalmente a través de internet. Por lo tanto, la cuestión de la competencia de las autoridades de control en los casos de tratamientos transfronterizos de datos no sólo no es excepcional sino tampoco novedoso, ya que en el antiguo régimen de la Directiva 95/46/CE se discutió mucho sobre el alcance de la competencia de las autoridades de control y de hecho existen importantes decisiones emanadas del TJUE que han ayudado a su interpretación.

Una de las sentencias más ilustrativas al respecto, como ya se mencionó en el primer capítulo, fue la STJUE en el caso *Weltimmo*[64], referida a una controversia entre la autoridad húngara de protección de datos y una empresa, con domicilio social en Eslovaquia, que gestionaba una página web de intermediación inmobiliaria en la que se anunciaban inmuebles sitos en Hungría y algunos de cuyos anunciantes, residentes en Hungría habían presentado reclamaciones ante la autoridad húngara que pretendía sancionar a la empresa con domicilio social en Eslovaquia[65].

[63] 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 (REDI)*, núm. 1, 2017, pp. 18-19.

[64] Sentencia de 1 de octubre de 2015, en el asunto C-230/14, *Weltimmo*. ECLI:EU:C:2015:639.

[65] DE MIGUEL ASENSIO, P.A.: "Ley aplicable y autoridad competente en materia de protección de datos: la sentencia *Weltimmo*". http://pedrodemiguelasensio.blogspot.com. (fecha de entrada: 06-10-2015).

A efectos de valorar la existencia de un establecimiento, el Tribunal considera que debe valorarse "el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades… tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión", lo que facilita la posibilidad de determinar que exista una instalación estable en un Estado distinto al del domicilio social, especialmente para las empresas que se dedican a ofrecer servicios por Internet[66]. La actividad puede llevarse a cabo a través de Internet, por ejemplo, cuando tiene lugar mediante un sitio web dirigido a ese territorio, aunque resulta preciso además que disponga ahí de una instalación estable[67].

Sin duda, fija un criterio de interpretación flexible del concepto de "establecimiento". La sentencia se completa con el criterio base acogido por el Tribunal de la correlación entre legislación aplicable y autoridad de control competente, puesto que una autoridad de control "no puede imponer sanciones fuera del territorio de su propio Estado miembro" (apartado 57 de la sentencia), debiendo instar, en cumplimiento de la obligación de cooperación, a la autoridad de control de ese Estado para que verifique la vulneración y, si procede, imponga una sanción al sujeto responsable del tratamiento.

Actualmente con el Reglamento está correlación ya no existe como tal, puesto que debe entenderse entre el RGPD y las autoridades de control nacionales.

Otra sentencia muy relevante fue la STJUE en el caso *Google Spain*, que determinó la competencia de la AEPD para conocer de una reclamación, en un supuesto en el que el responsable realizaba el tratamiento de los datos en un establecimiento fuera de la UE pero que tenía una conexión con un establecimiento ubicado en la Unión.

Con el nuevo RGPD se supera esta problemática, en base al nuevo ámbito territorial establecido en el art. 3.2 que permite determinar la sujeción al Reglamento de aquellas actividades de tratamientos destinadas a ofrecer bienes o servicios a personas en la UE, o con una finalidad de control de las mismas, sin que sea necesario que exista un establecimiento en alguno de los Estados miembros.

De acuerdo al RGPD, los tratamientos transfronterizos de datos pueden entenderse en dos sentidos. Caso de una organización que tiene establecimientos en Francia y España, y el tratamiento de datos personales tenga lugar en el contexto de sus actividades, dicho tratamiento constituirá un tratamiento transfronterizo. Otra posibilidad es que la

[66] Apartado 29 STJUE *Weltimmo*.

[67] Apartado 32 STJUE *Weltimmo*.

organización solo realice actividades de tratamiento en su establecimiento de Francia. Aún en ese caso, si la actividad afecta sustancialmente, o es probable que afecte sustancialmente, a interesados de Francia y España, entonces constituirá también un tratamiento transfronterizo[68].

B. *Autoridad de control competente*

Para resolver la cuestión de la autoridad de control competente, el RGPD distingue entre la autoridad de control "principal" y las autoridades de control "interesadas". En el primer caso, será la autoridad del establecimiento principal o del único establecimiento del responsable o del encargado[69]. Mientras que las autoridades de control "interesadas" serán el resto de las autoridades a las que afecta el tratamiento por estar establecido el responsable o encargado en el territorio de su Estado miembro (sin tener allí su establecimiento principal), por ser probable que se vean sustancialmente afectados los interesados que residen en su Estado, o por haberse presentado ante ella una reclamación (art. 4.22 RGPD). En relación con los tratamientos transfronterizos opera el régimen especial de competencia previsto a favor de la autoridad de control principal (art. 56 RGPD), si bien se debe actuar conforme al procedimiento de cooperación con las autoridades de control interesadas (art. 60 RGPD). En este sentido, de acuerdo al Considerando 135 del RGPD se prevé un mecanismo de cooperación formal entre Estados a través del mecanismo de coherencia, "cuando una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros".

El objetivo perseguido por el RGPD es introducir un modelo "de ventanilla única" como régimen específico para la determinación de las autoridades de control competentes en ciertas situaciones vinculadas con dos o más Estados miembros, que evite el sometimiento cumulativo a varias autoridades de control[70].

---

[68] Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento, adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. emitido por el Grupo de trabajo sobre protección de datos del artículo 29 WP 244 rev.01. Visto en: https://www.aepd.es/.

[69] Art. 56.1 del RGPD.

[70] 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 (REDI)*, núm. 1, 2017, pp. 18-19.

Para ello, es fundamental la determinación del establecimiento principal en aquellos casos en los que el responsable o encargado tenga varios establecimientos en la Unión. Se sigue el criterio del establecimiento principal como el lugar donde se lleva a cabo su administración central, o en su caso, donde se toman las decisiones sobre los fines y medios del tratamiento de datos personales[71].

Así mismo, el RGPD prevé que el interesado presente la reclamación ante la autoridad de control del lugar de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción (art. 77.1). La norma prevé un criterio bastante flexible en cuanto al lugar donde presentar la reclamación, en favor de facilitar al reclamante de elegir el lugar que considere más idóneo o accesible, con el menor coste y menos obstáculos. Sin embargo, sí resulta relevante la autoridad de control que dicta la resolución a efectos de su impugnación ante los Tribunales judiciales (tutela judicial efectiva, art. 78 RGPD). El art. 78.3 establece que las acciones ante una autoridad de control deberán ejercitarse ante los tribunales de dicha autoridad. Aunque sólo se le permitirá tomar acciones, si la autoridad es competente en virtud de los art. 55 y 56 del RGPD, es decir, se trata del lugar de establecimiento principal o del Estado al que pertenece la autoridad pública que efectúa el tratamiento.

Las principales ventajas de este modelo son, por una parte, que contiene los elementos suficientes para determinar quién es la autoridad de control principal, y por tanto la competente para conocer del caso. Y además, en los casos de tratamientos transfronterizos se establece el deber de cooperación entre las autoridades afectadas pudiendo consensuar entre todas ellas cuál es la solución o medida más adecuada. Por su parte, para los ciudadanos implica su derecho efectivo a la tutela administrativa y facilita que no tengan que relacionarse con varias autoridades de control, sino que puedan presentar su reclamación ante la autoridad nacional donde residan (en el caso de España, la AEPD)[72]. Y este organismo realizará las gestiones pertinentes dando traslado, si procede, a otras autoridades y será la responsable de informar al interesado del resultado final de su reclamación o denuncia.

[71] ¿Qué pasa si tratamos datos en distintos países? (fecha de consulta: 23-05-2019) https://ec.europa.eu/.

[72] 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 (REDI)*, núm. 1, 2017, p. 27.

Sin duda representa una evolución del DIPr tal y como queda reflejado en la sentencia del TJUE en los asuntos *eDate Advertising* y *Martinez*[73]. Lo más destacable de la sentencia es "la facultad de elección que se le reconoce a la presunta víctima de un atentado a sus derechos de la personalidad en la red a la hora de elegir dónde ejercitar la acción de responsabilidad. Según el pronunciamiento, el perjudicado podrá ejercitar una acción de responsabilidad por la totalidad del daño causado, bien en el Estado miembro del lugar de establecimiento del emisor de los contenidos lesivos, bien ante los tribunales del Estado donde la víctima tenga su centro de intereses, lo que coincidirá normalmente con el Estado de su residencia habitual. Pero también puede optar por ejercitar su acción en cada uno de los Estados miembros en cuyo territorio el contenido publicado en Internet sea o haya sido accesible, en cuyo caso los tribunales de cada uno de esos Estados serán exclusivamente competentes para conocer de los daños sufridos en su jurisdicción"[74].

El RGPD, también permite a los interesados que sean representados en favor de entidades entre cuyos objetivos se encuentra la persecución del interés público, y dentro de este, la protección de los derechos y libertades de los interesados en materia de protección de datos. Los interesados podrán otorgar a estas entidades un mandato para la presentación de reclamaciones y ejercicios de derechos en su nombre. En algunas ocasiones, se pueden dar una duplicidad de procedimientos entre diferentes Estados miembros, por lo que los Tribunales de los diferentes países tomarán las medidas a su alcance para suspender el procedimiento que corresponda (art. 81 del RGPD).

C. *Reclamaciones ante los Delegados de Protección de Datos*

Introducido también como novedad en la LOPDGDD consecuencia de la introducción de la nueva figura del Delegado de Protección de Datos[75] (DPD) y de la finalidad protectora del Reglamento en favor de los interesados, es posible, en los casos

---

[73] STJUE de 25 de octubre de 2011, asuntos C-509/09 y C-161/10, *eDate Advertising y Martínez*, ECLI:EU:C:2011:685, apdo. 49. A mayor abundamiento, vid. FORNER DELAYGUA, J.J.: "Sentencia de 25 de octubre de 2011, Asuntos acumulados C-509/09 y C-161/10, eDate Advertising GmbH c. X y Olivier Martínez y Robert Martínez c. MGN Limited", *Revista Jurídica de Catalunya*, núm. 2, 2012, pp. 549-556.

LEIN, E.: "Competencia judicial internacional - Sentencia del Tribunal de Justicia de la Unión Europea, de 25 de octubre de 2011, asuntos acumulados C-509/09 y C-161/10, eDate Advertising GmbH c. X y Olivier Martínez y Robert Martínez c. MGN Limited", *Revista española de Derecho Internacional*, núm. 1, 2012 pp. 193-198.

[74] CORDERO ÁLVAREZ, C. I.: "Asuntos Acumulados *eDate Advertising* y *Martínez Martínez* (Sentencia del TJUE de 25 de octubre)", *Foro, nueva época,* núm. 14, 2011, pp. 267-268.

[75] Arts. 37, 38 y 39 del RGPD.

de aquellas organizaciones que cuenten con un Delegado de Protección de Datos, que la persona afectada antes de presentar una reclamación ante la Agencia de protección de Datos, se dirija en primer término al Delegado para que le atienda. El DPD comunicará al ciudadano la decisión que se hubiera adoptado en el plazo máximo de dos meses.

De igual manera, cuando el ciudadano presente una reclamación ante la agencia está podrá remitir la reclamación al responsable del tratamiento de datos o al DPD si lo hubiera para que este responda en el plazo de un mes.

La finalidad de estos procedimientos, es que el afectado pueda obtener una resolución rápida del conflicto planteado[76].

3. Tutela judicial efectiva

El RGPD reconoce la tutela judicial efectiva con respecto a las resoluciones dictadas por una autoridad de control y el derecho de indemnización contra el responsable del tratamiento o encargado por un tratamiento de datos ilícito.

3.1. Resoluciones de las autoridades de control

Con respecto a la posibilidad de recurrir una decisión de una autoridad de control, el art. 78 del RGPD contempla "el derecho a la tutela judicial efectiva contra un decisión jurídicamente vinculante de una autoridad de control que le concierna". Este derecho se podrá ejercitar ante tribunales del Estado miembro en que esté establecida la autoridad de control (art. 78.3). En el ámbito nacional, las resoluciones dictadas por la AEPD ponen vía a la vía administrativa y son recurribles, directamente, ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional (art. 48.6 LOPDGDD).

3.2. Derecho de indemnización

A. *Apunte preliminar*

Otra de las novedades que introduce el RGPD, es que reconoce explícitamente el derecho a una indemnización derivado del tratamiento ilícito de datos de carácter personal. Si bien, en la ya derogada Directiva 95/46/CE se preveía este derecho a la luz del Considerando 55 "las legislaciones nacionales deben prever un recurso judicial para

[76] Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Novedades para los ciudadanos. (fecha de consulta: 10-06-2019). https://www.aepd.es/.

los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos". Y a su vez, en el artículo 23.1, bajo el título responsabilidad, preveía el derecho de toda persona "a obtener del responsable del tratamiento la reparación del perjuicio sufrido"[77].

En el actual Reglamento, el derecho a una indemnización por los daños y perjuicios causados se encuentra recogido el art. 82. En su inciso primero, se establece la responsabilidad tanto del responsable del tratamiento como del encargado en caso de incumplimiento de las disposiciones del Reglamento[78] que causen un daño o perjuicio para el interesado. Por lo que la interposición de una reclamación ante la autoridad de control no es una vía que permita obtener la reparación del daño, es el ejercicio de acciones judiciales lo que resulta necesario para hacer efectivo el derecho a indemnización[79].

Es preciso mencionar que la acción de responsabilidad contemplada en el RGPD se refiere a una responsabilidad extracontractual, puesto que se resuelve fuera de un hipotético marco contractual. Aunque debemos destacar la existencia de una eventual responsabilidad contractual en el caso de que una empresa se haya comprometido a custodiar los datos conforme a la legislación vigente y a los fines que se determinen en el propio contrato[80], cuestión que se analiza con mayor profundidad en el siguiente capítulo.

En este punto cabe distinguir, una doble esfera de responsabilidad[81], la que se deriva del incumplimiento de las disposiciones del RGPD y sus normas de desarrollo, demostrar la ausencia de responsabilidad en el hecho que haya generado el daño, habiéndose aplicado las medidas técnicas y organizativas, tal y como dispone el art. 24 del RGPD.

Pese a que determina una responsabilidad para ambas figuras. Responde de forma general el responsable del tratamiento por cualquier incumplimiento del Reglamento que derive en un daño o perjuicio para el interesado. Y de manera excepcional, responderá el

[77] Derecho a indemnización. Art. 82 RGPD.

[78] Incumplimiento de los dispuesto en el Reglamento, incluye también las normas de desarrollo adoptadas por los Estados miembros en cumplimiento del RGPD. Considerando 146 del RGPD.

[79] SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido digital*, 2012, Tirant lo Blanch, Valencia, 2012, pp. 190-194.

[80] GONZALO DOMÉNECH, J.J.: "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, núm. 26, 2018, pp. 413-415.

[81] LÓPEZ ÁLVAREZ, L. F.: *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, Madrid, 2016, p. 176.

encargado en caso de incumplimiento de las disposiciones del Reglamento, o cuando haya actuado al margen o contra las instrucciones del responsable[82]. Cabe entender como lógica esta limitación, puesto que el encargado del tratamiento actúa por mandato del responsable[83].

Por su parte, la LOPDGDD no establece nada al respecto, de manera que hay que atener a lo dispuesto en el RGPD.

B. *Alcance*

A diferencia de las reclamaciones contra la autoridad de control, las acciones por vía judicial tienen lugar ante los tribunales del orden civil (salvo que el responsable o encargado sea una administración pública). El recurso a la vía judicial no está únicamente ligado a la reclamación de una indemnización por tratamiento ilícito de datos, sino también puede resultar más eficaz y útil para logar una limitación o prohibición de tratamiento, que lo que supondría una reclamación ante la autoridad de control. Así se pone de relieve, por ejemplo en la STS (Sala de lo Civil) de 15 de octubre de 2015[84] en la que se reclama por parte del demandado a un periódico editor de una noticia la adopción de medidas para que la información relevante no pueda ser indexada por los motores de búsqueda, junto con la correspondiente indemnización por los daños sufridos[85].

Respecto al objeto que se debe indemnizar, son indemnizables los daños y perjuicios materiales o inmateriales; es decir, se cubren tanto los daños físicos como morales, interpretándose el concepto de "daños y perjuicios" conforme la interpretación del TJUE[86], por lo que se viene a buscar una reparación integral del daño sufrido. En cuanto a los daños morales, destacamos desde la perspectiva española, la reciente STS 261/2017, de 26 de abril[87] en la que establece los criterios para evaluar el daño moral por el incumplimiento de los requisitos de la legislación sobre protección de datos. En ella, el Tribunal considera como relevantes: 1) el tiempo de permanencia de los datos; 2) el

[82] Art. 82.2 del RGPD.

[83] RECIO GAYO, M.: "Acerca de la evolución de la figura del encargado del tratamiento", *Revista de Privacidad y Derecho Digital*, núm. 0, 2015, p. 37.

[84] STS 15 de octubre de 2015 (ECLI:ES:TS:2015:4162).

[85] 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 (REDI)*, núm. 1, 2017, pp. 24-25.

[86] Considerando 146 del RGPD.

[87] STS de 26 de abril de 2017 (ECLI:ES:TS:2017:1645).

alcance de la divulgación de los datos personales a terceros, y 3) la inacción del Responsable del tratamiento[88].

3.3. Interrelación con las reclamaciones ante una autoridad de control

Como se ha mencionado al inicio del capítulo, estas dos vías de reclamación son independientes entre sí, no excluyentes y además pertenecen a dos órdenes jurisdiccionales diferentes, las reclamaciones ante una autoridad de control al ámbito administrativo, mientras que la reclamación de indemnización se ejercita a través del orden civil. En este sentido, el RGPD no prevé ningún mecanismo de coordinación entre estas dos vías. Esta dualidad de órdenes jurisdiccionales competente se ha traducido en una falta de homogeneidad a la hora de interpretar conceptos en materia de protección de datos, como así se evidencia de las resoluciones emitidas por la Sala de lo Civil y la Sala de lo Contencioso del Tribunal Supremo respecto de las reclamaciones contra Google[89]. Es el caso del concepto de responsable del tratamiento, en cuanto a sujeto responsable por un tratamiento ilícito de datos. En la sentencia *Google Spain* la Sala de lo Contencioso determinó que la Sociedad matriz (Google Inc.) ubicada en Estados Unidos era la responsable del tratamiento de los datos, mientras que la Sala de lo Civil atribuía también corresponsabilidad a su filial en España, Google Spain S.L., por dicho tratamiento[90].

[88] GONZALO DOMÉNECH, J.J.: "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana de Derecho*, núm. 26, julio 2018, pp. 413-415.

[89] STS (Sala de lo Civil) de 5 de abril de 2016 ECLI:ES:TS:2016:1280, relativa al llamado derecho al olvido, y las sentencias 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).

[90] DE MIGUEL ASENSIO, P.A.: "La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google", *Diario La Ley*, núm. 8773, 2016, pp. 1-6.

CAPÍTULO III. CUESTIONES DE DERECHO INTERNACIONAL PRIVADO EN EL RGPD

1. Observaciones iniciales

Con respecto a la tutela judicial en materia civil, reviste particular importancia las novedades introducidas en el RGPD con respecto a las normas preexistentes de Derecho Internacional Privado, en materia de competencia judicial, litispendencia y ley aplicable.

En el presente capítulo se analiza los preceptos dedicados a esta materia así como su interrelación con la normativa vigente de DIPr.

2. Competencia judicial internacional

2.1. Regulación en el RGPD

En lo relativo a la competencia judicial, el RGPD introduce en su Considerando 147 que, siguiendo el principio de especialidad normativa, la aplicación de las normas generales sobre competencia judicial, como las establecidas en el Reglamento (UE) nº 1215/2012 del Parlamento Europeo y del Consejo[91], se aplicarán sin perjuicio de las específicas normas contenidas en el Reglamento sobre competencia judicial, en particular por lo que respecta a "*las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento*".

Por su parte, el artículo 82.6 del RGPD relativo al ejercicio de las acciones judiciales por parte del interesado para reclamar una indemnización contra el responsable o encargado del tratamiento a causa de un tratamiento de datos ilícito, establece que dichas acciones *"se presentarán ante los tribunales competentes con arregla al Derecho del Estado miembro que se indica en el artículo 79, apartado 2"*.

A su vez, el 79.2 RGPD determina que dichas acciones *"deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento"*. Teniendo en cuenta el concepto amplio de "establecimiento" conforme lo desarrollado en el capítulo relativo al ámbito territorial de aplicación (Cap. 1). Y como foro alternativo, *"tales acciones podrán ejercitarse ante los tribunales del Estado*

[91] 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 (*DOUE* 351, 20-XII-2012).

miembro en que el interesado tenga su residencia habitual"[92], con la excepción de que el responsable o encargado sea una autoridad pública qué actúe en ejercicio de sus poderes públicos.

De esta manera, se garantiza la tutela judicial efectiva de los interesados para reclamar una indemnización[93]. Si bien, el foro está delimitado a acciones judiciales contra el responsable o encargado del tratamiento como únicos dos sujetos responsables de un tratamiento ilícito de datos[94]. Para los supuestos en los que más de un responsable o encargado del tratamiento, o un responsable y un encargado, sean responsables del daño o perjuicio causado por dicho tratamiento, el Reglamento prevé que cada uno de ellos será considerado responsable de los daños causados, a fin de indemnizar al interesado[95]. Y a su vez, si únicamente uno de ellos abona la indemnización, podrá dirigirse contra los demás a fin de reclamar a la parte de indemnización correspondiente a su parte de responsabilidad[96].

2.2. Naturaleza de las acciones

Estas acciones judiciales tienen naturaleza "civil-mercantil" y, por lo tanto, se encuadran dentro del ámbito de aplicación del artículo 1.1 del Reglamento (UE) 1215/2012 "Bruselas I Bis"[97] ("RBIbis"), cuya materia no está excluida en los supuestos de exclusión del artículo 1.2. Lo que implica la interacción entre lo dispuesto en el art.79.2 del RGPD y lo dispuesto en el RBIbis.

Como ya se mencionaba en el capítulo precedente, la tutela judicial efectiva amparada en el art. 82.6 del RGPD a causa de un tratamiento ilícito de datos, podría considerarse como una indemnización por responsabilidad extracontractual derivada de un incumplimiento de las disposiciones del RGPD. Pero puede darse el caso, que entre el responsable y el interesado medie un contrato (caso de un prestador de servicios de la sociedad de la información) y según la jurisprudencia del TJUE, una acción de

[92] En concordancia con lo establecido en el Considerando 145 RGPD.

[93] ÓRTEGA GIMÉNEZ, A.: *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal*, Aranzadi, Navarra, 2017, pp. 51-54.

[94] Art. 79.2 del RGPD.

[95] Art. 82.4 del RGPD.

[96] Art. 82.5 del RGPD.

[97] 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. *DOUE* 351/1, de 20-XII-2012.

responsabilidad civil de naturaleza extracontractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del Reglamento "Bruselas I Bis" si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales cuando se estudie caso por caso el objeto del contrato[98]. Puesto que en un contrato se puede pactar el compromiso del cuidado de los datos personales en virtud de la legislación vigente; aunque la mayoría de los supuestos que nos encontraremos en la práctica serán de naturaleza extracontractual[99].

Pese a todo, teniendo en cuenta la naturaleza protectora que otorga el RGPD a favor del interesado, y a falta una mención expresa en el art. 79, no cabe excluir el foro especial contenido en el art. 79.2 RGPD cuando se ejerce una acción judicial en la que medie un contrato entre el responsable e interesado por la vulneración de las disposiciones contenidas en el RGPD[100].

A. *Foro del establecimiento*

El primero de los foros comprendidos en el art. 79.2 del RGPD, permite demandar en el Estado miembro en el que el responsable o el encargado tengan un establecimiento.

Como ya se ha mencionado, el RGPD recoge un concepto flexible y amplio de "establecimiento", que lo hace extensible "*a cualquier actividad real y efectiva, aún mínima, ejercida mediante una instalación estable*"[101]. También es relevante al respecto, la STJUE *Amazon EU Sàri*[102] donde se indica que es posible considerar la existencia de un establecimiento en un Estado miembro cuando no exista ni una filial o sucursal, siendo necesario valorar el grado de estabilidad de la instalación y la efectividad del desarrollo

[98] STJUE de 13 de marzo de 2014, asunto C-548/12, *Brogsitter*, ECLI:EU:C:2014:148; y STJUE de 14 de julio de 2016, asunto C-196/15, *Granarolo*, ECLI:EU:C:2016:559.

[99] GONZALO DOMÉNECH, J.J.: "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana. de Derecho*, núm. 26, julio 2018, p. 418.

[100] 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 (REDI)*, núm. 1, 2017, pp. 29-30.

[101] Apartados 31 de la STJUE *Weltimmo* y apartado 75 de la sentencia *Verein für Konsumenteninformation* (STJUE de 28 de julio de 2016, *Verein für Konsumenteninformation*, asunto C-191/15, ECLI:EU:C:2016:612).

[102] STJUE de 21 de diciembre de 2016, asunto C-362/14, *Amazon EU Sàrl*. ECLI:EU:C:2015:650.

de las actividades en ese Estado[103], siendo posible considerar como "establecimiento" un representante de la sociedad si actúa con un grado de estabilidad suficiente[104].

De esta consideración se desprende que cualquier establecimiento del encargado o del responsable permite atribuir la competencia a los tribunales del Estado miembro en el que esté sito. Tampoco será necesario que la acción esté dirigida a las actividades de ese concreto establecimiento, sino que la existencia de cualquier establecimiento extiende el daño causado[105].

A pesar de que en muchas situaciones el "establecimiento" coincidirá con el Estado en el que se localiza el domicilio del demandado en el sentido del fuero general del art. 4.1 RBIbis, son dos categorías diferentes. El art. 62 del RBIbis para las personas físicas, conduce a la ley interna del foro para determinar si el demandado está ahí domiciliado. Por su parte, el art. 79.2 del RGPD no utiliza ese concepto de domicilio al atribuir competencia a los tribunales de cualquier Estado miembro en el que tenga un "establecimiento".

El objetivo de garantizar los derechos de los afectados, justifica el empleo del concepto amplio y flexible de "establecimiento" como fuero de competencia. Además, de él también se infiere que pueda servir para atribuir competencia a tribunales de Estados miembros que no la tendrían con base en el art. 4 del RBIbis o incluso otras normas de competencia de ese instrumento, lo que podría ser de particular utilidad en relación con el ejercicio de acciones colectivas por parte de interesados procedentes de diversos Estados.

Sobre esta cuestión, reviste particular interés la STJUE *Schrems contra Facebook*[106], a pesar de que esta sentencia acaparó mucha atención por la declaración de invalidez de la Decisión 2000/520/CE de la Comisión relativa a los principios de puerto seguro[107], el Tribunal Austriaco conocedor del asunto planteó una cuestión prejudicial al

---

[103] Apartados 76 y 77 STJUE *Amazon EU Sàrl*.

[104] Apartado 30 de la STJUE *Weltimmo.*

[105] GONZALO DOMÉNECH, J.J.*:* "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos", *Revista Boliviana. de Derecho*, núm. 26, julio 2018, p. 419.

[106] STJUE de 25 enero 2018, *Maximilian Schrems* y *Facebook Ireland Limited*, asunto C-498/16, ECLI:EU:C:2018:37. A mayor abundamiento, vid. GUTIÉRREZ COLOMINAS, D.: "Schrems v Facebook: the consumer definition in the framework of digital social networks", *European Data Protection Law Review*, núm. 4, 2018, pp. 542-546. CAAMIÑA DOMÍNGUEZ, C.M.: "La noción de "consumidor" en internet: El asunto C-498/16, Maximilian Schrems y facebook Ireland Limited", *Cuadernos de derecho transnacional*, núm. 1, 2019, pp. 711-721.

[107] Esta Decisión constituía el marco normativo a través del cual era posible la transferencia internacional de datos entre los estados Unidos y la Unión Europea, al considerar que quien se adhería a este sistema

TJUE sobre la interpretación de la definición de "consumidor"[108] del artículo 15 del Reglamento (CE) nº44/2001[109] (derogado por el actual RBIbis), en el caso de una cuenta privada de Facebook y si el artículo 16 del citado Reglamento, debe interpretarse en el sentido de que un consumidor también puede ejercitar en un Estado miembro, en el fuero del demandante, junto con sus propias acciones derivadas de un contrato celebrado con consumidores, pretensiones en idéntico sentido de otros consumidores con residencia en el mismo Estado miembro, en otro Estado miembro, o bien en un tercer país que, derivadas de contratos celebrados por consumidores con la misma parte demandada y en el mismo contexto jurídico, le hayan sido cedidas por dichos consumidores, siempre que el contrato de cesión no se inserte en una actividad empresarial o profesional del demandante, sino que persiga el ejercicio colectivo de las pretensiones[110].

En aquella ocasión, el TJUE, siguiendo el criterio expuesto por el Abogado General[111], dictaminó que el demandante no tenía derecho a ejercer acciones contra Facebook Irlanda cedidas por otros consumidores domiciliados en el mismo país de la UE u otros países porque ello permitiría acumular acciones en una jurisdicción determinada y escoger los tribunales más favorables en el caso de acciones colectivas cediendo todas al consumidor con domicilio en dicha jurisdicción más favorable[112].

garantizaban un nivel adecuado de protección. DE MIGUEL ASENSIO, P.A.: "Aspectos internacional de la protección de datos: la sentencia *Schrems* y *Weltimmo* del Tribunal de Justicia", *La Ley Unión Europea*, núm. 31, 2015, pp. 3-4.

[108] Vid. STJUE de 25 de enero de 2018, asunto C-498/16, *Schrems* (ECLI:EU:C:2018:37) que es en la que se analiza el «fuero del consumidor» en relación con las acciones civiles ejercitadas por el Sr. Schrems contra Facebook. A mayor abundamiento, vid. MORENO GARCÍA, L.: "Delimitación del «fuero del consumidor» en asuntos relacionados con redes sociales y protección de datos", *Diario La Ley*, núm. 9270, 2018, pp. 1-17. GONZALO DOMENECH, J.J.: "El régimen de corresponsabilidad en el tratamiento en una red social y el régimen de competencia de una autoridad de control: comentario a la STJUE de 5 de junio de 2018", *Diario la Ley*, núm. 9258, 2018, pp. 1-18. DE MIGUEL ASENSIO, P.A.: "Demandas frente a redes sociales por daños en materia de datos personales: precisiones sobre competencia judicial", *La Ley Unión Europea*, núm. 56, 2018, pp. 1-11.

[109] Reglamento (CE) nº 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. (*DOUE* 12, 16-I-2001).

[110] FONT I SEGURA, A.; OTERO GARCÍA-CASTRILLÓN, C.: "Crónica de actualidad de Derecho Internacional Privado (Julio - Diciembre 2016)", *Revista electrónica de estudios internacionales (REEI)*, núm. 33, 2017, p. 27.

[111] TJUE. Conclusiones del Abogado General en el asunto C-498/16 Maximilian Schrems / Facebook Ireland Limited. (fecha de entrada: 14-11-2017) https://curia.europa.eu/.

[112] Apartados 45 y 49 de la STJUE de 25 enero 2018, *Maximilian Schrems* y *Facebook Ireland Limited*.

B. *Residencia habitual*

Como foro alternativo, se prevé que los afectados puedan demandar en los tribunales del Estado donde tengan su residencia habitual. Para la consideración de la residencia habitual, será necesario que el interesado tenga un grado de permanencia que revele una situación de estabilidad[113]. La residencia habitual no es un concepto sinónimo al de "centro de intereses de la víctima" emanado de la jurisprudencia del TJUE[114], como criterio atributivo de la competencia para concretar el lugar donde se ha producido el daño a los efectos del art. 7.2 del RBIbis, en los supuestos de lesión de un derecho de la personalidad a través de Internet.

Puede darse el caso de que una persona tenga su centro de intereses en un Estado miembro donde no resida habitualmente cuando exista un vínculo particularmente estrecho con ese otro Estado, como el ejercicio de una actividad profesional. La consideración de este foro de competencia no parece ser la más adecuada para determinar el tribunal que debe conocer de la pretensión, puesto que no exige que exista una vinculación entre el centro de intereses y el lugar donde efectivamente se produce el daño[115].

A falta de restricciones y teniendo en cuenta la naturaleza protectora de la norma, se infiere que el alcance de la competencia fundada en la residencia habitual del interesado se extiende también al conjunto del daño que el tratamiento por el demandado le haya causado, de modo que no se limita al producido en el Estado de su residencia habitual[116].

2.3. Compatibilidad entre el RGPD y las normas de DIPr

La compatibilidad entre los foros de competencia del artículo 79.2 y los del RBIbis se extrae de lo dispuesto en artículo 67 de este último Reglamento, al estipular que no prejuzgará la aplicación de las disposiciones contenidas en instrumentos particulares, como es el caso del artículo 79.2 del RGPD. Por su parte, el Considerando 147 del RGPD

[113] STJUE de 22 de diciembre de 2010, *Mercredi*, asunto C-497/10, ECLI:EU:C:2010:829.

[114] STJUE *eDate Advertising*, C-509/09 y C-161/10, ECLI:EU:C:2011:685.

[115] OREJUDO PRIETO DE LOS MOZOS, P.: "La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia", *La Ley Unión Europea*, núm. 4, 2013, p. 23.

[116] 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 (REDI)*, núm. 1, 2017, pp. 33-34.

afirma que las normas generales de competencia judicial del RBIbis "deben entenderse sin perjuicio de la aplicación de las normas específicas del RGPD". El Considerando 145 estipula que el demandante "deberá tener la opción" de ejercitar las acciones en los tribunales de los Estados miembros.

Por lo tanto, cabe entender que los foros reconocidos en el RGPD son complementarios a los del RBIbis, teniendo la posibilidad el interesado de acogerse a ellos si concurren las circunstancias necesarias, en el caso concreto[117]. Estos foros alternativos podrían ser la prórroga de jurisdicción, que comprende la sumisión expresa (art. 25 RBIbis) también conocida como la prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional[118] y la sumisión tácita (art. 26 RBIbis), si bien en la práctica resultará poco frecuente que el interesado pretenda hacer valer esta posibilidad en detrimento de la competencia de los Estados miembros designados por el art. 79.2 del RPD que tiene carácter preferente. El fuero general del domicilio del demandado (art. 4 RBIbis), que normalmente coincidirá con un Estado miembro en el que el demandado tenga "un establecimiento" a los efectos del art. 79.2, los fueros basados en una relación de conexidad (art. 8 RBIbis que incluye el de la pluralidad de demandados), o el fuero especial en materia extracontractual del art. 7.2 RBIbis.

Lo que puede añadir este último foro especial en materia extracontractual en comparación con el foro del art.79.2 del RGPD, es que permitiría no sólo demandar por la totalidad del daño causado ante los tribunales del Estado donde tuviese el "centro de intereses" la víctima, conforma la interpretación ya mencionada del TJUE en la sentencia *eDate Advertising*, sino también, aunque con alcance limitado, ante los tribunales de otros lugares de manifestación del daño[119], como por ejemplo donde se hayan divulgado los datos. Este criterio ha sido interpretado por el TJUE en relación con derechos de propiedad intelectual[120] pero falta que se pronuncie sobre su viabilidad en un litigio referido a derechos de la personalidad.

Como ya se ha mencionado, el carácter protector del RGPD y la ausencia de previsiones que digan lo contrario, hace que las acciones contra el responsable o

[117] Vid. STJUE de 20 de mayo de 2010, *Česká podnikatelská v. Michal Bilas*, C-111/09; STJUE de 28 de enero de 2015, *Kolassa*, C-375/13, EU:C:2015:37.

[118] ORTEGA GIMÉNEZ, A.: "Imagen y circulación internacional de datos", *Revista boliviana de Derecho*, núm. 15, 2013, p. 138.

[119] STJUE *eDate Advertising y Martinez*, apartados 41 a 44.

[120] STJUE de 3 de octubre de 2013, asunto C-170/12, *Pinckney*, ECLI:EU:C:2013:635 y de STJUE de 22 de enero de 2015, asunto C-441/13, *Hejduk*, ECLI:EU:C:2015:28.

encargado contempladas en el art. 79.2 RGPD sean extensibles no sólo a acciones por responsabilidad extracontractual sino también contractual, siempre que se hayan vulnerado las disposiciones del RGPD. Salvo la excepción, de que sea materia contractual y la persona física tenga la consideración de consumidor, podrán ser de aplicación las normas de protección de los consumidores contempladas en los arts. 6.1 y 17 a 19 del RBIbis, y en su caso, el art. 22 quinquies de la LOPJ[121], que conducen igualmente a atribuir competencia a los tribunales del domicilio del consumidor o interesado con respecto a acciones contractuales.

3. Litispendencia

En el art. 80 del RGPD, enunciando como "suspensión de los procedimientos", se regulan los casos en los que pueda existir una duplicidad de acciones contra el mismo responsable o encargado por los mismos hechos. En este sentido, en el apartado segundo se dice que deberán suspender el procedimiento aquellos tribunales distintos a aquel donde se inició el procedimiento. Y en el apartado tercero, se establece que cuando el caso esté pendiente en primera instancia, cualquier parte interesada podrá solicitar la inhabilitación de otros tribunales en favor del tribunal donde se iniciaron las acciones, siempre que sea el competente y la acumulación, si procede, sea conforme a derecho.

Estas reglas parecen desplazar a las reglas de litispendencia y conexidad de los arts. 29 y 30 del RBIbis.

Aunque pueda parecer que el art. 80 del RGPD se refiere a acciones judiciales en materia civil, teniendo en cuanta lo dispuesto en el Considerando 144 del RGPD parece que estás reglas de litispendencia se refieren a reclamaciones hechas contra las resoluciones de las autoridades de control, ya que se dice que "si un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento", por lo tanto serían aplicables en el orden administrativo pero en materia civil sería de aplicación las reglas contenidas en el RBIbis.

Para apoyar esta interpretación, se añade lo dispuesto en el Considerando 147 del RGPD que establece el principio de especialidad normativa del RGPD respecto a otras normas con la única referencia a "normas específicas sobre competencia judicial". Las

[121] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. *BOE*, núm. 157, 02-VII-1985.

normas sobre litispendencia y conexidad entre tribunales de Estados miembros del RBIbis se vinculan con su sistema de reconocimiento y ejecución, por lo que resulta apropiado que esas disposiciones del RBIbis sigan siendo aplicables al ejercicio de acciones de responsabilidad civil por la infracción de la normativa sobre protección de datos[122].

4. Ley aplicable

Por lo que respecta a la ley aplicable, no hay un artículo o Considerando en el texto del RGPD dedicado a esta cuestión, por lo que surge la necesidad de observar otras normas generales nacionales e internacionales que lo regulen. Como previamente se ha mencionado, en el capítulo relativo al ámbito de aplicación territorial (cap. 1), la aplicación del RGPD tiene carácter imperativo siempre que se vulneren sus disposiciones en materia de protección de datos. Incluso en el seno de un litigio entre particulares, ya sea de naturaleza contractual o extracontractual, será de aplicación el Reglamento siempre que haya existido una vulneración o incumplimiento contractual en materia de protección de datos, es decir, siempre que se englobe dentro de su ámbito de aplicación. A pesar de que dicha relación contractual o responsabilidad civil se rija por la ley de un tercer Estado, de conformidad con el Reglamento (CE) 594/2008 "Roma I"[123]. Incluso en estos casos, las partes pertenecientes a los Estados miembros deberán aplicar el RGPD en la medida que se englobe dentro de su ámbito de aplicación[124]

Ahora bien, en el marco de un litigio en materia civil, como son las acciones judiciales del derecho a una indemnización, el RGPD resulta insuficiente en cuanto que no recoge previsiones específicas sobre, por ejemplo, las reclamaciones de los daños en materia civil, sino únicamente una previsión general acerca de los sujetos responsables y el alcance amplio de los daños y perjuicios causados. Esto conlleva que habrá que estar a lo dispuesto en las leyes nacionales de los Estados miembros, como legislación general sobre esta cuestión. Lo que se traduce en una gran inseguridad jurídica, incremento de

[122] 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 (REDI)*, núm. 1, 2017, pp. 38-39.

[123] Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I). *DOUE* L 177/6, 4-VII-2008.

[124] 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 (REDI)*, núm. 1, 2017, pp. 39-41. ÓRTEGA GIMÉNEZ, A.: *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal*, Aranzadi, Navarra, 2017, pp. 55-62.

costes, dificultades para el demandante, ya que será necesario observar una pluralidad de ordenamientos jurídicos con disparidad de normas al respecto, y con su consiguiente jurisprudencia.

En el caso de España, será preciso acudir a lo dispuesto en las normas nacionales. Esto es, a lo dispuesto en el art. 10.9 CC[125], "*las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven*", lo que en muchos casos se corresponderá con la ley del lugar de la residencia habitual (o centro de intereses) del interesado[126], al menos, a falta de un regulación armonizada se corresponde con el propósito perseguido por el RGPD[127].

De igual manera, en las transferencias internacionales de datos pueden surgir importantes problemas en cuanto a la delimitación y determinación de la ley aplicable. Para resolverlo, parece apropiado acudir a la normativa internacional que sería de aplicación, esto es, el Reglamento (CE) 864/2017 "Roma II" [128] relativo a la ley aplicable a las obligaciones extracontractuales, que además tiene carácter universal y no únicamente para los Estados miembros. Sin embargo, no parece posible aplicar esta norma pues de acuerdo a su art. 1.2 g) del, el RR II no es aplicable a "*las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación*". Por tanto, las acciones extracontractuales relativas a los daños y perjuicios sufridos por un interesado como consecuencia del tratamiento de sus datos personales por un responsable o encargado están excluidas de la norma, exclusión que ha sido criticada por la doctrina[129].

Para revertir esta situación, actualmente existe una propuesta de reforma[130] para

---

[125] Código Civil. *BOE* núm. 206, 25-VII-1889.

[126] SANCHO VILLA, D.: *Negocios internacionales de tratamiento de datos personales*, Civitas, Navarra, 2010, pp. 99-107.

[127] Art. 79.2 del RGPD: "*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. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos*".

[128] Reglamento (CE) n° 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). *DOUE* L 199/40, 31-VII-2007.

[129] SANCHO VILLA, D.: *Negocios internacionales de tratamiento de datos personales*, Civitas, Madrid, 2010, pp. 97- 98.

[130] Resolución del Parlamento Europeo, de 10 de mayo de 2012, con recomendaciones destinadas a la Comisión sobre la modificación del Reglamento (CE) nº 864/2007 relativo a la ley aplicable a las obligaciones extracontractuales (Roma II). P7_TA-PROV(2012)0200. (fecha de consulta: 02-07-2019). http://www.europarl.europa.eu/.

modificar el RR II con el objetivo de que sea de aplicación una única norma de conflicto y desplazar así a la legislación interna. Esto, tendría consecuencias muy beneficiosas en el sentido de que de las partes involucradas en un litigio internacional privado por la vulneración del derecho a la protección de datos pueden acudir a un régimen único, evitando así observar las específicas normas de conflicto de los Estados y su jurisprudencia. También conllevaría una mayor seguridad jurídica, reducción de costes para la persona perjudicada, y menor desigualdad entre el causante del daño y la persona perjudicada.

Esta propuesta de modificación del RR II, conllevaría la introducción de un nuevo art. 5 bis (Privacidad y derechos relacionados con la personalidad), en el que se introducirían dos nuevos supuestos o puntos de conexión:

1. "*La ley aplicable a las obligaciones extracontractuales derivadas de violaciones de la privacidad o de los derechos relacionados con la personalidad, incluida la difamación, será la del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del daño o perjuicio*".

2. "*No obstante, la ley aplicable será la del país de residencia habitual del demandado si esta persona no puede haber previsto razonablemente consecuencias importantes de su acto en el país designado en el apartado 1*".

El primer supuesto adopta los criterios de la *lex loci damni* (la ley del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del daño) o *lex loci delicti commissi* (la ley del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del hecho lesivo) [131], que tiene un criterio localizador pero que no necesariamente tiene que coincidir con la residencia o centro de intereses del demandante, lo que pone en duda que pueda llegar a proteger a la parte perjudicada.

Mientras que el segundo supuesto, parece favorecer al responsable del daño[132], pues permite aplicar la ley del país de residencia del demandado cuando resulte imposible

[131] GONZALO DOMENECH, J.J.: "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros", *Cuadernos de Derecho Transnacional*, núm. 1, 2019, pp. 427-430. CARRASCOSA GONZÁLEZ, J.: "La protección de los datos personales en un escenario tecnológico supranacional *Cloud Computing*, tribunales competentes y ley aplicable", VALERO TORRIJOS, J. (aut.), *La protección de datos personales en internet ante la innovación tecnológica riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Navarra, 2013, pp. 113-128.

[132] ORTEGA GIMÉNEZ, A.: *Transferencias internacionales de datos de carácter personal ilícitas*, Aranzadi, Navarra, 2017, pp. 158-160.

determinar el elemento o los elementos más significativos del daño o perjuicio (elemento objetivo); y b) que el causante del daño no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país (elemento subjetivo). Conforme a esta propuesta de reforma puede llevar a que se beneficie al causante del daño pues permite aplicar la ley del lugar residencia del demandado. La consecuencia de la no regulación conlleva a la aplicación de normas autónomas como el artículo 10.9 del CC, que hace que apliquemos la ley del lugar donde se ha cometido el hecho (*lex loci delicti commissi*). Además, la precisión del lugar en el que se produce el daño puede resultar controvertida en situaciones en las que las consecuencias lesivas del hecho dañoso no son de carácter material, y esta norma no precisa cuál es el lugar del daño en las situaciones en las que el hecho causal y el resultado lesivo se producen en distintos países[133].

[133] DE MIGUEL ASENSIO, P. A.: *Derecho privado de Internet*, Civitas, Madrid, 2015, p. 201.

CAPÍTULO IV. TRANSFERENCIAS INTERNACIONALES DE DATOS

1. Reseña introductoria

Ni la Directiva 95/46/CE ni el RGPD define qué se entiende por transferencia internacional de datos. Sin perjuicio de que la definición de transferencia no es nada fácil[134], sobre todo en un mundo tecnificado como el actual, si es posible identificar los presupuestos que nos sitúan ante una transferencia internacional sometida al Reglamento[135].

Desde un punto de vista general, "una transferencia internacional de datos se produce cuando los datos personales que son tratados por un responsable o encargado del tratamiento en el Espacio Económico Europeo (países de la Unión Europea más Islandia, Liechtenstein y Noruega) son enviados a un tercer país u organización internacional, fuera de dicho territorio"[136].

Desde un punto de vista nacional, se consideraría transferencia internacional de datos todo flujo de datos que parta desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo[137].

Para entender mejor qué es una transferencia internacional de datos, conviene analizar de manera autónoma cada uno de los elementos que las componen[138]:

Primero: Debe tratarse de datos de carácter personal; esto es, de "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". Entendiendo por "tratamiento", "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no*" [139].

---

[134] ABERASTURI GORRIÑO, U.: "Movimiento internacional de datos. Especial referencia a la transferencia internacional de datos sanitarios", *Revista de administración pública*, núm. 186, 2011, pp. 333-340.

[135] PIÑAR MAÑAS, J.L.: "Transferencias de datos personales a terceros países u organizaciones internacionales", PIÑAR MAÑAS J.L. (Dir.) / ÁLVAREZ CARO, M.; RECIO GAYO, M. (Coords.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Barcelona, 2016, pp. 431.

[136] Art. 44 del RGPD.

[137] Transferencias internacionales (fecha de consulta: 22-04-2019). https://www.aepd.es/.

[138] ORTEGA GIMÉNEZ, A., *Transferencias internacionales de datos de carácter personal ilícitas*, Aranzadi, Navarra, 2016, p. 23.

[139] Art. 4.2 del RGPD.

Segundo: Los datos de carácter personal que vayan a transmitirse vienen referidos tanto a aquellos que son tratados de forma automatizada (movimientos realizados por medios informatizados) como a los tratados de forma no automatizada (aquellos realizados por medios convencionales).

Tercero: La transferencia internacional de datos se efectúa con el objeto de realizar un tratamiento de datos de carácter personal por parte del destinatario de los mismos, ya sea tanto cesión (a otro responsable[140]) como prestación de un servicio (encargado de tratamiento[141]).

Cuarto: El traslado físico efectivo de los datos de carácter personal, de un lugar del Espacio Económico Europeo a cualquier otro Estado, región, u Organización Internacional.[142]

Quinto: El lugar de destino de los datos de carácter personal debe encontrarse en un territorio externo al EEE o de las partes no contratantes.[143]

Sexto: Existirá transferencia internacional de datos personales en cualquiera de los dos casos siguientes: cuando constituya una cesión o comunicación de datos o cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable.

Misma interpretación se desprende de la STJUE[144] en el caso *Lindqvist*, que lleva a concluir que el tratamiento en que consiste una transferencia de datos es el envío de información a un país tercero o a una organización internacional. En este sentido, facilitar o poner a disposición información en internet no implicaría una transferencia de datos[145]. Sin embargo, la prestación de servicios de computación en la nube o *cloud computing* si,

[140] Art. 4.7 RGPD: «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

[141] Art. 4.8 RGPD: «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

[142] GONZALO DOMENECH, J.J.: "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros", *Cuadernos de Derecho Transnacional*, núm. 1, 2019, pp. 353-354.

[143] *Ibídem*.

[144] STJUE, de 6 de noviembre de 2003, asunto C 101-01, *Lindqvist* (ECLI:EU:C:2003:596). A mayor abundamiento, 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.

[145] PIÑAR MAÑAS, J.L.: "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, núm. 19-20, 2013, pp. 58-60. Y ORTEGA GIMÉNEZ, A.: "Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE "*Lindqvist*", de 6 de noviembre de 2013", *Revista de derecho de Extremadura*, núm. 7, 2010, pp. 101-105.

pues es un caso donde hay tratamiento de datos que exigen el envío de información, en su caso a terceros países[146].

2. Regulación y tipología de transferencias internacionales de datos

2.1. Regulación

Se regulan en el Capítulo V del RGPD, artículos 44 a 50, con el nombre de "transferencias de datos personales a terceros países u organizaciones internacionales". Mientras que en la LOPDGDD se regulan en su Título VI, "transferencias internacionales de datos". En el Directiva 95/46/CE re regulaban únicamente en los artículos 25 y 26[147]. Pasando de dos a seis artículos conforme la legislación vigente. Ya sólo este dato es indicativo de la importancia que han adquirido las transferencias internacionales en un mundo globalizado y conectado como el actual[148].

2.2. Principio general

El principio general de las transferencias internacionales ha evolucionado con el nuevo RGPD, conforme el régimen anterior de la Directiva 95/46/CE, las transferencias internacionales solamente eran posibles si el tercer país garantizaba un nivel adecuado de protección (art. 25.1). Sin embargo, el RGPD introduce un nuevo supuesto de legitimación, junto al de garantizar el nivel adecuado de protección (art. 45), también son posibles cuando el responsable o encargado ofrezcan garantías adecuadas (art. 46). Dentro de ese último tipo se incluyen las normas corporativas vinculantes (art. 48). De no darse estos supuestos, solamente serán posibles si se encuadran dentro de alguno de los supuestos de excepción contemplados en el art. 49.

Por lo tanto, se puede decir que existen dos de tipos de transferencias de datos, atendiendo al criterio del país de destino[149]:

---

[146] ÁLVAREZ RIGAUDIAS, C.: "Condiciones para las transferencias internacionales de datos personales en servicios de *cloud*", MARTÍNEZ MARTÍNEZ, R. (Ed.), *Derecho y Cloud Computing*, Aranzadi, Navarra, 2012, pp. 5-6.

[147] Y Considerandos 56 a 60.

[148] PIÑAR MAÑAS, J. L.: "Transferencias de datos personales a terceros países u organizaciones internacionales", ÁLVAREZ CARO, M. / RECIO GAYO, M. (Coord.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Edición I, Reus, Madrid, 2016, pp. 428-429.

[149] ORTEGA GIMÉNEZ, A.: *Transferencias Internacionales de Datos de Carácter Personal Ilícitas*, Aranzadi, Navarra, 2017, pp. 55-59.

1) Las transferencias a Estados miembros de la UE. Serían los casos de "tratamientos trasfronterizos"[150], quedan amparadas bajo lo establecido en el RGPD, por cumplir con los requisitos específicos de la ley se presumen que "cuentan con un nivel adecuado de protección".

2) Transferencias a terceros Estados u organización internacional fuera de la UE. Aquí se incluyen las transferencias internacionales de datos.

2.3. Tipología

Como se ha mencionado, el primero de los supuestos permitidos es cuando el tercer país u organización internacional garantiza un nivel adecuado de protección declarado por la Comisión Europea. En virtud de lo establecido en el art. 45 RGPD "podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado". Hasta la fecha los países y territorios declarados como adecuados son[151]: Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Estados Unidos[152] y Japón. "Las nuevas decisiones sobre el carácter «adecuado» de la protección tendrán que revisarse al menos cada cuatro años. Las autorizaciones y decisiones existentes sobre esa «adecuación» seguirán en vigor hasta que se modifiquen, sustituyan o deroguen. En definitiva, el Reglamento introduce un mecanismo vinculante de actualización periódica para evitar que la evolución tecnológica haga inútiles las garantías legales y deje a los ciudadanos desprotegidos de facto en sus derechos"[153].

En segundo lugar, el RGPD introduce como novedad las transferencias a terceros Estados que ofrezcan suficientes garantías y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas"[154]. Asegurar las suficientes garantías en una transferencia internacional, no se limita a ofrecer garantías adecuadas únicamente

[150] Art. 4.23 del RGPD.

[151] Transferencias internacionales (fecha de consulta: 06-05-2019). https://www.aepd.es.

[152] Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU.

[153] DÍAZ DÍAZ, E.: "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones", *Revista Aranzadi Doctrinal*, núm. 6, 2016, p. 10.

[154] Art. 46.1 del RGPD.

a la transferencia realizada desde cualquier territorio del EEE a un tercer país u organización internacional, sino también sobre las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. "Por lo tanto, si un responsable pretende transferir datos personales a un tercer Estado, región u organización internacional no solo debe afirmar que es "segura", también debe acreditar que cumple con todos los elementos obligatorios y que, en caso de efectuar sucesivas transferencias internacionales de datos a otros proveedores, también estos adoptan las garantías tecnológicas suficientes"[155].

Dentro de este supuesto, se encuentran las normas corporativas vinculantes o *Binding Corporate Rules* ("BCRs" en sus siglas en inglés). Se regulan en el artículo 47 del RGPD, y son "las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta"[156]

"Las BCRs son originariamente un conjunto de normas para flexibilizar las transferencias internacionales de datos a nivel de grupo desde las sociedades del grupo ubicadas en la Unión Europea hacia las sociedades del grupo ubicadas en países que no ofrezcan un nivel de protección de datos adecuado. El RGPD aboga por un marco único para responsables y encargados del tratamiento y hace referencia a la utilización de este instrumento no sólo en el seno de un grupo sino también en uniones de empresas que lleven a cabo una actividad económica conjunta"[157]. El Grupo de Trabajo del artículo 29 dedica a las normas corporativas vinculantes un documento en el que se describe su procedimiento y su finalidad como mecanismo para que el encargado del tratamiento proporcione las garantías adecuadas al responsable a fin de cumplir con la ley aplicable[158].

[155] GONZALO DOMENECH, J.J.: "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados miembros", *Cuadernos de Derecho Transnacional*, núm. 1, 2019, pp. 354-355.

[156] Art. 4. 20) del RGPD.

[157] RODRÍGUEZ BALLANO, S.: "Habemus nuevo Reglamento General de Protección de Datos". *Actualidad Jurídica Aranzadi*, núm.919, 2016, p. 2.

[158] Documento del Grupo de trabajo del artículo 29 explicativo del procedimiento de las normas corporativas vinculantes adoptado el 19 de abril de 2013 y revisado el 22 de mayo de 2015 (WP 204 rev.01). (fecha de consulta: 25-06-2019). https://ec.europa.eu/.

Finalmente, a falta de decisión de adecuación y de garantías adecuadas, únicamente se podrán realizar si se cumplen alguna de las condiciones enumeradas en el art. 49. del RGPD[159]. Entre las cuales destacan los casos en los que el interesado haya dado explícitamente su consentimiento, transferencias necesarias para la ejecución de un contrato o para la ejecución de medidas precontractuales. Transferencias basadas en un interés público o aquellas necesarias para proteger los intereses vitales del interesado o de otras personas. También se incluyen aquí las transferencias realizadas desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo.

3. Especial régimen de transferencias con los EE.UU

3.1. Evolución

La importancia de las transferencias internacionales de datos con los EE.UU siempre ha tenido un papel relevante, tanto con el antiguo régimen de la Directiva 95/46/CE, como con el actual RGPD. La importancia de las relaciones comerciales entre los EU y la UE, la gran cantidad de datos que se transfieren y la ubicación de importantes empresas tecnológicas ubicadas en EE.UU pero ofrecen sus bienes o servicios a personas ubicadas en la UE. Unido a la falta de legislación sobre protección de datos en EE.UU y el carácter extraterritorial de la legislación europea, han llevado a articular mecanismos que permitan las transferencias conforme la normativa europea de protección de datos.

En este sentido, la Comisión Europea, fruto de una negociación con el Departamento de Comercio de los Estados Unidos de América, aprobó la Decisión de la Comisión, de 26 de julio de 2000[160], mediante la cual se estableció un sistema de autocertificación, por el cual las empresas estadounidenses se comprometían a gestionar los datos personales que fueran transferidos a EE.UU bajo el amparo de los principios de Puerto Seguro (*Safe Harbor*)[161]. Una vez que las empresas autocertificaban su adhesión

[159] Transferencias internacionales (fecha de consulta: 06-05-2019). https://www.aepd.es.

[160] Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América [notificada con el número C (2000) 2441]. *DO L, núm. 215, 25-VIII-2000.*

[161] El *Safe Harbor Agreement* estaba formado por un conjunto de siete principios que garantizan un nivel adecuado de protección de los datos personales transferidos desde la UE a empresas establecidas en Estados

a estos principios se presumía que cumplían con el nivel de protección adecuado exigido por la Directiva[162].

Sin embargo, el TJUE en la ya mencionada sentencia *Schrems* declaró la invalidez de la Decisión por una serie de fundamentos jurídicos. Uno de los elementos centrales que sirvió al TJUE para anular el acuerdo de Puerto Seguro, era que la Decisión 2000/520 no contenía ninguna constatación sobre la existencia en EE.UU de reglas estatales destinadas las limitas las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la UE a EE.UU, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional[163].

3.2. Escudo de Privacidad o *EU-U.S, Privacy Shield*

Ante la inseguridad jurídica que había provocado la declaración de invalidez de la Decisión 2000/520 que hasta le fecha hacia viables las transferencias internacionales de datos a los EE.UU, la Comisión Europea y el Departamento de Comercio de los Estados Unidos de América reanudaron las negociaciones a fin de alcanzar un nuevo acuerdo que permitiera las transferencias internacionales entre ambos territorios, que termino con la aprobación de la conocida como *EU-U. S. Privacy Shield framework* (escuso de privacidad)*[164]*. Al igual que el anterior acuerdo, el marco normativo sobre el escudo de privacidad parte también de un mecanismo de autocertificación que debe de notificarse ante el Departamento de Comercio de los Estados Unidos, mediante la adhesión al cumplimiento de una serie de principios (siete principios generales y dieciséis con carácter complementario) [165].

Unidos. ÁLVAREZ CARO, M. y RECIO GAYO, M. "Hacia un acuerdo Safe Harbor renovado para la transferencia internacional de datos entre EE.UU y la UE". *Papeles de Derecho Europeo e Integración Regional*, núm. 25, 2015, Madrid, pp. 6-7.

[162] URÍA GAVILÁN, E.: "Derechos fundamentales *versus* vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 *Schrems*". *Revista de Derecho Comunitario Europeo*, núm. 53, 2016, p. 265.

[163] VILLARINO MARZO, J.: *La privacidad en el entorno del cloud computing*, Reus, Madrid, 2018, pp. 202-215.

[164] Decisión de ejecución (UE), núm. 2016/1250, de la Comisión, de fecha 12 de julio de 2016, con arreglo a la Directiva 95/46/ CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. *DOUE* L, núm. 207, 12-VII-2016.

[165] 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, Barcelona, pp. 27-28.

El nuevo marco normativo ha supuesto una mejora, en detrimento de lo que se venía efectuando hasta el momento, pero carece aún de aquellos elementos indispensables que equiparen su protección a la que realiza la legislación comunitaria, teniendo en cuenta que son ordenamientos jurídicos antagónicamente diferentes. Es por ello por lo que, a grandes rasgos, se puede afirmar su positividad, debido a que ha puesto fin a la situación de inseguridad jurídica que se venía sucediendo hasta su entrada en vigor y que perjudicaba tanto a las organizaciones como a los propios particulares, pero recordando, en todo momento, que se ha seguido el mismo modelo que el adoptado para el anterior Acuerdo, introduciendo, como otra de las novedades importantes, la figura del Defensor del Pueblo como otro de los recursos a disposición de los ciudadanos europeos afectados por la recogida de sus datos personales, a pesar de que existen dudas de que este órgano goce de la suficiente independencia y posea las competencias necesarias para desarrollar sus funciones de manera eficiente[166].

4. Circulación de datos no personales en la UE

La UE consciente de la digitalización de la economía y el auge de tecnologías emergentes (como el 5G, Internet de las cosas, Blockchain, etc.) está orientando sus esfuerzos legislativos para crear un marco jurídico común que permita aumentar y dar seguridad jurídica al intercambio transfronterizo de datos e impulsar la "economía de los datos"[167]. En este nuevo escenario, el RGPD ya constituye una manifestación del legislador europeo de crear un régimen común (Mercado Único Digital) que facilite el libre intercambio de datos entre los países de la UE, aplicable desde el 25 de mayo de 2018. Ahora, un año después, la UE ha aprobado el Reglamento 2018/1807[168] relativo a un marco para la libre circulación de datos no personales en la Unión Europea., aplicable desde el 29 de mayo de 2019. A través de estos dos Reglamentos se pretende crear un

[166] *Ibídem*.

[167] Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. "Building a European Data Economy". European Commission, COM (2017) 9 final, (fecha: 10-01-2017), (en línea). Consultado en: https://eur-lex.europa.eu/.

[168] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea. (*DOUE* L, 303/1, 28-XI-2018).

marco integral para un espacio de datos europeo común y la libre circulación de todos los datos de la UE[169].

Conforme el objetivo del Reglamento 2018/1807, que busca "garantizar la libre circulación en la Unión de datos que no tengan carácter personal mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales"[170]. Se puede decir que presenta tres características principales[171]:

1) Se prohíbe a los Estados miembros imponer requisitos sobre dónde deben localizarse los datos. Las excepciones a esta regla solo pueden justificarse por razones de seguridad pública.
2) Establece un mecanismo de cooperación para garantizar que las autoridades competentes puedan seguir ejerciendo los derechos que tienen para acceder a los datos que se están tratando en otro Estado miembro.
3) Proporciona incentivos para que el sector, con el apoyo de la Comisión, elabore "Códigos de conducta autorreguladores sobre el cambio de proveedores de servicios y la transferencia de datos"[172].

Con respecto a la interacción entre este Reglamento y el RGPD pueden surgir algunas dudas acerca de la aplicación de cada uno de ellos. En este sentido, es conveniente definir el ámbito de aplicación material del Reglamento 2018/1807. En su art. 2.1 se dice que "se aplica al tratamiento en la Unión de datos electrónicos que no tengan carácter personal[173]". En este concepto se englobarían:

- Aquellos que originariamente no se relacionaban con una persona física identificada o identificable (como los datos sobre las condiciones climáticas generados por los sensores instalados en aerogeneradores o los datos sobre las necesidades de mantenimiento de las máquinas industriales).

[169] El RGPD se aplica el EEE, que incluye Islandia, Liechtenstein y Noruega. Además, el Reglamento de libre circulación de datos no personales se considera pertinente a efectos del EEE.

[170] Art. 1 del Reglamento 2018/1807.

[171] Comunicación de la Comisión al Parlamento Europeo y al Consejo. Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea. COM (2019) 250 final, (fecha: 29-05-2019), (en línea). Consultado en: https://eur-lex.europa.eu/.

[172] Art. 6.1 del Reglamento 2018/1807.

[173] De acuerdo con la definición del RGPD. Art. 4.1: "datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente".

- Aquellos que inicialmente eran personales, pero que posteriormente se convirtieron en anónimos.

Para solventar estas dudas, la Comisión ha publicado una guía titulada "Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea" que pretende ayudar a los usuarios, especialmente a las pequeñas y medianas empresas, a comprender la interacción entre el Reglamento de libre circulación de datos no personales y el Reglamento general de protección de datos[174].

También se regulan aquellos supuestos, que suelen ser la mayoría, de aquellas actividades que implican un tratamiento de datos personales y no personales, que se conoce como "conjunto de datos mixtos".

Con respecto a los conjuntos de datos mixtos, el Reglamento de libre circulación de datos personales[175] establece que:

"En el caso de los conjuntos de datos compuestos por datos personales y no personales, el presente Reglamento debe aplicarse a los datos no personales de dichos conjuntos. Cuando los datos no personales y personales estén inextricablemente ligados, el presente Reglamento debe aplicarse sin perjuicio del Reglamento (UE) 2016/679".

Por lo tanto, cada Reglamento se aplicará para aquellos datos que se engloben dentro del ámbito material de aplicación de cada uno de ellos, y en los casos en los que parte de datos no personales y las partes de datos personales están "inextricablemente ligados", los derechos y obligaciones de protección de datos derivados del RGPD se aplicarán completamente a todo el conjunto de datos mixtos.

[174] Considerando 37 del Reglamento (UE) 2018/1807.

[175] Art. 2.2 del Reglamento 2018/1807.

CONCLUSIONES

PRIMERA. *El carácter de "norma universal" del RGPD*. El nuevo supuesto de aplicación territorial del RGPD, que contempla la aplicación de la norma en aquellos casos en los que se traten datos personales de interesados en la UE, cuando el responsable o encargado no está establecido en la Unión, pero las actividades de tratamiento tienen por objeto la oferta de bienes o servicios, u observen el comportamiento de los interesados, define su carácter de "norma universal" por cuanto su aplicación traspasa las fronteras de la UE. Este supuesto incluido en su art. 3 RGPD, supone la materialización en una norma de supuestos que ya habían sido reconocidos por la jurisprudencia del TJUE. Ello constituye una evolución loable en cuanto a su ámbito espacial de aplicación, pues no se precisa de un establecimiento físico en la UE para su puesta en práctica. Este carácter universal, encuentra su razón de ser, en el hecho de la inexistencia o no reconocimiento de este derecho en otros ordenamientos jurídicos de hondo calado tales como EEUU, Rusia, China... Con esta norma, el poder legislativo europeo demuestra su fuerza europeísta al erigirse con estándares referenciales convirtiéndose no sólo en el principal activo intangible para las empresas, sino que además, su defensa y salvaguarda conforma la esfera más íntima y personal de los seres humanos.

SEGUNDA. *Tardía aprobación en España de la LOPDGDD*. El RGPD entró en vigor el 25 de mayo de 2016. No obstante, debido a la profunda modificación que supuso con respecto a la normativa hasta ese momento en vigor, Directiva 95/46/CE, se concedió un plazo de dos años para que fuese directamente aplicable para todos los Estados miembros, es decir, a partir del 25 de mayo de 2018. A pesar de que por su propia naturaleza jurídica de Reglamento, resulta directamente aplicable, sin necesidad de una norma de transposición interna en las diferentes legislaciones nacionales. El RGPD remite en numerosas ocasiones a la normativa nacional que lo complementa para precisar determinados aspectos, que se dejan a discreción de los Estados. En el caso de España, esta ley nacional de la que habla el RGPD, es la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales, que entró en vigor el 6 de diciembre de 2018, tras meses de borradores y dilación, debido en gran medida a una situación de inestabilidad política, que ha tenido como consecuencia una situación de inseguridad jurídica durante los primeros meses de aplicación del Reglamento, que ciertamente podría haberse evitado como ha ocurrido en otros países de nuestro entorno.

TERCERA. *Disparidad de foros de competencia en materia de CJI*. El RGPD reconoce expresamente el derecho a una indemnización a través del ejercicio de acciones judiciales en vía civil. El reconocimiento a la tutela judicial efectiva va acompañado del reconocimiento de reglas especiales de competencia judicial internacional para acciones contra el responsable o encargado del tratamiento, que prevalen, de acuerdo con el principio de especialidad normativa, con los foros contemplados en el Reglamento Bruselas I Bis. El RGPD contempla dos foros alternativos, uno ante los Tribunales del Estado miembro donde el responsable o encargado tenga un establecimiento, o bien, ante los Tribunales del Estado miembro donde el demandante tenga su domicilio. Los foros reconocidos en el RGPD, son complementarios a los recogidos en el Reglamento Bruselas I Bis, lo que puede llegar a ocasionar un problema de inseguridad jurídica y falta de protección para la persona que ha sufrido el daño. Esta diversidad de foros, generales y especiales, se rigen por criterios de interpretación diferentes. En el caso de los especiales, es preciso un vínculo de conexión entre el foro y la cuestión jurídica objeto del caso, mientras que en los foros generales, prevalece la naturaleza protectora en favor de los interesados, con interpretaciones propias de esta regulación, como el concepto amplio de "establecimiento". Por ello, sería conveniente una modificación del RGPD que venga a aclarar la relación entre las dos normas, o como solución alternativa, que las normas relativas a Competencia Judicial Internacional en materia de protección de datos estuviesen contenidas únicamente en el Reglamento Bruselas I Bis, como norma única de referencia.

CUARTA. *Modificación del Reglamento Roma II para la inclusión en su ámbito de aplicación de cuestiones relativas al derecho de la personalidad*. En cuanto a la determinación de la ley aplicable, a pesar del carácter de norma imperativa del RGPD en materia de protección de datos personales, no hay ninguna mención expresa en el RGPD sobre determinación de la ley aplicable. Ello conlleva, en cuestiones tales como las reclamaciones por responsabilidad civil, en el marco de un litigio para la reclamación de una indemnización al responsable o encargado del tratamiento, acudir a la legislación nacional para encontrar una solución, en el caso de España, al art. 10.9 CC. Esta situación pone en evidencia la existencia de un vacío legal a nivel comunitario, puesto que la norma de referencia, el Reglamento Roma II, excluye expresamente de su ámbito de aplicación las cuestiones relativas a derechos de la personalidad como sería la protección de datos personales. Si bien ya hay una propuesta de reforma del Reglamento Roma II, con la

inclusión de un nuevo art. 5 bis, que incluye dentro de su ámbito de aplicación cuestiones relativas a protección de datos personales, los supuestos contemplados en esa reforma se antojan poco protectores para la parte demandante, por lo que sería deseable una *lege ferenda* que incluya un nuevo supuesto que permita aplicar la ley de un tercer país que presente vínculos más estrechos con el caso, que su interpretación permita que sea de aplicación la ley más protectora, equilibrada y favorable para la parte que sufre el daño, evitando que sea de aplicación la ley del país del lugar de residencia del demandado.

QUINTA. *Mecanismos efectivos de control para las transferencias internacionales de datos*. Las transferencias internacionales de datos, encuentran su cobertura legal en un sistema de "garantías adecuadas" previsto por el RGPD que se ha demostrado en algunos casos insuficiente. En este sentido, la STJUE del caso *Schrems* debería de servir como punto de inflexión en cuanto a los intercambios de datos entre la UE y los EE.UU, en la que TJUE declaró inválida la Decisión 2000/520/CE, de la Comisión Europea, de 26 de julio del año 2000 que permitía el intercambio de datos a aquellas empresas adheridas al sistema de Puerto Seguro o *Safe Harbour* por la falta de garantías adecuadas para asegurar que el intercambio cumplía con los parámetros de la entonces Directiva 95/46/CE, a raíz de que trascendieran públicamente noticias sobre programas del Gobierno de los EE.UU de control y vigilancia de las comunicaciones tanto a nivel nacional como internacional (caso Snowden). A pesar de que, a raíz de esta sentencia se creó un nuevo sistema de intercambio de datos conocido como Escudo de Privacidad UE-EE.UU ó *Privacy Shield*, que incluye mejoras para garantizar que los intercambios se realizan con arreglo a los dispuesto en el RGPD, falta todavía un órgano con competencias suficiente para conocer, denunciar y si procede sancionar, en caso de que no se estén llevando esos intercambios con las debidas garantías. Los estrictos mecanismos y medidas de protección establecidas en el RGPD para las transferencias transfronterizas dentro de la UE, no deberían de perder tal condición en los casos de transferencias internacionales de datos a través del sistema de "garantías adecuadas". Para ello, resultaría conveniente reforzar y garantizar las competencias otorgadas a las autoridades nacionales de control, como órganos encargados de tratar las reclamaciones de los interesados, poner en conocimiento de los tribunales si procede, y suspender de manera efectiva las transferencias internacionales a otros países cuando consideren que no cumplen con un nivel adecuado de protección.

De esta manera, se pretende asegurar que los intereses comerciales o políticos no interfieran en los mecanismos legales creados para asegurar los intercambios de datos a nivel internacional.

BIBLIOGRAFÍA

ABERASTURI GORRIÑO, U.: "Movimiento internacional de datos. Especial referencia a la transferencia internacional de datos sanitarios", *Revista de administración pública*, núm. 186, 2011, pp. 329-369.

ÁLVAREZ CARO, M. / RECIO GAYO, M.: "Hacia un acuerdo Safe Harbor renovado para la transferencia internacional de datos entre EE.UU y la UE", *Papeles de Derecho Europeo e Integración Regional*, núm. 25, 2015, pp. 1-28.

ÁLVAREZ RIGAUDIAS, C.: "Condiciones para las transferencias internacionales de datos personales en servicios de *cloud*", MARTÍNEZ MARTÍNEZ, R. (Ed.), *Derecho y Cloud Computing*, Aranzadi, Navarra, 2012.

CAAMIÑA DOMÍNGUEZ, C.M.: "La noción de "consumidor" en internet: El asunto C-498/16, Maximilian Schrems y facebook Ireland Limited", *Cuadernos de derecho transnacional*, núm. 1, 2019, pp. 711-721.

CALVO CARAVACA, A-L. / CARRASCOSA GONZÁLEZ, J.: *Derecho internacional privado*, Comares, Granada, 2016.

CARRASCOSA GONZÁLEZ, J.: "La protección de los datos personales en un escenario tecnológico supranacional Cloud Computing, tribunales competentes y ley aplicable", VALERO TORRIJOS, J. (aut.), *La protección de datos personales en internet ante la innovación tecnológica riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Navarra, 2013, pp. 113-128.

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. 5-35.

CORDERO ÁLVAREZ, C. I.: "Asuntos Acumulados *eDate Advertising* y *Martinez Martinez* (Sentencia del TJUE de 25 de octubre)", *Foro, nueva época*, núm 14, 2011, pp. 267-268.

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.

--: “Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia”, *La Ley Unión Europea*, núm. 31, 2015, pp. 1-10.

--: *Derecho privado de Internet*, Civitas, Madrid, 2015.

--: “La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google”, *Diario La Ley*, núm. 8773, 2016, pp. 1-6.

--: “Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea”, *Revista Española de Derecho (REDI)*, núm. 1, 2017, pp. 75-108.

--: “Demandas frente a redes sociales por daños en materia de datos personales: precisiones sobre competencia judicial”, *La Ley Unión Europea*, núm. 56, 2018, pp. 1-11.

DÍAZ DÍAZ, E.: “El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones”, *Revista Aranzadi Doctrinal*, núm. 6, 2016, pp. 1-23.

DÍAZ MARTÍN, C.: “El Reglamento General de Protección de Datos, su implementación y la transición para el responsable público”. *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 47, 2018, pp. 1-14.

DOPAZO FRAGUÍO, P.: “La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente. (Novedades del Reglamento General de Protección de Datos)”. *Revista Española de Derecho Europeo*, núm. 68, 2018, pp. 113-148.

ERDOZÁIN LÓPEZ, J. C.: “La protección de los datos de carácter personal en las telecomunicaciones”, *Revista Doctrinal Aranzadi*, núm. 1, 2007, pp. 1845-1889.

FONT I SEGURA, A.; OTERO GARCÍA-CASTRILLÓN, C.: “Crónica de actualidad de Derecho Internacional Privado (Julio - Diciembre 2016)”, *Revista electrónica de estudios internacionales (REEI)*, núm. 33, 2017, pp. 1-56.

FORNER DELAYGUA, J.J.: "Sentencia de 25 de octubre de 2011, Asuntos acumulados C-509/09 y C-161/10, eDate Advertising GmbH c. X y Olivier Martínez y Robert Martínez c. MGN Limited", *Revista Jurídica de Catalunya*, núm. 2, 2012, pp. 549-556.

GEIST, M.: "Is There a There There? Toward Greater Certainty for Internet Jurisdiction", *Berkeley Technology Law Journal*, núm. 3, 2001, pp. 1345-1406.

GONZALO DOMÉNECH, J.J.*:* "Algunas cuestiones relevantes de derecho internacional privado del Reglamento General de Protección de Datos"*, Revista Boliviana de Derecho*, núm. 26, 2018, pp. 404-437.

--: "Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros", *Cuadernos de Derecho Transnacional*, núm. 1, 2019, pp. 354-355.

--: "El régimen de corresponsabilidad en el tratamiento en una red social y el régimen de competencia de una autoridad de control: comentario a la STJUE de 5 de junio de 2018", *Diario La Ley*, núm. 9258, 2018, pp. 1-18.

GUTIÉRREZ COLOMINAS, D.: "Schrems v Facebook: the consumer definition in the framework of digital social networks", *European Data Protection Law Review*, núm. 4, 2018, pp. 542-546.

JERKER SVANTESSON, D.: "The CJEU's Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, Yet So Very Important", *Maastricht Journal of European and Comparative Law*, núm. 1, 2016, pp. 332-34.

KUNER, C.: "The European Union and the Search for an International Data Protection Framework", *Groningen Journal of International Law*, núm. 1, 2015, pp. 55-71.

LEIN, E.: "Competencia judicial internacional - Sentencia del Tribunal de Justicia de la Unión Europea, de 25 de octubre de 2011, asuntos acumulados C-509/09 y C-161/10, eDate Advertising GmbH c. X y Olivier Martínez y Robert Martínez c. MGN Limited", *Revista española de Derecho Internacional*, núm. 1, 2012, pp. 193-198.

LÓPEZ ÁLVAREZ, L. F.: Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo, Francis Lefebvre, Madrid, 2016.

MORENO GARCÍA, L.: "Delimitación del «fuero del consumidor» en asuntos relacionados con redes sociales y protección de datos", *Diario La Ley*, núm. 9270, 2018, pp. 1-17.

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.

ORDÓÑEZ SOLÍS, D.: "El derecho al olvido en Internet y la sentencia Google Spain", *Revista Aranzadi Unión Europea*, núm. 6, 2014, pp.27-50.

OREJUDO PRIETO DE LOS MOZOS, P.: "La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia", *La Ley Unión Europea*, núm. 4, 2013, pp.18-27.

ORTEGA GIMÉNEZ, A.: "Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE "*Lindqvist*", de 6 de noviembre de 2013", *Revista de derecho de Extremadura*, núm. 7, 2010, pp. 101-105.

--: "Imagen y circulación internacional de datos", *Revista Boliviana de Derecho*, núm. 15, 2013, pp. 130-147.

--: *Transferencias Internacionales de Datos de Carácter Personal Ilícitas*, Aranzadi, Navarra, 2017.

--: *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal*, Aranzadi, Navarra, 2017.

PADOVA, Y., «What the European Draft Regulation on Personal Data is going to change for companies», *International Data Privacy Law*, núm. 4, 2014, pp. 39-52.

PIÑAR MAÑAS, J.L.: "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", *Cuadernos de Derecho Público*, núm. 19-20, 2013, pp. 45-90.

--: "Transferencias de datos personales a terceros países u organizaciones internacionales", PIÑAR MAÑAS J.L. (Dir.) / ÁLVAREZ CARO, M.; RECIO GAYO, M. (Coords.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Barcelona, 2016, pp. 427-460.

RECIO GAYO, M.: "Acerca de la evolución de la figura del encargado del tratamiento", *Revista de Privacidad y Derecho Digital*, núm. 0, 2015, pp. 30-37.

--: "Los derechos a presentar reclamaciones ante la autoridad de control y a la tutela judicial efectiva", PIÑAR MAÑAS J.L. (Dir.) / ÁLVAREZ CARO, M.; RECIO GAYO, M. (Coords.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Barcelona, 2016, pp. 543-557.

RODRÍGUEZ BALLANO, S. / VIDAL. M.: "Habemus nuevo Reglamento General de Protección de Datos". *Actualidad Jurídica Aranzadi*, núm. 919, 2016, pp. 1-9.

SANCHO VILLA, D.: *Negocios internacionales de tratamiento de datos personales*, Civitas, Navarra, 2010.

SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012.

TAYLOR, M.: "Permissions and prohibitions in data protection jurisdiction", *Brussels Privacy Hub working paper*, núm. 6, 2016, pp. 1-25.

TRANCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Madrid, 2010.

URÍA GAVILÁN, E.: "Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 *Schrems*". *Revista de Derecho Comunitario Europeo*, núm. 53, 2016, pp. 261-282.

URIARTE LANDA, I.: "Ámbito de aplicación material", PIÑAR MAÑAS J.L. (Dir.) / ÁLVAREZ CARO, M.; RECIO GAYO, M. (Coords.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, Barcelona, 2016, pp. 63-76.

VILLARINO MARZO, J.: *La privacidad en el entorno del cloud computing*, Editorial Reus, 2018, Madrid.

ZANFIR FORTUNA, G.: "A Missed Opportunity: The Amazon Case That Almost Made Data Subjects Into Consumers", *European Data Protection Law Review*, núm. 2, 2016, pp. 585-589.

ANEXO LEGISLATIVO

I. LEGISLACIÓN EUROPEA

TEXTO	REFERENCIA
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 respeta al tratamiento de datos personales y a la libre circulación de estos datos.	*DOCE* L 281, 23-XI-1995.
Reglamento (CE) nº 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.	*DOUE* L 12/1, 16-I-2001.
Reglamento (CE) n° 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).	*DOUE* L 199/40, 31-VII-2007.
Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales (Roma I).	*DOUE* L 177/6, 4-VII-2008.
Carta de los Derechos Fundamentales de la Unión Europea.	*DOUE* C 83, 30-III-2010.
Tratado de Funcionamiento de la Unión Europea	*DOUE* C 326, 26-X-2012.
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.	*DOUE* L 351/1, 20-XII-2012.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.	*DOUE* L 119/1, 4-V-2016.
Decisión de ejecución (UE), núm. 2016/1250, de la Comisión, de fecha 12 de julio de 2016, con arreglo a la Directiva 95/46/ CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.	*DOUE* L 207, 1-VII-2016.
Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.	*DOUE* L 303, 28-XI-2018.

II. DOCUMENTOS DE TRABAJO UE

TEXTO
COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Estrategia para el Mercado Único Digital de Europa. COM (2015) 192 final.
COMISIÓN ERUOPEA. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. "Building a European Data Economy". European Commission, COM (2017) 9 final
COMISIÓN EUROPEA. Comunicación de la Comisión al Parlamento Europeo y al Consejo. Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea. COM (2019) 250 final.
GTDP. Documento explicativo del procedimiento de las normas corporativas vinculantes adoptado el 19 de abril de 2013 y revisado el 22 de mayo de 2015 (WP 204 rev.01).
GTDP. Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento, adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017 (WP 244 rev.01).

III. LEGISLACIÓN NACIONAL

TEXTO	REFERENCIA
Código Civil.	*BOE* núm. 206, 25-7-1889.
Ley 9/1968, de 5 de abril, sobre Secretos Oficiales	*BOE* núm. 84, 06-IV-1968.
Constitución Española.	*BOE* núm. 311, 29-XII-1978.
Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.	*BOE* núm. 157, 02-VII-1985.
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.	*BOE núm.* 298, 14-XII-1999.
Ley 36/2015, de 28 de septiembre, de Seguridad Nacional	*BOE* núm. 233, 29-09-2015.
Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.	*BOE* núm. 294, 06-XII-2018.

ANEXO JURISPRUDENCIAL

I. JURISPRUDENCIA EUROPEA DEL TJUE

TRIBUNAL	**ASUNTO**	**PARTES**	**ECLI**
STJUE, 6 noviembre 2003	C-101-01	*Lindqvist*	EU:C:2003:596
STJUE 7 diciembre 2010	C-585/08 y C-144/09	*Pammer y Hotel Alpenhof*	EU:C:2010:740
STJUE 22 diciembre 2010	C-497/10	*Mercredi*	EU:C:2010:829
STJUE 20 de mayo 2010	C-111/09	*Česká podnikatelská v. Michal Bilas*	EU:C:2010:290
STJUE 25 octubre 2011	C-509/09 y C-161/10	*eDate Advertising GmbH*	EU:C:2011:685
STJUE 3 octubre 2013	C-170/12	*Pinckney*	EU:C:2013:635
STJUE 13 marzo 2014	C-548/12	*Brogsitter*	EU:C:2014:148
STJUE 13 mayo 2014	C-131/12	*Google Spain S.L contra Agencia Española de Protección de Datos*	EU:C:2014:317
STJUE 22 enero 2015	C-441/13	*Hejduk*	EU:C:2015:28
STJUE 1 octubre 2015	C-230/14	*Weltimmo*	EU:C:2015:639
STJUE 6 octubre 2015	C-362/14	*Schrems I*	EU:C:2015:650
STJUE 28 enero 2015	C-375/13	*Kolassa*	EU:C:2015:37
STJUE 14 julio 2016	C-196/15	*Granarolo*	EU:C:2016:559
STJUE 28 julio 2016	C-191/15	*Verein für Konsumenteninformation vs Amazon EU Sàrl*	EU:C:2016:612
STJUE 25 enero 2018	C-498/16	*Schrems II*	EU:C:2018:37

II. JURISPRUDENCIA NACIONAL

TRIBUNAL	**ECLI**
STC de 20 de noviembre de 2000	ES:TC:2000:292
STS de 15 de octubre de 2015	ES:TS:2015:4162
STS de 11 de marzo de 2016	ES:TS:2016:1057
STS de 14 de marzo de 2016	ES:TS:2016:1056
STS de 15 de marzo de 2016	ES:TS:2016:1103
STS de 5 de abril de 2016	ES:TS:2016:1280
STS de 26 de abril de 2017	ES:TS:2017:1645

PÁGINAS WEBS VISITADAS

NOMBRE	ENLACE
Agencia Española de Protección de Datos	https://www.aepd.es/
Comisión Europea	https://ec.europa.eu/
Tribunal de Justicia de la Unión Europea	https://curia.europa.eu/
Agencia Estatal Boletín Oficial del Estado	https://www.boe.es/
Pedro de Miguel Asensio	http://pedrodemiguelasensio.blogspot.com/
Centro de Documentación Judicial (CENDOJ)	http://www.poderjudicial.es/