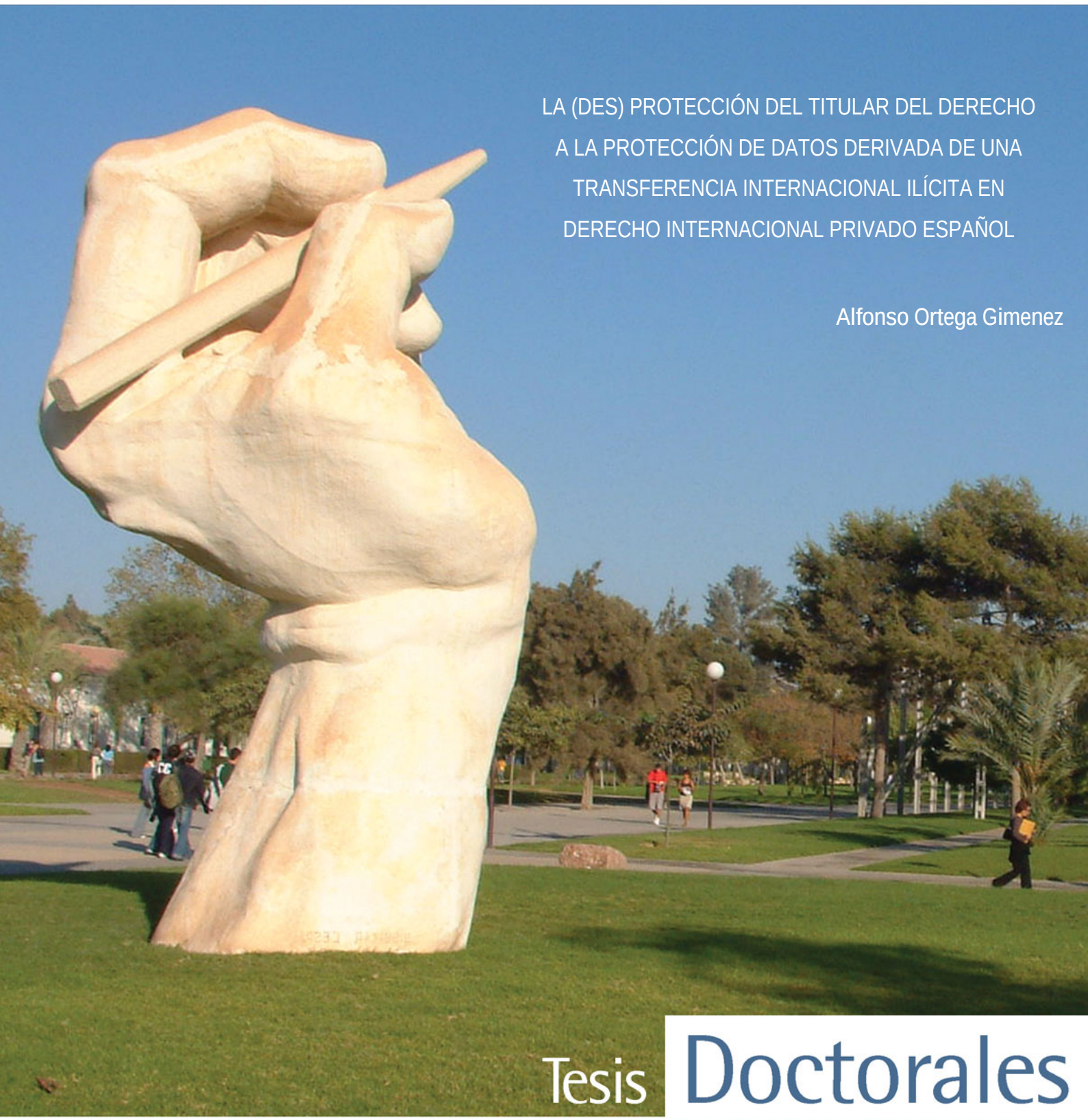
Universitat d'Alacant
Universidad de Alicante

LA (DES) PROTECCIÓN DEL TITULAR DEL DERECHO A LA PROTECCIÓN DE DATOS DERIVADA DE UNA TRANSFERENCIA INTERNACIONAL ILÍCITA EN DERECHO INTERNACIONAL PRIVADO ESPAÑOL

Alfonso Ortega Gimenez



Tesis Doctorales

www.eltallerdigital.com

UNIVERSIDAD de ALICANTE

Universidad de Alicante
Facultad de Derecho

LA (DES) PROTECCIÓN DEL TITULAR DEL DERECHO A LA PROTECCIÓN DE DATOS DERIVADA DE UNA TRANSFERENCIA INTERNACIONAL ILÍCITA EN DERECHO INTERNACIONAL PRIVADO ESPAÑOL

Alicante, 5 de septiembre de 2014

TESIS DOCTORAL

Presentada por:
Alfonso ORTEGA GIMÉNEZ

Dirigida por:
Dr. D. Manuel DESANTES REAL y
Dr. D. Manuel E. MORÁN GARCÍA

Índice

Abreviaturas más utilizadas

ADR	*Alternative Dispute Resolution*
AEPD	Agencia Española de Protección de Datos
AELC	Asociación Europea de Libre Comercio
APEC	Foro de Cooperación Económica Asia-Pacífico
BCR	*Binding Corporate Rules*
BOE	Boletín Oficial del Estado
CB	Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Bruselas, el 27 de septiembre de 1968
CC	Código Civil
CCI	Cámara de Comercio Internacional
CE	Constitución Española de 1978
CEDH	Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950
CL II	Convenio de «Lugano II» de 30 de octubre de 2007 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil
DOCE/DOUE	Diario Oficial de las Comunidades Europeas / desde 1 de febrero 2003, Diario Oficial de la Unión Europea
EEE	Espacio Económico Europeo

ISO	Organización Internacional para la Normalización
LEC	Ley de Enjuiciamiento Civil
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos
LSSI	Ley de Servicios de la Sociedad de la Información
OCDE	Organización para la Cooperación y el Desarrollo económico
ODR	*On line Dispute Resolution*
OIT	Organización Internacional del Trabajo
OMC	Organización Mundial del Comercio
ONU	Organización de Naciones Unidas
RB	Reglamento (CE) núm. 44/2001, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Reglamento «Bruselas I»)
RJ	Repertorio Aranzadi de Jurisprudencia
RLOPD	Reglamento de desarrollo de la Ley Orgánica de Protección de datos de carácter personal
RMS	Reglamento de Medidas de seguridad
SAN	Sentencia de la Audiencia Nacional
STC	Sentencia del Tribunal Constitucional español
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STS	Sentencia del Tribunal Supremo español
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TUE/TFUE	Tratado de la Unión Europea / Tratado de Funcionamiento de la Unión Europea
UE	Unión Europea
UNCITRAL	Comisión de las Naciones Unidas para la unificación del derecho mercantil internacional

Introducción

1. De acuerdo con la tradición académica universitaria, el desarrollo de un Proyecto de Tesis Doctoral suele venir precedido por una introducción que justifique, en primer lugar, las razones que llevan a la selección del objeto de estudio (I); en segundo término, la opción u opciones de tratamiento metodológico que se aplicarán sobre el mismo (II); y, finalmente, la estructura lógica y sistemática con la que se expondrán los resultados del proceso investigador (III). A cumplir con dichas exigencias se dedican las páginas que siguen.

I. JUSTIFICACIÓN DE LA ELECCIÓN DEL OBJETO DE ESTUDIO

2. Esta Tesis Doctoral pretende demostrar que, en la situación actual, el titular del derecho a la protección de datos de carácter personal ante una transferencia internacional ilícita de dicho datos se encuentra en una situación de (des) protección. El objeto de estudio se circunscribe a la responsabilidad extracontractual derivada de una trans-

ferencia internacional de datos de carácter personal ilícita, en la medida en que sus aspectos contractuales están suficientemente estudiados por la doctrina.[1]

Cuatro argumentos justifican la elección del objeto de estudio: *a)* su incardinación en una de las líneas de investigación emprendidas por el área de Derecho Internacional Privado de la Universidad de Alicante; *b)* su importancia como intersección entre dos vectores que explican y definen nuestra realidad: por un lado, el advenimiento de la Sociedad de la Información y el Conocimiento y, por otro, la posible colisión del uso generalizado de las Tecnologías de la Información y la Comunicación con la *vis* expansiva de los Derechos Fundamentales; *c)* desde un punto de vista jurídico general, su regulación encierra no pocas complejidades, dada la variedad de intereses y valores en pre-

[1] *Vid.* de Helena ANCOS FRANCO, «Las Transferencias Internacionales de datos de carácter personal como barrera al comercio internacional. El caso de los EE.UU.», en, Miguel Ángel DAVARA RODRÍGUEZ (Coord.), *III Jornadas sobre Informática y Sociedad 2000*, Universidad Pontificia de Comillas, Madrid, 2001, pp. 23-42; «La progresiva configuración de las transferencias de datos como objeto del tráfico comercial internacional», en *Boletín ICE*, núm. 788, noviembre 2000, pp. 147-160; y «La regulación de las transferencias internacionales de datos de carácter personal como barrera al comercio internacional: de la Directiva 95/6 a los Acuerdos UE-Terceros Estados», en *RDCE*, núm. 6, Julio-Diciembre 1999, pp. 497-516; Rafael GARCÍA DEL POYO y Francisco GARI, «Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales», en *Revista Española de Protección de Datos*, núm. 2, Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, 2007, pp. 239-266; Diana SANCHO VILLA, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010; «Protección de datos personales y transferencia internacional: cuestiones de ley aplicable», en *Revista Jurídica de Castilla y León*, núm. 16, Septiembre 2008, pp. 401-445; y *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003.

sencia: del titular del derecho fundamental a la protección de los datos de carácter personal, de las autoridades estatales, internacionales o supraestatales, o los más difusos, pero no menos relevantes, del Comercio Internacional; y *d)* por la escasez de trabajos específicos en esta materia, desde la más concreta perspectiva del Derecho internacional privado español.

3. El primero de los argumentos que justifican la elección del objeto de estudio tiene que ver con su incardinación en una de las líneas de investigación desarrolladas por el equipo académico del área de Derecho internacional privado de la Universidad de Alicante. Entre otras obras, se pueden reseñar como resultado de dicho emprendimiento los trabajos de la profesora Dra. Dña. Lydia Esteve González, *Aspectos internacionales de las infracciones de derechos de autor en Internet*, del profesor Dr. D. Aurelio López-Tarruella Martínez, *Contratos internacionales de software*, y de la profesora Dra. Dña. Carmen García Mirete, *Las Bases de Datos Electrónicas Internacionales*, dirigidos por el profesor Dr. D. Manuel Desantes Real. Este trabajo pretende ser una progresión lógica de continuidad y avance en este campo, incidiendo en la necesidad de proporcionar una protección jurídica adecuada al polo subjetivo más débil de las relaciones que surgen con el tratamiento ilícito internacional de datos de carácter personal.

4. El segundo argumento para seleccionar como objeto de estudio el problema de la desprotección del titular de datos de carácter personal ante una transferencia internacional está conectado con el particular contexto tecnológico, social, económico e histórico en que tales transferencias se desarrollan. Si en cualquier época el intercambio de datos entre los diferentes países ha sido una realidad, hoy en día, su volumen y su importancia han adquirido un crecimiento rápido y expo-

nencial gracias a dos circunstancias que han cambiado radicalmente la percepción de la sociedad respecto a las transferencias internacionales de datos de carácter personal: por un lado, el perfeccionamiento de las tecnologías de la información y de la comunicación, que favorecen el flujo global y exponencial de información; y, por otro lado, la propia mundialización de las transferencias internacionales de datos de carácter personal.[2]

En primer lugar, los avances tecnológicos —en particular, el desarrollo de Internet— facilitan considerablemente el tratamiento y el

[2] El desarrollo de la normativa sobre protección de datos es una realidad que desde sus inicios tiende a mundializarse. Así, comenzando por Alemania (1977), Francia (1978), Israel (1981), Australia (1988), España y Suiza (1992), Hong Kong (1996), Reino Unido y Suecia (1998), Argentina (2000), Japón (2003), Colombia (2008), México (2010) y hasta más de 50 Estados que, en la actualidad, disponen de su propia legislación en materia de protección de datos. Existen dos enfoques principales a la hora de regular la protección de datos en los distintos Estados: el enfoque *omnibus*, que protege los datos personales de modo general en todas las actividades económicas y la mayoría de entornos —que es el enfoque seguido en Europa— y el enfoque *sectorial* que establece los requisitos para el tratamiento de datos en determinadas actividades económicas y en entornos concretos —que es el enfoque seguido por los Estados Unidos—. A pesar de los particularismos existentes entre todos los Estados, lo cierto es que las distintas legislaciones nacionales comparten un notable grado de estandarización en relación con los principios fundamentales de la protección de datos y difieren algo más con respecto a las obligaciones básicas a cumplir por los responsables de ficheros; por ejemplo, la inscripción de ficheros en el Registro de las correspondientes agencias nacionales de protección de datos es obligatoria en más de 30 Estados (p. ej., Argentina, Mónaco, Túnez, o Vietnam), mientras que en otros Estados (p. ej., Australia, Brasil, Egipto, o Japón) no existe tal obligación o bien se habilita una alternativa a la inscripción de ficheros, como sería el caso de Alemania. La mundialización de la normativa sobre protección de datos está en constante evolución. Como consecuencia de ésta y de las posibles sanciones previstas para casos de infracción de tal normativa, la forma de acometer su cumplimiento normativo está igualmente en evolución.

intercambio de información, permiten compartir recursos tecnológicos, centralizar determinadas actividades y procesos, y abaratar costes en la prestación de servicios por las propias empresas, fuera del país en el que se encuentran establecidas. Estos avances permiten que los datos de naturaleza personal, siempre útiles e interesantes para el desarrollo de cualquier actividad a gran escala, puedan hoy circular internacionalmente de manera rápida y ser almacenados indefinidamente.

En segundo término, las transferencias internacionales de datos personales, en áreas tales como los recursos humanos, los servicios financieros, la educación, el comercio electrónico o la investigación en el área de la salud, se han convertido en parte integral e integradora de la economía globalizada. Efectivamente, el flujo internacional de datos personales no sólo constituye una industria auxiliar respecto de empresas, entidades o personas que se dedican a realizar o utilizar las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional sino en un sector económico creciente, en sí mismo considerado.

5. Es innegable que esta transformación cualitativa y cuantitativa en los flujos internacionales de datos personales ha hecho más eficientes a las empresas y ha coadyuvado al desarrollo de la Sociedad de la Información y a la mundialización de la actividad económica. Pero tales contribuciones no se han realizado sin costes, ya que han puesto en peligro la vida privada del titular de esos datos. A nadie escapa que, sin demasiadas dificultades técnicas, la información puede ser objeto de un tratamiento ilícito; esto es, de una transferencia internacional de datos personales sin consentimiento del interesado, concluyendo en una violación de sus derechos fundamentales, constitucionalmente protegidos. De ahí la aparición de diversos expedientes reguladores, presentes en los distintos niveles de producción jurídica –

supraestructura jurídica internacional, plataformas de integración regional, estados y entidades subordinadas– y la necesaria cooperación de autoridades al efecto de prevenir y combatir dichas violaciones.

6. El objeto de la protección de datos es proporcionar a su titular mecanismos de defensa adecuados y efectivos frente a la obtención o tratamiento ilícito de la información de naturaleza personal. Esto se logra mediante un juego contrapuesto de atribución de derechos para el titular de los datos y de imposición de obligaciones para aquellos que captan o procesan los mismos y/o ejercen un control sobre dicho tratamiento de datos. La búsqueda de soluciones equidistantes en la satisfacción de los intereses legítimos implicados en las transferencias internacionales de datos no es fácil. En especial, debido a las diferencias palmarias existentes en el panorama comparado entre los distintos niveles de protección de los derechos y libertades de las personas y su intimidad.

En esta materia el mundo se encuentra dividido en tres grandes grupos de regulación de la protección de datos de carácter personal –y, por tanto, de las transferencias internacionales de datos personales–: primero, el que forman los Estados donde existe legislación en materia de protección de datos;[3] segundo, el que forman aquellos Estados en los que se está trabajando en *pro* de una legislación en materia de protección de datos;[4] y tercero, el que integran aquellos Estados donde la legislación en materia de protección de datos brilla

[3] Así, p. ej., sería el caso de los Estados miembros de la UE, Argentina, México, Canadá o EE.UU.

[4] Así, p. ej., en algunos Estados de la región latinoamericana, como en Perú, Ecuador, Colombia, Chile o Uruguay.

por su ausencia.[5] La ausencia de protección puede dar lugar a lo que se denominan «paraísos de datos»: Estados donde pueden tratarse todo tipo de datos de carácter personal, sin ningún tipo de restricciones o límites legales; datos que, una vez tratados, se pueden expedir a otros en los que sí existe un nivel de protección, burlándose, de esta forma, la aplicación de la legislación de protección de datos de dicho país[6] y haciendo patentes las dificultades o imposibilidades del titular del derecho a la protección de datos de carácter personal para obtener tutela en caso de un litigio internacional por el tratamiento ilícito de sus datos de carácter personal.

Las diferencias existentes en la tutela dispensada por las disposiciones pertinentes de los diferentes ordenamientos son susceptibles tanto de obstaculizar la libre transmisión de datos cuanto de burlar su correcta realización: si el régimen de tratamiento es más gravoso en un país que en otro, ello puede incentivar el desarrollo de estrategias comerciales o de establecimiento que busquen evitar la aplicación de estándares elevados de protección.[7] Con ello entramos en el tercer argumento esgrimido para justificar el objeto del presente proyecto de investigación: la complejidad de la protección jurídica de los derechos del titular de datos de carácter personal ante una transferencia internacional de los mismos.

7. La paulatina configuración de un mercado a escala mundial y la consiguiente multiplicación de transacciones económicas y relaciones derivadas de las mismas ha ocasionado un aumento notable de los

---

5 Sería el caso, p. ej., de Estados como Rusia, Malasia o Taiwán.

6 *Vid.* Rafael VELÁZQUEZ BAUTISTA, *Protección jurídica de datos personales automatizados*, Colex, Madrid, 1993, p. 184.

7 *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.*, pp. 21-22.

flujos transfronterizos de datos de carácter personal, entre distintos agentes públicos y privados establecidos en diferentes Estados. La necesidad de regular adecuadamente este fenómeno es innegable pero es evidente que se trata de una materia compleja, dada la difícil conciliabilidad de intereses tan dispares como la protección de la intimidad personal, las legítimas aspiraciones comerciales de las empresas involucradas en el tratamiento internacional de datos, y la libertad de información y comunicación.[8] Tal variedad de intereses y su relevancia hacen aparecer relaciones que afectan a ramas tan distintas del ordenamiento jurídico como el Derecho internacional público, con la creciente celebración de acuerdos internacionales de cooperación entre autoridades de control; el Derecho internacional privado, con la multiplicación de situaciones derivadas del incumplimiento de un contrato internacional de tratamiento de datos personales, la cesión o transferencia no consentida de los mismos a escala mundial; el Derecho público, con el manejo de datos por parte de la Administración o con la imposición de sanciones administrativas por el incumplimiento de la normativa aplicable en materia de protección de datos personales.

8. Como se acaba de exponer, la protección de datos de carácter personal puede ser contemplada desde posiciones muy distintas, en función de los intereses concurrentes —los derechos fundamentales de las personas *vs.* la consideración económica de la información personal y la diversidad de sistemas—[9] o de las diferentes ramas del Derecho implicadas en la regulación de un fenómeno que no es sencillo. Esa

---

8 *Vid.*, en el mismo sentido, Olga ESTADELLA YUSTE, «La transmisión internacional de datos personales y su control», en *Jornadas sobre Derecho Español de Protección de Datos Personales*, Agencia de Protección de Datos, Madrid, 1996, p. 195.

9 *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.*, p. 20.

complejidad no sólo ocupa y preocupa al común de la población, sino que presenta un innegable atractivo académico y práctico, que se explica por dos factores básicos:

Primero, por el desarrollo global del comercio electrónico y demás servicios de la Sociedad de la Información. Resulta evidente que esta nueva configuración del marco económico y social redunda en un incremento de relaciones en las que está implicada la transferencia internacional de información sensible, con el consiguiente aumento de la litigiosidad y la creciente dimensión económica que está cobrando el libre tránsito de la información. El acceso y uso de la información por parte de empresas, administraciones e individuos se ha convertido en un precioso bien intangible, causa y efecto a la vez de la progresiva integración económica y social. Como no podía ser de otro modo, dicha expansión supone afrontar la difícil tarea de compatibilizar los derechos fundamentales con las exigencias del comercio internacional, cuya liberalización —entronizada como principio rector por textos jurídicos fundamentales a escala mundial (OMC) o regional (UE, Mercosur, etc.)— es un límite básico a la hora de desarrollar expedientes reguladores.

Segundo, por la presencia de empresas transnacionales que actúan a escala mundial, lo que en buena lógica supondría la necesidad de articular una respuesta tuitiva de los derechos del titular de datos de carácter personal también a escala global. No obstante, las dificultades teóricas y prácticas de tal empeño suponen que, de momento, nos debamos contentar con llegar a simples acuerdos de cooperación entre las distintas autoridades reguladoras.[10] Así, en el seno de la UE, se van

[10] *Vid.* Considerando 56.º de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas

realizando esfuerzos de coordinación de la legislación de los Estados Miembros, de modo que dispensen una defensa «adecuada» o «equivalente», sin perjuicio de reconocerles un margen de maniobra, que han de ejercer de conformidad con el Derecho de la UE y dentro de los límites de la propia Directiva 95/46/CE.[11]

9. Curiosamente, y con ello pasamos a exponer otro de los elementos anunciados para justificar la elección del objeto de estudio, pese a la actualidad, relevancia y virtualidad práctica de las cuestiones expuestas, falta en nuestra doctrina un estudio de los problemas que plantean las transferencias internacionales de información de carácter personal desde la perspectiva concreta del Derecho internacional privado y la protección del titular de los datos.[12] Cierto que contamos con magníficas contribuciones que abordan cuestiones generales, como el

---

en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: «Considerando que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias.»

11 Con ese propósito, la propia Directiva 95/46/CE obliga a los Estados miembros a garantizar las libertades y los derechos fundamentales de los individuos en lo que respecta al tratamiento de los datos personales y su transferencia internacional, sin que les quepa restringir ni prohibir la libre circulación de esos datos por motivos relacionados con tal tutela.

12 Es preciso destacar un par de estudios específicos sobre las operaciones de tratamiento internacional de datos personales y sobre el régimen jurídico aplicable a la transferencia internacional de datos de carácter personal: Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.;* y Diana SANCHO VILLA, *Transferencia internacional...*, *op. cit.*

derecho privado de Internet,[13] o aspectos puntuales como la iniciativa del Parlamento Europeo tendente a revisar el Reglamento «Roma II», con el objeto de incluir una regla específica en materia de violación de la intimidad o de los derechos relacionados con la personalidad.[14] Pero, a mi juicio, falta una contribución que abandone el enfoque general, propio de una perspectiva estructural, para centrarse en una visión finalista o tuitiva, que ponga el acento en la protección del titular de los datos de carácter personal ante una transferencia internacional ilícita de los mismos.

10. La ausencia de una tan deseable como, por el momento, irrealizable regulación verdaderamente internacional de las transferencias internacional de datos de carácter personal y el carácter potencialmente limitado de las experiencias reguladoras regionales convierten a los sistemas nacionales de Derecho internacional privado en el último refugio del titular de datos de naturaleza personal, enfrentado a una violación de sus derechos.

En primer lugar, las soluciones uniformes se ven dificultadas por las distintas calificaciones que reciben las diferentes categorías de datos personales y por el carácter dinámico del comercio internacional, poco favorable a la esclerotización que siempre supone la regulación de un determinado sector. Los logros más fundamentales, al menos por el momento, consisten en las acciones concertadas entre diferentes sistemas jurídicos, que permiten, además de la consecución de

---

13 Alfonso-Luis Calvo Caravaca y Javier Carrascosa González, *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001; Pedro De Miguel Asensio, *Derecho privado de Internet*, 4.ª ed., Civitas, Cizur Menor (Navarra), 2011.

14 Documento de Trabajo del Comité de Asuntos Legales del Parlamento Europeo. DT\836983EN.doc, de 23/05/2011.

economías de escala sobre los costes de circulación internacional de la información, un aumento de la seguridad jurídica, impidiendo la constitución de «paraísos de datos»[15] y la deslocalización de actividades informáticas.

En segundo lugar, la especial volatilidad de las transferencias internacionales de datos complica extraordinariamente la definición del derecho sustantivo aplicable. Las características de los flujos de información y el carácter abierto de las redes posibilitan el acceso a los datos, así como su recopilación y tratamiento simultáneo en y desde varios países, por lo que distintos Estados podrán reclamar competencia jurisdiccional y/o normativa para definir los términos y las condiciones de las prácticas apropiadas en el ámbito del tratamiento de la información sensible.

11. La innegable vocación de internacionalidad propia de las relaciones implicadas en una transferencia de datos de carácter personal es terreno abonado para la aparición de problemas que son objeto de estudio por parte del Derecho internacional privado. Por un lado, la inmensa mayoría de las operaciones de tratamiento de datos personales son *supuestos con repercusión transfronteriza*. Así, las relativas a las prestaciones de servicios de tratamiento que acuerdan los empresarios entre sí —ya impliquen la cesión o comunicación de datos entre responsables o bien el acceso a los mismos por un encargado o suben-

[15] La idea es clara: «se persigue, de este modo, que el tratamiento de los datos se lleve a cabo en países carentes de una legislación que protege la *privacy* de los individuos frente al uso de la informática o que disponen de una legislación poco exigente al respecto —los llamados 'paraísos informáticos'—». *Vid.* Javier CARRASCOSA GONZÁLEZ, «Circulación internacional de datos personales informatizados y la Directiva 95/46/CE», en *Actualidad Civil*, núm. 23, 1997, p. 512.

cargado— donde la presencia de uno o varios elementos de extranjería las pueden convertir en *internacionales.* Sería el caso de la localización de los profesionales implicados en Estados diferentes, o por la propia salida de los datos de un Estado a otro, o de un territorio de protección a un tercer Estado. Por otro lado, al margen de su innegable pluridisciplinariedad, las transferencias internacionales de datos son susceptibles de originar múltiples relaciones jurídicas *privadas*, tanto contractuales como extracontractuales. Así, por ejemplo, la que vincula a la persona física afectada por la transferencia de sus datos de carácter personal con un empresario establecido en el extranjero, que capta o trata irregularmente esos datos.

12. La potencial pluralidad de ordenamientos jurídicos implicados en la protección de la correcta circulación internacional de datos de naturaleza personal y la existencia en sí de transferencias internacionales de tales datos, consecuencia del creciente carácter internacional de las relaciones personales y comerciales, exige la intervención del Derecho internacional privado;[16] pero no una intervención cualquiera. Como se expondrá a lo largo de este proyecto de investigación, se trata tanto de describir, analizar y comparar el sistema vigente cuanto de explorar la virtualidad de dicho sistema frente a un problema jurídico específico: la tutela adecuada, equilibrada y eficaz del perjudicado por un tratamiento ilícito de sus datos de carácter personal, derivado de una transferencia internacional. Esta visión particular y tuitivamente orientada exige una metodología especial, que no parte de la tradicional

[16] *Vid.* de Javier CARRASCOSA GONZÁLEZ, «Circulación internacional..., *op. cit.,* pp. 510-511; y «Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado», en *Revista Española de Derecho Internacional,* vol. XLIV, núm. 2, 1992, pp. 417-418.

exposición de las cuestiones clásicas del Derecho internacional privado sino del problema en sí: la desprotección del titular de datos de carácter personal. Para demostrar tal estado deficitario, muchas de las páginas que siguen se servirán de contribuciones de otras disciplinas jurídicas (Derecho Económico Internacional, Derecho internacional público o Derecho de la UE) para acabar concluyendo que las transferencias internacionales de datos de carácter personal ilícitas constituyen un auténtico desafío para el Derecho internacional privado.

II. MÉTODOLOGÍA DE INVESTIGACIÓN

13. Explicadas las variadas razones que justifican la elección del objeto de estudio, a continuación se pasa a exponer la metodología de investigación que se aplicará sobre el mismo. El Proyecto de Tesis Doctoral tiene como objeto demostrar la situación de desprotección en que se encuentra una persona, enfrentada a la obtención y/o tratamiento ilícito de sus datos de carácter personal, en el marco de una transferencia internacional de información.

La comprobación de tal estado de cosas se inicia con un análisis de las reglas y mecanismos existentes en los distintos niveles de producción normativa: superestructura jurídica internacional, plataformas de integración regional, respuestas autónomas estatales, e iniciativas propias del llamado «espacio transnacional». Análisis que revela una situación que dista mucho de ser satisfactoria y que concluirá demostrando que la normativa de Derecho internacional privado es, de lejos, la más sencilla y manifiestamente mejorable. En efecto, con un mínimo coste nomogenético, tanto la posible reinterpretación de las normas vigentes cuanto la eventual elaboración de nuevas reglas arrojan resultados mucho más equilibrados, efectivos y adecuados, al menos

desde la perspectiva del titular del derecho a la protección de datos de carácter personal.

14. El carácter deslocalizado de la mayoría de las infracciones de derechos que traen su causa de una transferencia internacional de datos de carácter personal suponen un auténtico desafío para la metodología aplicada habitualmente en los estudios de Derecho internacional privado, entendida como estudio del tríptico de problemas específicamente propios de las relaciones privadas internacionales: competencia judicial internacional, determinación de la ley aplicable, reconocimiento de actos y decisiones extranjeros. Esta plantilla tradicional resulta poco clarificadora cuando se refiere a problemas que se sitúan en la intersección misma de dos fenómenos —superación de los mercados nacionales e infracciones en Internet— que rompen los moldes localizadores tradicionales.

La posible solución a los conflictos que surgen en ese contexto aparece con mayor nitidez a partir de un enfoque problemático. Visto el supuesto desde esa perspectiva, resulta evidente que la salvaguarda de los legítimos intereses del titular del derecho a la protección de datos personales puestos en peligro por una transferencia internacional ilícita, se puede conseguir si se adoptan las medidas adecuadas que equilibren la balanza entre la protección de los derechos fundamentales de la persona y las exigencias del comercio internacional, en general, y el establecimiento, en particular, de un auténtico mercado internacional de datos.

15. La metodología a seguir se desplazará en un triple sentido: punto de partida problemático, descripción de la normativa existente o legislación de *lege data*, y proposición de nuevas reglas o propuestas de *lege ferenda*. Planteado inicialmente el supuesto típico —los litigios

relativos a la responsabilidad extracontractual derivada del tratamiento ilícito de datos de carácter personal, consecuencia de una transferencia internacional— se analizarán las lagunas y limitaciones del régimen jurídico vigente, su aplicación e interpretación, recurriendo a fuentes legislativas y jurisprudenciales y a las contribuciones doctrinales más relevantes. La implementación de esta metodología trifronte permitirá poner de relieve las dificultades o incluso la imposibilidad del titular del derecho a la protección de datos de carácter personal para obtener una tutela que debe reunir las siguientes características: adecuada, equilibrada y eficaz.

16. Dicha caracterización parte de la toma de conciencia de la necesidad de encontrar un punto de equilibrio entre la actual situación de desprotección y las tentaciones de caer en propuestas superprotectoras que conduzcan a resultados contrarios a los perseguidos. Consecuentemente, el presente proyecto de investigación no se detiene en la denuncia del *status quaestionis*, sino que propone una mejora relativamente sencilla de las reglas de Derecho internacional privado que procuren al titular de un derecho fundamental, enfrentado al tratamiento ilícito internacional de sus datos de carácter personal, una protección suficientemente adecuada, que generalmente consistirá en una reparación económica; equilibrada, que tenga en cuenta la complejidad derivada de la pluralidad de intereses legítimos en presencia; y eficaz, es decir, fácilmente realizable y accesible.

III. METODOLOGÍA DE EXPOSICIÓN

17. El método de investigación referido se desarrolla en el siguiente esquema lógico o método de exposición. En primer lugar, se partirá

del deslinde del objeto de estudio, para establecer el supuesto típico a examinar: los problemas de desprotección del titular del derecho a la protección de sus datos de carácter personal, derivados de una infracción extracontractual que trae su causa de la transferencia internacional de información (**capítulo I**). A continuación, se analizan los diferentes mecanismos de protección a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, para obtener una tutela adecuada, equilibrada y efectiva en los distintos centros de producción normativa: superestructura jurídica internacional, sistemas de integración regional, y espacio transnacional (**capítulo II**). En tercer lugar, se estudiará la posible satisfacción de los problemas derivados del supuesto típico, desde la perspectiva del Derecho internacional privado, centrándose en los sectores de la resolución judicial de controversias (**capítulo III**) y la determinación de la ley aplicable (**capítulo IV**). No se analizarán los problemas de reconocimiento y ejecución de resoluciones judiciales porque no presentan ninguna particularidad en este caso. Finalmente, el proyecto de investigación se cierra con unas ***conclusiones*** que permitirán reivindicar las posibilidades de mejora del sistema de Derecho internacional privado para procurar al titular del derecho a la protección de datos personales una tutela adecuada, equilibrada y eficaz de sus intereses legítimos, cuando se enfrenta a una infracción extracontractual, derivada de la transferencia internacional ilícita de sus datos de carácter personal.

Capítulo 1.

Aproximación conceptual a las transferencias internacionales de datos de carácter personal

18. El presente proyecto de Tesis Doctoral parte de un problema identificado a partir del estudio de campo que conduce a un supuesto tipo: la situación de desprotección en que se encuentra una persona, enfrentada a la obtención y/o tratamiento ilícito de sus datos de carácter personal, en el marco de una transferencia internacional de información.

En este **capítulo I**, en primer lugar, se trata de deslindar el objeto de estudio y fijar el supuesto tipo. Para ello se procederá a dar respuesta a diferentes cuestiones tales como: ¿Qué debe entenderse por «transferencia internacional de datos»? y ¿Cuál es su importancia socioeconómica hoy día? (I) ¿Quiénes son los sujetos participantes en las transferencias internacionales de datos? (II) y ¿Qué criterios diferenciadores podemos utilizar para clasificarlas? (III); en última instancia, establecer el supuesto tipo a examinar: las dificultades con que se encuentra el titular del derecho a la protección de sus datos de carácter personal, derivados de una infracción extracontractual que trae su causa de la transferencia internacional de información (IV).

1. Concepto de transferencia internacional de datos de carácter personal

19. El primer objetivo, como se ha señalado, es deslindar el objeto de estudio: la transferencia internacional de datos de carácter personal. Para ello, en primer lugar, vamos a partir de un estudio de campo; en segundo lugar, daremos un concepto instrumental; para en tercer lugar, atender a la normativa y a la jurisprudencia del TJUE existente para deslindar el objeto de estudio y fijar el supuesto tipo.

20. El crecimiento de los flujos internacionales de información ha multiplicado las solicitudes de autorización de transferencias internacionales de datos de carácter personal: comunicaciones de datos personales entre las filiales de una empresa multinacional, utilización de herramientas multiacceso, prestación de servicios desde distintos países, o la gestión integral de los procesos de recursos humanos de una multinacional, están a la orden del día.[17]

El aumento de las transferencias internacionales de datos personales[18] en áreas tales como la de los recursos humanos, los servicios financieros, la banca, la educación, el comercio electrónico, el auxilio judicial internacional o la investigación en el área de la salud son aho-

[17] *Vid.*, en particular, Rafael García Del Poyo y Francisco Gari, «Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales», en *Revista Española de Protección de Datos*, núm. 2, Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, 2007, pp. 239-266.

[18] *Vid.* Juan Manuel Fernández López, «Movimiento internacional de datos y buen gobierno corporativo», en *Boletín del Ilustre Colegio de Abogados de Madrid*, núm. 35, 3.ª ép., Febrero 2007, p. 177.

ra una parte integral de la economía globalizada. En materia de regulación de la protección de datos de carácter personal pueden diferenciarse tres grandes grupos. Un primer grupo formado por los Estados donde existe legislación en materia de protección de datos actual, vigente y adaptada al momento actual (p. ej., sería el caso de los Estados miembros de la UE, Argentina, México, Canadá o EE.UU.); el segundo grupo, el formado por aquellos países en los que se está trabajando en *pro* de una legislación en materia de protección de datos (p. ej., en algunos países de la región latinoamericana, como en Perú[19], Ecuador[20], Colombia[21], Chile[22] o Uruguay[23] se están planteando en la actualidad «adaptaciones» de su legislación en materia de protección de datos)[24]; y el tercer grupo es el integrado por aquellos países donde, a día de hoy, la legislación en materia de protección de datos brilla por su ausencia (el caso, p. ej., de países como Rusia, Malasia o Taiwán).

Los principales sectores de actividad en que operan las entidades exportadoras de datos son telecomunicaciones, energía, servicios informáticos, banca, industria química y farmacéutica y publicidad di-

19 *Vid.* Reglamento de la Ley núm. 29733 peruana de «Protección de Datos Personales» (Decreto Supremo núm. 003-2013-JUS), Diario El Peruano, Lima, viernes 22/03/2013.

20 *Vid.* Proyecto de Ley sobre «Protección a la Intimidad y a los Datos Personales».

21 *Vid.* Ley Estatutaria núm. 1581, de 17 de octubre de 2012, «por el cual se dictan disposiciones generales para la protección de datos personales».

22 *Vid.* las modificaciones planteadas a la Ley núm. 19628 sobre «Protección a la vida privada o protección de datos de carácter personal», de 28/08/1999.

23 *Vid.* Ley núm. 18331 de «Protección de datos Personales y Acción de 'Habeas Data'» de 11/08/2008; y su Decreto regulatorio de 31/08/2009.

24 Si bien los países de América Latina han mirado hacia el modelo europeo, también han mantenido particularidades y motivaciones diferentes a la hora de aprobar su normativa de protección de datos.

recta. El conjunto de estos factores pone de manifiesto que se están produciendo decisiones empresariales autónomas que llevan consigo un fenómeno de deslocalización de actividades empresariales en estos sectores y países, para las que la obtención de una autorización de transferencia internacional de datos es un elemento instrumental necesario desde el punto de vista legal.[25]

21. En efecto, atendiendo a la modalidad, objeto y destino de las transferencias internacionales de datos autorizadas, destacan tres fenómenos interrelacionados donde debemos extremar la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: *1)* que la principal modalidad de transferencia es la que se lleva a cabo entre un responsable ubicado en España, principalmente dedicado a servicios de telecomunicaciones, y una empresa prestadora de servicios en un tercer país (encargado del tratamiento de datos), al amparo de las cláusulas contractuales tipo previstas en la Decisión de la Comisión Europea 2002/16/CE, de 27 de diciembre de 2001;[26] *2)* la diversifica-

[25] Las transferencias internacionales de datos responden a diversos objetivos que se pueden diferenciar entre: *a)* Aquellas relacionadas con la gestión empresarial en un contexto global. Las empresas multinacionales requieren la realización de transferencias internacionales de datos para finalidades tales como la gestión, mantenimiento y soporte técnico de los sistemas de información (sobre todo en relación con la gestión eficiente de los recursos humanos, los clientes y los proveedores, así como la prestación de servicios de apoyo administrativo en relación con estos); y *b)* Aquellas relacionadas con la atención telefónica a los clientes y otras acciones de marketing telefónico dirigidas a mejorar el grado de satisfacción de los mismos, como la gestión centralizada de los servicios de atención al cliente. En este grupo destacan principalmente las prestaciones de servicios de atención al cliente o *telemarketing*.

[26] *DO* 2002 L 6/52.

ción de las áreas geográficas a las que se transfiere los datos personales: los EE.UU. siguen siendo el primer importador de datos desde España y los países latinoamericanos se consolidan en segunda posición (principalmente, Chile, Colombia, Perú, Paraguay y Uruguay). Pero han aparecido nuevos países de destino de las transferencias en Asia, destacando India, que en los últimos años ha triplicado el número de expedientes tramitados y tiende a convertirse en uno de los principales importadores de datos personales. También ha aumentado el número de autorizaciones con destino a Marruecos; y, *3)* que las transferencias autorizadas corresponden, en un alto porcentaje, a prestaciones de servicios que se realizan en terceros países, lo que es indicativo de la importancia que va adquiriendo la deslocalización de actividades que se externalizan en dichos países.[27]

22. La transferencia internacional de datos de carácter personal merece especial atención tanto desde un punto de vista socioeconómico como jurídico por parte de todas las legislaciones en materia de protección de datos de nuestro entorno, aunque legalmente no se haya

[27] Desde la perspectiva española, las categorías de transferencias internacionales de datos de carácter personal son, en la práctica, de tres tipos: *a)* Transferencias de datos personales derivadas de la optimización de la gestión de recursos por una empresa, cuya matriz, española o central, se halla en un país extranjero; *b)* Transferencias de datos personales ligadas a la naturaleza de la actividad o producto (p. ej., reservas de billetes de avión o de plazas hoteleras en el extranjero contratadas a través de agencias de viajes en España); y, *c)* Transferencias de datos personales destinadas a mejorar el servicio al cliente (p. ej., en los casos en los que se encarga el tratamiento de datos a un tercero en el extranjero, cuya gestión permitirá que el servicio que se presta al cliente sea más eficaz).

conceptuado de forma completa lo que debe entenderse por «transferencia internacional de datos».[28]

---

[28] Se trata de un tema tratado ampliamente por la doctrina más autorizada, nacional y extranjera. *Vid.,* entre otros, Cristina ALMUZARA ALMAIDA (Coord.) y otros, *Estudio práctico sobre la protección de datos de carácter personal*, 2.ª ed., Lex Nova, Valladolid, 2007, pp. 383-417; Oscar José ÁLVAREZ CIVANTOS, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Comares, Granada, 2001, pp. 88-111; Javier APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Elcano (Navarra), 2000, pp. 213-214; Miguel Ángel DAVARA RODRÍGUEZ, (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2004*, Fundación VODAFONE, Madrid, 2004, pp. 15-27 y 38-56; *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2003*, Fundación VODAFONE, Madrid, 2003, pp. 3-21; Gabriel FREIXAS GUTIÉRREZ, *La protección de los datos de carácter personal en el Derecho español. Aspectos teóricos y prácticos*, Bosch, Barcelona, 2001, pp. 345-356; Ana GARRIGA DOMÍNGUEZ, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004, pp. 177-181; Vicente GUASCH PORTAS, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, 2014, pp. 46-48; Yves POULLET, «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid- CIVITAS, Madrid, 2007, pp. 93-113; François RIGAUX, «Le régime des données informatisées en droit international privé», en *Journal du droit international*, vol. 113, 1986, pp. 311-328; y, Santiago RIPOLL CARULLA, «El Movimiento Internacional de Datos en la Ley Española de Protección de Datos», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, números 6-7, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 1994, pp. 313-322. *Vid.*, sobre la terminología a utilizar —«transmisión internacional de datos», «flujo internacional de datos» o «transferencia internacional de datos»—, Joan PIÑOL I RULL y Olga ESTADELLA YUSTE, «La regulación de la transmisión internacional de datos en la L.O. 5/1992 de 29 de octubre», en Santiago RIPOLL I CARULLA (Coord.), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Universitat Pompeu Fabra, Barcelona, 1993, pp. 78-79.

La expresión «transferencia internacional de datos»[29] debe considerarse aplicable a todos los flujos de datos a través de las fronteras, independientemente de cuál sea el soporte mediante el que se envían los datos o la forma de tratamiento.

Desde la óptica española vendría a constituir todo «tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español» (arts. 5.1.s del ROLPD y 1.2 y 25 de la Directiva 95/46/CE).[30]

23. Varios son, a muestro juicio, los elementos a examinar para poder conceptuar una transferencia internacional de datos de carácter personal:

– **Primero:** Debe tratarse de datos de carácter personal, esto es, de «cualquier información numérica, alfabética, gráfica, fotográfica,

[29] *Vid.*, sobre la terminología a utilizar –«transmisión internacional de datos», «flujo internacional de datos», «transferencia internacional de datos», «movimiento internacional de datos», o «flujos de datos transfrontera»–, Joan PIÑOL I RULL, y Olga ESTADELLA YUSTE, «La regulación... *op. cit.*; Emilio Suñé Llinás, «Marco jurídico del tratamiento de datos personales en la Unión Europea y en España», en V*VID.*AA., *La armonización legislativa de la Unión Europea*, Dykinson, Madrid, 1999, pp. 267-269; Miguel Ángel DAVARA RODRÍGUEZ, «La Transferencia Internacional de Datos», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid-CIVITAS, Madrid, 2007, pp. 23-24; y, Diana SANCHO VILLA, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010, p. 23.

[30] La propuesta de Reglamento General de Protección de Datos (al igual que, en su día, la Directiva 95/46/CE) no define qué se entiende por «transferencia internacional de datos personales»

acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables».[31]

- **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) como prestación de un servicio (encargado de tratamiento).
- **Cuarto:** El traslado físico efectivo de los datos de carácter personal, de un lugar a otro, a través de las fronteras nacionales, ya sea dentro o fuera de la UE.
- **Quinto:** El lugar de destino de los datos de carácter personal debe encontrarse en un territorio distinto al de origen de los mismos.
- **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.

24. Con el propósito de seguir ahondando en el concepto de «transferencia internacional de datos» resulta necesario acudir a la jurisprudencia del TJUE que ha supuesto, en cierto modo, una reformulación del concepto en la Sentencia «Lindqvist», de 6 de noviembre de 2003, referente a la publicación de datos personales en Internet. Asunto C-

[31] *Vid.* arts. 3.a de la LOPD y 5.1.f del RLOPD.

101/01-Bodil Lindqvist),[32] al plantearse si la publicación de datos de carácter personal a través de una página *web* puede considerarse como tal.

La Sra. Lindqvist desempeñaba funciones de catequista en la parroquia de la localidad de Alseda, en Suecia. Hizo un curso de informática en el que, entre otras cosas, tenía que crear una página *web* en Internet. A finales de 1998, la Sra. Lindqvist creó, en su domicilio y con su ordenador personal, varias páginas *web* con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaran. A petición suya, el administrador del sitio Internet de la Iglesia de Suecia creó un enlace entre las citadas páginas y dicho sitio. Las páginas *web* de que

---

32 *Vid.* Joaquín BAYO DELGADO, «Derecho comunitario sobre protección de datos», en Carlos GÓMEZ MARTÍNEZ (Dir.), *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2004, pp. 59-60; Pedro A. DE MIGUEL ASENSIO, «Avances en la interpretación de la normativa comunitaria sobre protección de datos personales», en *La Ley Unión Europea*, núm. 5964, Madrid, 2003, pp. 1-4; Pedro A. DE MIGUEL ASENSIO, «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», en http://www.uaipit.com, 2003, pp. 1-12; M.ª Carmen GUERRERO PICÓ, *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 356-361; Manuel HEREDERO HIGUERAS, «La transmisión internacional de los datos de la salud...», *op. cit.*, pp. 192-195; Manuel PULIDO QUECEDO, «La catequista y los riesgos de Internet», en *Actualidad Jurídica Aranzadi*, año XIII, núm. 602, 4 de diciembre de 2003, Aranzadi, Cizur Menor (Navarra), pp. 14-15; y, Pedro SERRERA COBOS, *Buenas prácticas en protección de datos*, Fundación DINTEL, Madrid, 2007, pp. 28-31; y, sobre la actividad del TJUE en materia de protección de datos de carácter personal, Mónica ARENAS RAMIRO, «El derecho a la protección de datos personales en la jurisprudencia del TJCE», en Javier PLAZA PENADÉS (Coord.), *Cuestiones actuales de Derecho y Tecnologías de la información y la Comunicación (TICs)*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 95-119.

se trata contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre completo o, en ocasiones, sólo su nombre de pila. Además, la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar o el número de teléfono de sus compañeros. Asimismo, señaló que una de sus compañeras se había lesionado un pie y se encontraba en situación de baja parcial por enfermedad. La Sra. Lindqvist no había informado a sus compañeros de la existencia de estas páginas *web*, no había solicitado su consentimiento, ni tampoco había comunicado su iniciativa a la Datainspektion, organismo público para la protección de los datos transmitidos por vía informática. En cuanto supo que algunos de sus compañeros no apreciaban las páginas *web* controvertidas, las suprimió. En todo caso, por parte del Ministerio Fiscal se inició un proceso penal contra la Sra. Lindqvist por infracción de la Ley de Protección de Datos sueca (en lo sucesivo, la PUL), solicitándose que fuera condenada por: *a)* haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito a la *Datainspektion* (art. 36 de la PUL); *b)* haber tratado sin autorización datos personales delicados, como los relativos a la lesión en un pie y a la baja parcial por enfermedad (art. 13 de la PUL); y, *c)* haber transferido datos de carácter personal a países terceros sin autorización (art. 33 de la PUL).[33]

[33] La Sra. Lindqvist reconoció los hechos, pero, aunque negó que hubiera cometido una infracción, fue condenada al pago de una multa, interponiendo contra dicha resolución recurso de apelación. El importe de la multa ascendía a 4 000 SEK (aproximadamente 450 euros), tras haber aplicado a la suma de 100 SEK, que se calculó teniendo en cuenta la situación financiera de la Sra. Lindqvist, un multiplicador de 40 que representaba la gravedad de la infracción. Asimismo se con-

En opinión del TJUE, la Directiva 95/46/CE no define ni en su artículo 25 ni en ningún otro precepto, ni siquiera en su artículo 2, el concepto de «transferencia a un país tercero». Para determinar si la difusión de datos personales en una página *web* constituye una «transferencia» de dichos datos a un país tercero en el sentido del artículo 25 de la Directiva 95/46/CE por el mero hecho de que resultan accesibles a personas que se encuentran en un país tercero, es necesario tener en cuenta, por una parte, la naturaleza técnica de las operaciones efectuadas y, por otra, el objetivo y la organización sistemática del capítulo IV de la citada Directiva, en el que figura su artículo 25.

En consecuencia, procede responder a la cuestión que no existe una «transferencia a un país tercero de datos» en el sentido del artículo 25 de la Directiva 95/46/CE cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página *web*, almacenada por su proveedor de servicios de alojamiento de páginas *web* que tiene su domicilio en el mismo Estado o en otro Estado

---

denó a la Sra. Lindqvist a abonar 300 SEK a un fondo sueco que tiene por objeto ayudar a las víctimas de las infracciones.

Dado que albergaba dudas sobre la interpretación del Derecho de la UE aplicable al caso, en concreto, la Directiva 95/46/CE, el Göta hovrätt decidió suspender el procedimiento y plantear al TJUE, entre otras, la siguiente cuestión prejudicial: según la Directiva 95/46/CE, la transferencia de datos personales a países terceros está prohibida en determinados casos. ¿Constituye una transferencia a países terceros en el sentido contemplado en la Directiva 95/46/CE el hecho de que una persona divulgue datos personales en una página *web* que está almacenada en un servidor en Suecia, de modo que los datos personales resultan accesibles a nacionales de países terceros? ¿Sigue siendo idéntica la respuesta si, por lo que se sabe, ningún nacional de un país tercero ha accedido efectivamente a dichos datos o si el servidor en cuestión se encuentra físicamente situado en un país tercero?

miembro, de modo que dichos datos resultan accesibles cualquier persona que se conecte a Internet, incluidas aquéllas que se encuentren en países terceros.

No supone una transferencia a países terceros el hecho de que una persona divulgue datos personales en una página *web*, que está almacenada en un servidor en la UE, de modo que los datos personales resulten accesibles a nacionales de Estados extracomunitarios[34] —aunque sí constituye en sí mismo un tratamiento de datos conforme a la Directiva 95/46/CE—. Para que exista transferencia internacional de datos es fundamental el hecho de que «exista un cierto movimiento de los datos de carácter personal», esto es, que el emisor adopte una posición activa y transfiera los mismos; no pudiendo considerar como transferencia el hecho de que desde un tercer Estado, desde una posición pasiva, se acceda a unos datos colgados en una *web*.[35]

---

[34] La transferencia de datos, internacional o no, se produciría si existiera una transferencia directa entre quien revela los datos y quien los recibe, pero no, en palabras del propio TJUE, cuando «se han transmitido con la ayuda de la infraestructura informática del proveedor de servicios de alojamiento páginas web donde está almacenada la página». Ahora bien, la transmisión del contenido de la página *web* al proveedor de servicios de alojamiento sí que puede implicar una transferencia internacional de datos, al haber una transferencia directa entre quien revela los datos (el titular de la página *web*) y quien los recibe (el proveedor de servicios en suyo servidor se aloja esa información), cuando tenga lugar a un país tercero. *Vid.* Pedro A. De Miguel Asensio, «Avances..., *op. cit.*, p. 3-4.

[35] La misma solución plantea Suquet Capdevila en materia de infracciones de derecho de propiedad industrial en Internet. *Vid.* Josep Suquet Capdevila, «Internet, marcas y competencia judicial internacional: ¿O la superación de la regla *forum loci delicti commissi*? A propósito de la sentencia de la Cour de Cassation de 9 de diciembre de 2003», en *La Ley Unión Europea*, núm. 6073, Madrid, 2004, pp. 1-7; y Palao Moreno respecto de la consideración de la mera accesibilidad de un sitio *web* desde un determinado Estado como criterio para justificar la competencia de unos determinados tribunales, *Vid.* Guillermo Palao Moreno, «Com-

Parece evidente que el TJUE optó por la «solución más fácil»[36] al referirse a qué debemos entender por «transferencia internacional de datos», pues teniendo en cuenta el estado de desarrollo de Internet en el momento de elaboración de la Directiva 95/46/CE y la inexistencia de criterios aplicables al uso de Internet, el legislador comunitario no tenía la intención de incluir en el concepto de «transferencia a un país tercero de datos» la difusión de datos en una página *web*, ni siquiera cuando estos últimos resulten accesibles a personas de países terceros.[37]

25. Además, del supuesto analizado en la Sentencia «Lindqvist», existe un segundo supuesto de hecho excluido del concepto de transferencia internacional de datos: la transmisión de datos realizada por un usuario de Internet en España que visita un sitio *web* de un responsable

---

petencia judicial internacional en supuestos de responsabilidad civil en Internet», en Javier PLAZA PENADÉS, *Cuestiones actuales de derecho y Tecnologías de la Información y Comunicación (TICs)*, Editorial Aranzadi, Cizur Menor (Navarra), 2006, p. 291.

36 En palabras de Davara Rodríguez, «Concluyente pero, a nuestro entender, desilusionante». *Vid.* Miguel Ángel DAVARA RODRÍGUEZ, «La Transferencia Internacional...», *op. cit.*, pp. 54-56 (en particular, p. 56); y, según Poullet, «una decisión arriesgada del TJCE», *Vid.* Yves POULLET, «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid-CIVITAS, Madrid, 2007, pp. 106-108.

37 Como bien señala Pulido Quecedo, «una vez más, el TJUE actúa como instrumento de integración europeo, resaltando, en el presente caso, el carácter de normación completa de la Directiva, y no mínima, que puede ser desarrollada por los Estados miembros. Éstos podrán internamente regular aquellas situaciones no comprendidas en el ámbito de aplicación de esta última y cuando ninguna otra norma de Derecho comunitario se oponga a ello». *Vid.* Manuel PULIDO QUECEDO, «La catequista y los riesgos de Internet», en *Actualidad Jurídica Aranzadi*, año XIII, núm. 602, 4 de diciembre de 2003, Aranzadi, Cizur Menor (Navarra), p. 15.

establecido en un tercer Estado. Los datos que salen del territorio español no quedan bajo el ámbito territorial de la LOPD (= art. 2 de la LOPD), a pesar de que utilizan medios situados en España, pero tan sólo se utilizan con fines de mero tránsito.[38]

26. El TJUE en la Sentencia «Lindqvist» dictaminó que no existe una «transferencia a un país tercero de datos», en el sentido del artículo 25 de la Directiva 95/46/CE, cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página *web*, almacenada por su proveedor de servicios de alojamiento de páginas *web*, que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquéllas que se encuentren en países terceros.[39]

¿Qué hubiera ocurrido si la respuesta del TJUE hubiera sido otra? sí existe una transferencia de datos personales a un país tercero cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página *web*, almacenada por una persona física

---

38 *Vid.* Juan ZABÍA DE LA MATA, (Coord.), *Protección de datos. Comentarios al Reglamento*, 1.ª ed., Lex Nova, Valladolid, 2008, pp. 581-582.

39 *Vid.*, en el mismo sentido, STJUE (Sala Tercera) de 18 de octubre de 2012, «Football Dataco II», con ocasión del envío por una persona, a través de un servidor web situado en un Estado miembro A, de datos obtenidos por esta persona a partir de una base de datos al ordenador de otra persona establecida en un Estado miembro B, a solicitud de esta última para ser almacenados en la memoria de este ordenador y ser visualizado en su pantalla. *Vid.* Carmen GARCÍA MIRETE, «El lugar en el que se produce la reutilización de una base de datos electrónica en Internet: el caso Football Dataco vs. Sportradar», AEDIPr, t. XII, 2012, pp. 555–565; y «Localización del lugar o lugares en que se entiende cometida la infracción de los derechos de propiedad intelectual», AEDIPr, t. XII, 2012, pp. 970-974.

o jurídica que gestiona el sitio Internet en el que se puede consultar la página *web* y que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros.

¿Qué ocurriría si bajo el prisma del artículo 25 de la Directiva 95/46/CE, la difusión de datos personales en una página *web* constituyera una «transferencia internacional» de dichos datos a un país tercero, por el hecho de que resultan accesibles a personas que se encuentran en un país tercero?

Teniendo en cuenta el estado de desarrollo actual de Internet[40] y de los sistemas informáticos, el legislador comunitario debería reflexionar e incluir en el concepto de «transferencia a un país tercero de datos» la difusión de datos en una página *web*.[41] Es más, si para que

---

[40] En este mundo actual caracterizado por la *«velocité, ubiquité, liberté»*, las nuevas tecnologías, la comunicación e Internet entrañan una forma de vulneración de los derechos de los particulares. *Vid*., en general, Erik JAYME, «Le droit international privé du nouveau millénaire: la protection de la personne humaine face à la globalisation», en *Recueil des Cours. Collected Courses of The Hague Academy of International Law, Tome 282*, Martinus Nijhoff Publishers, The Hague, 2000, pp. 9-40; y, en relación con la problemática que plantea Internet en Alemania, Ulrich SIEBER, «Criminal Liability for the Transfer of Data in International Computer Networks. New Problems for German Law», en *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 5, núm. 1, 1997, pp. 134-143.

[41] Así, p. ej., a nuestro modo de ver, todas aquellas actuaciones del empresario establecido en un tercer Estado que supongan la colocación de *cookies* en el ordenador del usuario que se conecta a la página *web* de aquél o la descarga de aplicaciones *javascript* por el internauta para acceder a los contenidos de la página que quiere visitar y mediante las cuales el empresario recaba datos personales para su tratamiento, tiene una doble consecuencia: *a)* supone la utilización de un medio situado en España como criterio determinante de la aplicación de la LOPD; y *b)* los datos personales que *viajan* en la *cookie* rumbo al responsable establecido en ese

exista transferencia internacional de datos es fundamental el hecho de que «exista un cierto movimiento de los datos de carácter personal», bastaría con que el emisor colgara los datos permitiendo que el receptor accediera a ellos.

27. Además, en aras a la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita, el concepto de «transferencia internacional de datos de carácter personal» se debería ampliar y comprender en el sentido de «movimiento internacional de datos», acogiendo los supuestos de lo que podríamos llamar acceso *internacional* a los datos de carácter personal; de esta forma, deberíamos calificar como por transferencia internacional de datos «todo movimiento de datos de carácter personal, provisional o definitiva, sin importar el soporte en que se encuentren los mismos, los medios utilizados ni el tipo de tratamiento que reciban, a una persona ubicada fuera del territorio español, así como el acceso a los datos por parte de una persona ubicada fuera del territorio español».

II. SUJETOS DE UNA TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL

28. Analizada desde una perspectiva objetiva, qué es una «transferencia internacional de datos» y cuál es su importancia socioeconómica, ahora vamos a determinar, desde una perspectiva subjetiva, quiénes

---

tercer Estado estarán siendo objeto de una transferencia internacional de datos personales. *Vid.* Juan ZABÍA DE LA MATA, (Coord.), *Protección...*, p. 582.

participan en una transferencia internacional de datos, para comprobar si alguno de los sujetos intervinientes se encuentra o no en una situación de desprotección: el titular de los datos, el exportador y el importador de los datos objeto de una transferencia internacional.

En primer lugar, como sujeto relevante en una transferencia internacional de datos de carácter personal contamos *con la **persona física titular de los datos que son objeto de una transferencia internacional de datos de carácter personal ilícita.***[42] Nos referimos al del titular del derecho fundamental a la protección de datos. Éste es uno de los derechos fundamentales que se explicitan con mayor amplitud y que aparece deslindado, con claridad meridiana, de otros como el respeto de la vida privada y familiar (art. 7),[43] en el art. 8,[44] de la Carta de los

---

[42] Se trata de un elemento subjetivo presente siempre, ya sea un tratamiento de datos doméstico o una transferencia internacional de datos, es el afectado. *Vid.* Art. 5.1.a del RLOPD.

[43] El artículo 7 señala que «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones». Los derechos garantizados en el artículo 7 corresponden a los que garantiza el artículo 8 del CEDH. A fin de tener en cuenta la evolución técnica, se ha sustituido la palabra correspondencia por la de «comunicaciones». De conformidad con lo dispuesto en el apartado 3 del artículo 52, este derecho tiene el mismo sentido y alcance que el artículo correspondiente del CEDH.

[44] El artículo 8 señala que «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente». Este artículo se basa en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE, así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El de-

Derechos Fundamentales de la Unión Europea.[45] Así, la privacidad ha entrado en la categoría de los derechos humanos en la medida que garantiza libertades ulteriores como la de obtener trabajo, un crédito o de optar o acceder a determinados servicios: en definitiva, devuelve al individuo (persona física)[46] el control sobre su entorno y garantiza la sostenibilidad del desarrollo.[47]

En segundo lugar, debemos referirnos ***al exportador (o promotor) de datos:*** persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una transferencia de datos de carácter personal a un país tercero.[48]

En tercer lugar, se encuentra el ***importador (o receptor) de datos:*** persona física o jurídica, pública o privada, u órgano administrativo

---

recho a la protección de los datos de carácter personal se ejerce en las condiciones establecidas por la Directiva antes mencionada y puede limitarse en las condiciones establecidas por el artículo 52 de la Carta. *Vid.* M.ª Carmen GUERRERO PICÓ, *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 101-108; y, José MARTÍN Y PÉREZ DE NANCLARES, «Comentario al artículo 8. Protección de Datos de Carácter Personal», en *Carta de los Derechos Fundamentales de la Unión Europea*, Fundación BBVA, Madrid, 2008, pp. 223-243.

45 *DOUE* C 303, de 14 de diciembre de 2007, y C 83, de 30 de marzo de 2010.

46 Sin embargo, en determinados supuestos también las personas jurídicas, en tanto que destinatarias de las normas en materia de protección de datos, podrían ser titulares del derecho a la protección de datos. *Vid.* en el mismo sentido, José MARTÍN Y PÉREZ DE NANCLARES, «Comentario..., *op. cit.*, pp. 231-232.

47 Ya la STC 292/2000, de 30 de noviembre, indicaba el objeto y contenido propios del derecho fundamental a la privacidad –derecho fundamental que como tal es inherente a la persona e indisponible–. Protege un conjunto de datos de carácter personal, no necesariamente íntimos o incluso públicos, que, por su capacidad de ser tratados por medios informáticos, arrojan un perfil de la persona, y cuyo uso puede lesionar los derechos de los ciudadanos.

48 *Vid.* Art. 5.1.j del RLOPD.

receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.[49]

Cuando hablamos de ***exportador e importador*** de una transferencia internacional de datos de carácter personal nos estamos refiriendo al responsable y al encargado en el marco de tal transferencia. Se precisa con ello un poco más y «simplemente se crea un subconcepto para referirse con mayor precisión al empresario responsable establecido en la UE que promueve una transferencia internacional a un tercer Estado (que se denomina 'exportador'), dirigida a un empresario receptor establecido en ese lugar (que denominamos 'importador'), con independencia de que este último vaya a actuar como responsable o un encargado».[50]

Uno y otro (**exportador e importador de datos**) son empresarios que en su establecimiento y en nombre propio recogen, procesan y tratan datos personales que mantienen en ficheros de datos a los efectos de darles un determinado uso y con un objetivo claro: promover una transferencia internacional de datos de carácter personal.

29. Resulta esencial a los efectos de este estudio identificar y presentar a los diferentes protagonistas de una transferencia internacional de datos si un tratamiento de datos responde a la relación entre el responsable del fichero de datos (persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento),[51] y el encargado de su tratamiento (persona física o jurídica, pública o privada, u ór-

---

49 *Vid.* Art. 5.1.ñ del RLOPD.

50 Diana SANCHO VILLA, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010, p. 27.

51 Art. 3.d de la LOPD.

gano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio).[52]

30. En conclusión, es evidente la situación de desprotección del titular del derecho a la protección de datos ante un tratamiento ilícito internacional de sus datos frente al exportador y al importador de datos porque cuenta con desiguales armas frente a ellos.

III. TIPOLOGÍA DE TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

31. Una vez deslindado el objeto de estudio e identificados los sujetos participantes en una transferencia internacional de datos de carácter personal, debemos ocuparnos de los diferentes criterios que existen para clasificar las transferencias internacionales de datos; de forma que podamos, en última instancia, establecer el supuesto tipo a examinar: las transferencias internacionales de datos de carácter personal extracontractuales.

Si bien algunos autores clasifican las transferencias internacionales de datos sobre la base de tan sólo un criterio diferenciador: el de los sujetos que realizan la transferencia,[53] a nuestro modo de ver, con el

---

52 Art. 5.1.i del RLOPD.

53 Sancho Villa distingue entre «transferencias internacionales entre responsables del tratamiento» y «transferencia internacional a un encargado del tratamiento». *Vid.* Diana SANCHO VILLA, *Transferencia internacional de datos personales*, Agen-

fin de ahondar en la idea de la desprotección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita, debemos manejar no sólo éste sino también otros criterios diferenciadores: a) ***el del país de destino;*** b) ***el del objeto;*** c) ***el de los sujetos intervinientes;*** d) ***el de la finalidad con que se realiza la transferencia internacional de datos de carácter personal.*** Veamos cada una de estos tipos de transferencias internacionales de datos de carácter personal:

a) ***Atendiendo al criterio del país de destino de la transferencia internacional de datos***, ésta puede tener lugar *1)* hacia Estados miembros de la UE o *2)* hacia terceros Estados; dentro de estas últimas, hacia Estados que garantizan un «nivel de protección adecuado», hacia Estados que carecen de dicho nivel de protección,[54]

---

cia de Protección de Datos, Madrid, 2003, pp. 47-52; Del Peso Navarro y Ramos González, sobre la base de la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos, distingue entre: *1)* «transferencias al territorio de Estados que otorguen un nivel adecuado de protección» (norma cuarta); y, *2)* «transferencias al territorio de otros Estados no declarados de nivel adecuado» (norma quinta). *Vid.* Emilio DEL PESO NAVARRO, y Miguel Ángel RAMOS GONZÁLEZ, *La seguridad de los datos de carácter personal*, 2.ª ed., Díaz de Santos, Madrid, 2002, pp. 112-117; Davara Rodríguez se centra en el país de destino y en la finalidad con que se realiza la transferencia internacional de datos. *Vid.* Miguel Ángel DAVARA RODRÍGUEZ, «La Transferencia Internacional..., *op. cit.*, pp. 27-28; y, De Miguel Asensio la hace en función de si el desplazamiento de datos se realiza a países que proporcionan o no un nivel adecuado de protección. *Vid.* Pedro A. DE MIGUEL ASENSIO, Nota a la «Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal», en *Anuario de Derecho internacional Privado (2001)*, T l, Iprolex, Madrid, 2001, pp. 626-627.

54 Similar clasificación presenta la Instrucción 1/2000, cuando distingue entre *a)* «transferencias al territorio de Estados que otorguen un nivel adecuado de protección» (Norma cuarta) y *b)* «transferencias de datos al territorio de otros Esta-

o, en su caso, hacia Estados que carezcan de legislación de protección de datos.[55,56]

– ***Las transferencias a Estados miembros de la UE*** quedan bajo el paraguas de la Directiva 95/46/CE. El régimen de transferencia internacional de datos pivota sobre el concepto de «nivel de protección adecuado», que se presume tienen los Estados miembros de la UE. De esta forma, serán las autoridades de los Estados miembros quienes «evaluarán, en relación con la transferencia o categoría o clase de transferencias, si un tercer Estado ofrece o no un nivel de protección adecuado sobre la ba-

---

dos» (Norma quinta); y, el RLOPD cuando se refiere a «transferencias a Estados que proporcionen un nivel adecuado de protección» (Tít. VI; Cap. II; arts. 67 a 69) y a «transferencias a Estados que no proporcionen un nivel adecuado de protección» (Tít. VI; Cap. III; art. 70). Por su parte, en relación con la transferencia internacional de datos relativos a la salud, Heredero Higueras, se refiere a «transferencias intracomunitarias« –dentro del marco de la UE– y a «transferencias extracomunitarias» –de un país tercero a otro o de un país tercero a un Estado miembro de la UE–. *Vid.* Manuel HEREDERO HIGUERAS, «La transmisión internacional de los datos de la salud», en Santiago RIPOLL CARULLA (Ed.), Jordi BACARIA MARTRUS (Coord.) y otros, *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Agencia Catalana de Protección de Datos, Marcial Pons, Madrid, 2006, pp. 195-211.

55 Como bien señala Velázquez Bautista, «La transmisión de datos tendría lugar entre dos territorios con una situación legal equivalente, por lo que en ninguno de los Estados supondría un problema jurídico la transmisión de datos». *Vid.* Rafael VELÁZQUEZ BAUTISTA, *Protección jurídica de datos personales automatizados*, Colex, Madrid, 1993, p. 184.

56 *Vid.* Documento de trabajo WP12, de 24 de julio de 1998, del Grupo de Trabajo del artículo 29, y que lleva por título Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE.

se de los criterios que enumera el apartado 2 [del art. 25 de la Directiva 95/46/CE] al efecto».[57]

– ***Las transferencias a terceros Estados que garantizan un «nivel de protección adecuado»,*** cuya adecuación haya sido declarada por la Comisión Europea. Sobre la base de lo previsto en el Considerando 66.º de la Directiva 95/46/CE,[58] se habilita a la Comisión, en los apartados 4 a 6 del artículo 25 de la citada Directiva 95/46/CE, para que evalúe si un tercer Estado garantiza dicho «nivel de protección adecuado», obligando a los Estados miembros, si no es el caso, a adoptar «las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate».[59]

Hasta la fecha, sólo se consideraran adecuados los regímenes de los Estados miembros del EEE[60] y los afectados por las Decisiones de la Comisión Europea, que consideraron adecuado

---

57 Manuel HEREDERO HIGUERAS, *La directiva...*, *op. cit.*, p. 188.

58 Al señalar que «por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CE del Consejo».

59 Como bien señala Heredero Higueras, «este es el único contexto para el que la Directiva ha previsto una habilitación del Consejo a favor de la Comisión en materia de ejecución». *Vid.* Manuel HEREDERO HIGUERAS, *La directiva...*, *op. cit.*, p. 188.

60 El EEE se constituyó por un Acuerdo firmado el 2 de mayo de 1992 (y que entró en vigor el uno de de enero de 1994) entre los Estados miembros de la UE y los seis países que formaban la Asociación Europea de Libre Comercio (AELC), excepto Suiza. Después de la entrada en la UE de tres Estados de la AELC: Austria, Finlandia y Suecia, a comienzos de 1995, e Islandia, Noruega y Liechtenstein, pueden disfrutar de los beneficios del mercado único gracias al Acuerdo de constitución del EEE.

el nivel de protección de datos personales en Suiza y Hungría[61] (aunque la Decisión por la que se declaraba a Hungría como un país con un nivel de protección adecuado carece de fundamento, pues desde el 1 de mayo de 2004 es un Estado miembro de la UE), los EE.UU.,[62] Canadá,[63] Argentina,[64] la Bailía Guernesey,[65] la Isla de Man,[66] Jersey,[67] Islas Feroe,[68] Andorra,[69] Israel,[70] Uruguay[71] y Nueva Zelanda.[72,73]

---

61 Decisiones de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza y Hungría (*DO* 2000 L 215/1; y, *DO* 2000 L 215/4).

62 Decisión 2000/520/CE 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 conferida por los principios de Puerto Seguro («*Safe Harbour*») para la protección de la vida privada, y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (*DO* 2000 L 215/7). Las entidades con sede en EE.UU. que han certificado su adhesión a los principios de Puerto Seguro aparecen en una lista pública elaborada por el Departamento de Comercio de los EE.UU, (http://www.export.gov/safeHarbor).

63 Decisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *(Personal Information and Electronic Documents Act)* (*DO* 2002 L 2/13).

64 Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (*DO* 2003/490/CE L 168/19).

65 Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernesey (*DO* 2003/821/CE L 308/27).

66 Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man (*DO* 2004/411/CE L 208/47; y corr. de errores en DO L 151, de 30 de abril de 2004).

67 Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey (*DO* L 138/21).

Las Decisiones de la Comisión sobre el nivel adecuado de protección las podemos dividir en dos grupos: *a)* Suiza, Argentina, Guernesey, la Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda, donde la Comisión reconoce el nivel adecuado de protección de toda la normativa del país, lo que conlleva la liberalización de todas las transferencias de datos, sin limitaciones de ninguna clase; y *b)* los EE.UU. y Canadá, donde la Comisión reconoce su nivel de protección adecuada de forma limitada. Mientras que la Decisión referente a

---

68 Decisión 2010/146/CE de la Comisión, de 5 de marzo de 2010, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre tratamiento de datos personales (*DO* C(2010) 1130).

69 Decisión 2010/625/CE de la Comisión, de 19 de octubre de 2010, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra (*DO* 2010/87/UE).

70 Decisión de la Comisión, de 31 de enero de 2011, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales (*DO* 2011/61/UE).

71 Decisión de ejecución de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental de Uruguay en lo que respecta al tratamiento automatizado d datos personales (*DOUE* 2012/484/UE).

72 Decisión de Ejecución de la Comisión, de 19 de diciembre de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda (*DOUE núm.* 28, de 30 de enero de 2013).

73 Las nuevas potencias emergentes como la República Popular de China, la India, Brasil o Rusia quedan fuera de la relación antes citada de países. En estos momentos, la Comisión Europea está considerando países como Australia, Japón, o Quebec.

los EE.UU. reconoce un nivel de protección adecuada sólo a los destinatarios acogidos al sistema de Puerto Seguro, la Decisión que afecta a Canadá reconoce un nivel de protección adecuada sólo a aquellos destinatarios a los que se aplica la ley canadiense de protección de datos *(Personal Information and Electronic Documents Act)*.

– ***Las transferencias a terceros Estados que no garantizan un «nivel de protección adecuado»,*** pero que bien esté amparada en alguna de las excepciones legalmente previstas, o en alguna de las Decisiones de la Comisión Europea referidas a las cláusulas contractuales tipo, bien que medie autorización de la autoridad de protección de datos del país de origen de la transferencia internacional de datos.

El referido Principio de «nivel de protección adecuado» puede ser obviado a tenor de ciertos intereses que deben prevalecer y protegerse. Se trata de intereses jurídicamente protegidos —públicos y privados— que configuran en su haber, y de forma desglosada, una serie de excepciones. Además, existe una excepción al tal Principio que no alude a la defensa de otros intereses jurídicamente protegidos, sino a la presentación de «garantías suficientes» por el responsable del tratamiento de datos de carácter personal. En este último caso, lo que subyace con la flexibilización de las normas de protección de datos aplicables es la necesidad de eliminar los obstáculos en las relaciones comerciales internacionales existentes entre los Estados miembros de la UE y entre estos y terceros Estados.[74]

[74] Una vez que se haya efectuado la evaluación del nivel de protección adecuado del país destinatario de la transferencia de datos de carácter personal se deberá

Señala la normativa española que no se permiten transferencias de datos «a países que no proporcionen un nivel de protección equiparable al que ofrece la LOPD» («nivel de protección adecuado»), salvo que el transmitente cumpla lo previsto en la LOPD y el Director de la AEPD autorice la transmisión si se obtienen las garantías adecuadas; así, en el artículo 34 de la LOPD —en línea con el artículo 26 de la Directiva 95/46/CE— se recogen toda una serie de excepciones[75] en esta materia, que operan cuando no existe en el Estado de destino de la transferencia el «nivel de protección adecuado», a saber:

«*a)* Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

emitir una declaración de que efectivamente existe esa situación. Los instrumentos por los que se puede materializar dicha declaración del nivel de protección adecuado son variados y corresponden a distinta naturaleza: *a)* actos de carácter público —ya sean internacionales (p. ej. las Directrices de la OCDE, de la ONU o del Convenio 108/81/CE), comunitarios (p. ej. las Decisiones de la Comisión Europea) y/o estatales (p. ej. las Autorizaciones emitidas por el Director de la AEPD)—; y *b)* actos de carácter privado (p. ej. a través de los contratos-tipo o de las normas empresariales vinculantes).

75 Con la articulación de estas excepciones a la regla general prevista en el art. 33 de la LOPD el legislador español, claramente influido por la Directiva 95/46/CE, pretende establecer un marco comunitario que posibilite el comercio electrónico y el reconocimiento de la firma digital en la UE. *Vid.* José M.ª Álvarez-Cienfuegos Suárez, «Notas a la nueva regulación de la protección de datos de carácter personal», en *La Ley*, núm. 5036, 17 de abril de 2000, p. 1716.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.[76]

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.[77]

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.[78]

f) Cuando la transferencia sea necesaria para la ejecución da un contrato[79] entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.[80]

---

[76] A nuestro modo de ver, es un error gravísimo que el legislador haya incluido entre las excepciones del artículo 34 de la LOPD los datos relativos a la salud, esto es, una categoría de datos sensibles, tal y como establece el artículo 7 de la LOPD. Es más, se trata de un doble error: por un lado, obviar la naturaleza sensible de estos datos; y, por otro lado, eludir el control del Director de la AEPD. *Vid.*, en el mismo sentido, Miguel VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001, pp. 377-378. En el mismo contexto es, en nuestra opinión, una clara omisión legal y un error muy grave el hecho de que en la Ley 14/2007 de Investigación Biomédica no se haga mención alguna acerca de la transferencia de datos genéticos. No olvidemos que los datos genéticos son datos personales y sensibles y han de ser protegidos. Aunque la Ley permite que una muestra salga del territorio español y sea objeto de transferencia internacional, para que llegue a determinados Estados que no tienen un nivel de protección adecuado será necesaria la autorización del Director de la AEPD o que concurra una circunstancia excepcional: el consentimiento informado, expreso y por escrito del sujeto que se somete a investigación biomédica o que la transferencia de la muestra sea necesaria para prever la salud del sujeto al que se refiere.

[77] Excepción heredada de la LORTAD.

[78] Evidentemente, puesta esta excepción en conexión con su referente: los artículos 3.h y 11 de la LOPD; así, el consentimiento del afectado debería ser previo, libre, específico e informado.

[79] Como señala De Miguel Asensio, «La solución contractual [...] parece resultar un instrumento apropiado básicamente en situaciones de intercambio estable y continuado de datos, habida cuenta del coste (de negociación y redacción) asociado a esta solución [...] que en particular tiende a hacerla poco apropiada en supues-

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.[81]

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.[82] [...]

---

tos en los que entre emisor y receptor de los datos existe una transferencia internacional aislada». Pedro DE MIGUEL ASENSIO, *Derecho privado de Internet*, 4.ª ed., Civitas, Cizur Menor (Navarra), 2011, p. 568.

80 Como señala Herrán Ortiz, «la idea es resolver, caso por caso, por vía de contratos o convenios entre responsables de los tratamientos de los Estados de origen y de destino, tiene su antecedente en las prácticas y usos alemanes en materia de transferencia de datos sensibles con fines de evaluación de la solvencia y fue recogida y desarrollada en forma de Recomendación por el Consejo de Europa». Ana Isabel HERRÁN ORTIZ, *El derecho a la protección de datos personales en la sociedad de la información*, Cuadernos Deusto de derechos Humanos, Universidad de Deusto, Bilbao, 2003, p. 181.

81 En palabras de Garriga Domínguez, «el ejemplo más típico sería la reserva de una habitación de hotel en un país tercero. En este caso será necesario que el responsable del tratamiento, por ejemplo una agencia de viajes que actúa de intermediaria, ceda al hotel situado en el territorio de un país extranjero, no comunitario, los datos personales necesarios del interesado para formalizar la reserva o, por ejemplo para el alquiler de un coche o cualquier otro bien o servicio». Ana GARRIGA DOMÍNGUEZ, *La protección de los datos personales en el Derecho español*, Dykinson, Madrid, 1999, p. 332. Ahora bien, nos encontramos ante una excepción que plantea en la práctica algunos interrogantes: ¿quién debe valorar la existencia del interés del afectado?, si el afectado tuviera limitada su capacidad de obrar, ¿quién debe velar por su interés? *Vid.* Miguel VIZCAÍNO CALDERÓN, *Comentarios...*, *op. cit.,* p. 380.

82 Acorde con el propio artículo 34 de la LOPD —y con el Considerando 58 de la Directiva 95/46/CE— «tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias». Sin embargo, hablar de «interés público» es enfrentarse a un concepto jurídico indeterminado, por lo que, como señalan Herrán Ortiz y Heredero Higueras, «hubiera sido deseable concretar este concepto jurídico indeterminado mediante una lista o relación de supuestos de intereses o necesidades públicas en concreto, que prevalecieran sobre el interés del afectado, en que sus datos no sean

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.[83]

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las

---

transmitidos a un país tercero sin protección adecuada». Ana Isabel HERRÁN ORTIZ, *El derecho...*, *op. cit.*, p. 181; y Manuel HEREDERO HIGUERAS, *La directiva comunitaria de protección de los datos de carácter personal: Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos*, Aranzadi, Pamplona, 1997, p. 191. Se trata de una excepción cuya redacción deja mucho que desear, prestándose a todo tipo de comentarios; así, señala Vizcaíno Calderón, que la norma «es tan amplia que prácticamente resiste a cualquier tipo de limitaciones. Si por lo menos, se hubiera limitado a la habilitación legal, sería posible concretar el supuesto a la vista de la concreta previsión legal que en cada caso se aplicare. Ahora bien, la referencia a la necesidad para la protección del mencionado interés público destruye racionalmente cualquier posibilidad de concretar el supuesto. Tampoco nos dice la norma a quién compete la apreciación del citado interés público». Parece que ante cualquier petición por una Administración fiscal o aduanera de un país tercero se debe proceder a la transferencia de datos; pues no es así, ya que se hace necesaria la oportuna justificación, y el control de la propia AEPD. *Vid.*, en el mismo sentido, Miguel VIZCAÍNO CALDERÓN, *Comentarios...*, *op. cit.*, pp. 381-382.

83 Se trata de una excepción inspirada en el artículo 26.1.f de la Directiva 95/46/CE, que se incluyó «para dar satisfacción a la preocupación manifestada por la delegación alemana en su nota sobre las repercusiones que la Directiva pudiera tener en el régimen de los registros públicos (Registro inmobiliario, Registro Mercantil, Registro de buques, etc.)». Doc. 4848/94, ECO 21. *Vid.* Manuel HEREDERO HIGUERAS, *La directiva...*, *op. cit.*, p. 192. No obstante, el Considerando 58 de la Directiva 95/46/CE matiza la excepción al señalar «[...] cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo».

> Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado».[84]

b) Atendiendo a su objeto, los criterios a manejar son la modalidad del fichero y la titularidad del mismo. Así, por un lado, en base a la modalidad de fichero de datos personales, existen las transferencias cuyo objeto sean ficheros no automatizados (todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica)[85] o automatizados (todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados),[86] y, por otro, atendiendo a la titularidad del fichero de datos personales, podemos diferenciar aquéllas referidas a ficheros de titularidad pública (ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el

---

84 *Vid.*, en el mismo sentido, el artículo 68 del RLOPD.

85 *Vid.* art. 5.1.n del RLOPD.

86 Están claramente incluidos dentro de este concepto los ficheros de datos personales que almacenan la información en soportes informáticos (bases de datos, archivos, carpetas, etc.) y que se encuentran organizados de manera que se pueda acceder a los datos personales utilizando cualquier tipo de aplicación o procedimiento informatizado.

ejercicio de potestades de derecho público)[87] de aquellas de titularidad privada (ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica).[88]

c) ***Atendiendo a los sujetos intervinientes***, es posible distinguir entre el «exportador o transmitente» de los datos de carácter personal (persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero)[89] y el «importador o destinatario» de los mismos (persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero).[90] Existen también transferencias internacionales entre responsables del tratamiento de datos personales[91] o entre responsable y encargado

---

87 *Vid.* art. 5.1.m del RLOPD.

88 *Vid.* art. 5.1.l del RLOPD.

89 *Vid.* art. 5.1.j del RLOPD.

90 *Vid.* art. 5.1.ñ del RLOPD.

91 El responsable originario del tratamiento de los datos de carácter personal, que tiene la categoría de transmitente de los datos, transfiere dichos datos a otra persona independiente de ésta, que tendrá la categoría de destinatario de los datos y que se encuentra ubicado en un Estado distinto, para que efectúe un tra-

del tratamiento de datos personales,[92] aunque la cesión se realice entre empresas de un mismo grupo,[93] Además, la LOPD se refiere en su artículo 5.1 a los supuestos en los que el responsable del tratamiento no esté establecido en territorio de la UE y utilice para el tratamiento medios situados en el territorio español, en cuyo caso se le exigirá la designación de un responsable en España.[94]

d) ***Atendiendo a la finalidad o marco jurídico en el que se realizan***, las transferencias internacionales pueden ser *contractuales* (transmisiones internacionales como consecuencia de relaciones contractuales y comerciales entre empresas con vinculación jurídica o el flujo que se mantiene con fines comerciales), cuando existe un acuerdo previo entre exportador e importador de los datos de ca-

---

tamiento de los datos de carácter personal por su propia cuenta, convirtiéndose, a su vez, en responsable del tratamiento que le dé a esos datos de carácter personal.

92 Es decir, el tratamiento de datos de carácter personal que realiza una persona por el encargo y a cuenta del responsable del tratamiento que se lo ha encomendado.

93 Se considera «transferencia internacional de datos» aunque la cesión se realice entre empresas españolas que, una ubicada en España y otra/s en el extranjero, pero formando parte de un grupo empresarial multinacional y con ocasión de procesos de reorganización en los mismos en el ámbito internacional, pretenden efectuar transferencias de datos que en ocasiones obedecen a la centralización de procesos de gestión y en otras a simples supuestos de utilización compartida de recursos por filiales de distintos países, al hilo de las posibilidades brindadas por las nuevas tecnologías, al tratarse de entidades jurídicas diferentes y, por tanto, de responsables de ficheros de datos diferentes.

94 *Vid.* José M.ª Álvarez-Cienfuegos Suárez, «Notas a la nueva regulación de la protección de datos de carácter personal», en *La Ley*, núm. 5036, 17 de abril de 2000, p. 1711.

rácter personal o *no contractuales* (realización de un tratamiento ilícito de datos),[95] cuando no existe tal acuerdo.

32. De entre todos los criterios enunciados, a los efectos del Derecho internacional privado el que nos interesa en este trabajo (la desprotección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita) es el de la finalidad o marco jurídico en el que se realiza la transferencia, lo que nos permite distinguir entre ***transferencias internacionales de datos contractuales*** (consensuales) y ***extracontractuales*** (no consensuales):

– Las primeras (transferencias internacionales de datos «contractuales») se refieren a aquellos ***negocios internacionales de tratamiento de datos entre el afectado y el responsable.*** Es frecuente que la celebración o ejecución de un determinado acuerdo entre un sujeto y un empresario (o entre éste y un tercero en interés de aquél) necesite de un tratamiento de sus datos personales. En estos casos, la transferencia internacional de tales datos tiene un carácter accesorio respecto del negocio principal.[96] En otras ocasio-

[95] Consecuentemente, existirá daño –y, por tanto, reclamación– si se verifica que se ha producido un tratamiento ilícito de datos de carácter personal.

[96] Tal sería el caso, por ejemplo, de la reserva de un billete de avión en una agencia de viajes para la ejecución de un contrato de transporte entre el pasajero y la compañía aérea (que supone el envío de los datos personales del cliente por parte de la agencia a la central de tratamiento en el extranjero), en el marco de un contrato de tarjeta de crédito (pago de las facturas o de las devoluciones de efectivo a los suministradores de bienes y servicios por parte de la entidad emisora), o del supuesto en el que la persona física contrata con una empresa especializada un servicio que implica necesariamente la elaboración de un perfil de solvencia.

nes, la transferencia internacional de datos se desarrolla en el marco de un negocio cuyo objeto principal es precisamente esa transmisión: son transmisiones de datos que se producen con carácter principal.[97]

– Junto a estos supuestos, son frecuentes los ***casos de vulneración del derecho a la protección de datos de afectados por un tratamiento ilícito de datos realizado por un empresario al margen de una relación preexistente entre las partes*** (transferencias internacionales de datos «extracontractuales»), ***donde el afectado*** (perjudicado) ***plantea una reclamación por daños y perjuicios frente al causante del daño*** (persona física o jurídica que ha tratado ilegalmente los datos).[98]

---

[97] Por ejemplo, la transferencia de datos relativos a sus clientes o a sus empleados de la filial española a su sede en otro país, la compraventa de ficheros de datos personales a una empresa establecida en España que se dedica al marketing, por parte de una empresa establecida en el extranjero que quiere dirigir una campaña de publicidad al mercado español, o la contratación de un servicio de administración y gestión de los ficheros de un empresario por cuenta de un tercero y en nombre de aquél.

[98] Así, p. ej., si un ciudadano portugués reserva un billete en una agencia de viajes de Lisboa para volar con una compañía aérea con sede en España y los datos recabados incluyen información sobre la discapacidad del ciudadano y sobre el hecho de que utiliza una silla de ruedas. Los datos se introducen en un sistema informático internacional de reservas y, desde allí, la compañía aérea los descarga en su base de datos sobre pasajeros, ubicada en España, donde los conserva indefinidamente porque decide utilizar los datos para prestar un mejor servicio al pasajero en caso de que viaje con ellos en el futuro, así como para la planificación de su gestión interna. Imaginemos otro supuesto en el que una empresa de los Países Bajos está especializada en la elaboración de listas de direcciones y, empleando muchas fuentes distintas de información pública disponibles en los Países Bajos, junto con listas de clientes alquiladas a otras empresas holandesas, las listas resultantes pretenden incluir a personas que se ajusten a un perfil socioeconómico concreto. Tiempo después, la empresa vende estas listas a clientes

Así las cosas, nuestro objeto de estudio se centra en las reclamaciones que tienen fundamento extracontractual, las cuales suelen concluir con una pretensión de satisfacción económica. Por ello se prescinde del análisis de otro tipo de situaciones relacionadas con el flujo transfronterizo de datos personales tales como las que traen su causa de relaciones contractuales entre perjudicado e infractor.

IV. SUPUESTO TIPO

33. El estudio de campo, el análisis objetivo, subjetivo y taxonómico realizado en los apartados (I), (II) y (III) nos conduce a un supuesto tipo, no analizado y relevante: las dificultades que encuentra una persona, cuyos datos de carácter personal han sido objeto de un tratamiento ilícito, para obtener una justa reparación cuando ese tratamiento tiene lugar en el marco de una transferencia internacional de datos. Pues bien, son frecuentes los casos de vulneración del derecho a la protección de datos de carácter personal por un tratamiento ilícito internacional de datos realizados al margen de una relación preexistente entre las partes (transferencias internacionales de datos «extracontractuales»). Veamos algunos ejemplos prácticos:

A) Un ciudadano portugués (**afectado**) reserva un billete en una agencia de viajes de Lisboa para volar con una compañía aérea con sede en España (**exportador de datos**). Los datos recabados inclu-

no sólo de los Países Bajos y de la UE sino también de muchos otros países y las empresas clientes receptoras utilizan las listas (que incluyen direcciones postales de correo electrónico, números de teléfono y, a menudo, direcciones de correo electrónico) para entrar en contacto con las personas relacionadas con vistas a vender una desconcertante o no selección de diferentes productos y servicios.

yen información sobre la discapacidad del ciudadano y sobre el hecho de que utiliza una silla de ruedas. Los datos se introducen en un sistema informático internacional de reservas y, desde España, la compañía aérea los descarga en su base de datos sobre pasajeros, ubicada en Reino Unido (**importador de datos**), donde se conservan indefinidamente. La compañía aérea decide utilizar esos datos para prestar un mejor servicio al pasajero en caso de que viaje con ellos en el futuro, así como para la planificación de la gestión interna.

B) Una empresa de los Países Bajos está especializada en la elaboración de listas de direcciones. Empleando muchas fuentes distintas de información pública disponibles en los Países Bajos, junto con listas de clientes adquiridas a otras empresas holandesas, las listas resultantes pretenden incluir a personas que se ajusten a un perfil socioeconómico concreto (**afectado**). Después, la empresa holandesa (**exportador de datos**) vende estas listas a clientes no sólo de los Países Bajos y de la UE, sino también de muchos otros países (**importador de datos**). Las empresas clientes receptoras utilizan las listas (que incluyen direcciones postales de correo electrónico, números de teléfono y, a menudo, direcciones de correo electrónico) para entrar en contacto con las personas relacionadas con vistas a vender diferentes productos y servicios.

C) La transferencia internacional de datos de carácter personal de sus empleados (**afectado**) desde una empresa establecida en España (**exportador de datos**) a otra establecida en Rusia (**importador de datos**) sin contar con la autorización correspondiente del titular de dichos datos.

34. Como vemos, nos referimos a aquellos supuestos en los que, como consecuencia de una transferencia internacional ilícita, se produce una

vulneración del derecho a la protección de datos de carácter personal y, por ende, el perjudicado[99] no le queda más remedio que, para resarcirse del daño causado, plantear una reclamación por daños y perjuicios frente a aquel que ha tratado ilícitamente sus datos.

El objeto de estudio está definido, deslindado y perfilado Ahora, en el **capítulo II** pasamos al estudio de las normas que se proyectan sobre el supuesto tipo. La comprobación de tal estado de cosas se iniciará con un análisis de las reglas y mecanismos existentes en los distintos niveles de producción normativa: superestructura jurídica internacional, plataformas de integración regional, respuestas autónomas estatales, e iniciativas propias del llamado «espacio transnacional». Análisis que revelará una situación que dista mucho de ser satisfactoria y que concluirá demostrando que la normativa de Derecho internacional privado es, de lejos, la más sencilla y manifiestamente mejorable.

99 Evidentemente el perjudicado, titular del derecho fundamental a la protección de datos de carácter personal, podrá también ejercitar los derechos Arco (Acceso —art. 15 de la LOPD—, Rectificación y Cancelación —art. 16 de la LOPD— y Oposición —arts. 35 y 36 del RLOPD—), así como el «derecho al olvido» (*Vid.* STJUE (Gran Sala) de 13 de mayo de 2014. Asunto C-131/12, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, recibido en el Tribunal de Justicia el 9 de marzo de 2012, en el procedimiento entre Google Spain, SL, Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González) con el fin de garantizarse un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo los mencionados deberes de hacer.

Capítulo II.

La desprotección del titular del derecho a la protección de datos de carácter personal en los distintos centros de producción normativa

35. Una vez definido, deslindado y perfilado el objeto de estudio en el capítulo anterior, ahora, en este **capítulo II**, vamos a estudiar las normas que se proyectan sobre el supuesto tipo. Se analizarán los diferentes mecanismos de protección a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, para obtener una tutela adecuada, equilibrada y efectiva en los distintos centros de producción normativa: superestructura jurídica internacional (I), sistemas de integración regional (II) espacio transnacional (III). Análisis que revelará una situación que dista mucho de ser satisfactoria y que concluirá demostrando que el Derecho internacional privado es, claramente, la posibilidad más plausible para que el perjudicado obtenga una satisfacción a sus legítimos intereses (IV).

1. SUPERESTRUCTURA JURÍDICA INTERNACIONAL

36. A partir del Acuerdo General sobre Aranceles Aduaneros y Comercio de la OMC[100] es innegable la tendencia creciente a la institucionalización en la regulación de los intercambios comerciales internacionales. Eso da como resultado la creación de instituciones internacionales de cooperación de muy distinto signo.

El presente apartado tiene por objeto ***identificar las iniciativas normativas provenientes de aquellas instituciones internacionales que se han ocupado de la protección de datos personales de los particulares***, con el fin de determinar si les ofrecen una tutela adecuada, equilibrada y efectiva en caso de tratamiento ilícito internacional de sus datos personales. En particular, nos vamos a detener en las siguientes instituciones: *1)* **la ONU**; *2)* **la OCDE**; y *3)* **la Conferencia Internacional de Autoridades de Protección y Privacidad**; en la medida en que otras instituciones internacionales como la OMC[101] o la

[100] El Acuerdo sobre la OMC incluye el *Acuerdo General sobre Aranceles Aduaneros y Comercio de 1994* («GATT de 1994»), que se basa en el texto del *Acuerdo General sobre Aranceles Aduaneros y Comercio* original, denominado «GATT de 1947».

[101] El estado actual de los acuerdos adoptados en el seno de la OMC sobre protección de datos personales es todavía muy embrionario. Aunque, con motivo de la Tercera Conferencia Interministerial celebrada en Seattle, en noviembre de 1999, los distintos comités de trabajo elaboraron una serie de informes, donde se llegaba a la conclusión de que la inmensa mayoría de las transacciones realizadas a través de Internet son servicios abarcados por el Acuerdo General sobre Comercio de Servicios, con lo que puede concluirse la extensión de las normas del GATT a las actividades de comercio electrónico. El objetivo, hoy día, es alcanzar un acuerdo sobre los principios básicos que permita la libre circulación de datos personales en el comercio electrónico mundial mientras se respeta el derecho a la privacidad de los individuos y se asegure, por tanto, un marco electrónico seguro.

OIT,[102] a pesar de que su ámbito de competencia y las necesidades de sus objetivos requerirían actuar en este ámbito, a día de hoy, no lo han hecho.

1. Organización de las Naciones Unidas[103]

37. A pesar de que el derecho a la intimidad puede ser concebido de forma distinta dependiendo del entorno cultural en el que nos encontremos, no podemos ignorar la existencia de un denominador común en todas las legislaciones y ordenamientos jurídicos: el hecho de entenderla como el «respeto a la protección personal y familiar» de todo individuo. Buena prueba de ello es el reconocimiento que de la misma hacen los textos internacionales, como la *Declaración Universal de los Derechos Humanos* de 1948[104] o el *Pacto Internacional de Derechos*

---

[102] Debemos reseñar sólo un hito jurídico: en la 264.ª Reunión de expertos sobre la *protección de la vida privada de los trabajadores* de la OIT, celebrada en Ginebra, del 1 al 7 de octubre de 1996, se examinó un proyecto de repertorio de recomendaciones prácticas sobre la «protección de los datos personales de los trabajadores» (documento MEWP/1995/1). Los presupuestos, que se tienen en cuenta para la realización del referido documento fueron los siguientes: *a)* Utilización de técnicas informáticas de recuperación de datos; *b)* Los sistemas automatizados de información del personal; *c)* La vigilancia electrónica; y *d)* Los exámenes genéticos y toxicológicos.

[103] La ONU es la mayor organización internacional existente. Se define como una asociación de gobierno global que facilita la cooperación en asuntos como el Derecho internacional, la paz y seguridad internacional, el desarrollo económico y social, los asuntos humanitarios y los derechos humanos. Cuenta con 193 Estados miembros, prácticamente todos los países soberanos reconocidos internacionalmente, más tres miembros en calidad de observadores: la Ciudad del Vaticano, la Orden Soberana y Militar de Malta y el Estado de Palestina.

[104] Adoptada y proclamada por la Resolución de la Asamblea General 217 A (iii) del 10 de diciembre de 1948. Su contenido puede consultarse en:

Civiles y Políticos de 1966,[105] que sitúan siempre su protección en la esfera de la vida privada.

Si bien es cierto que ese concepto ha sido válido y útil durante muchos años, no podemos ignorar que en algunos ámbitos, como el que nos ocupa, la realidad social va por delante de las normas. Debido al continuo avance de la técnica y la informática ha sido necesario dotar de una cierta autonomía al derecho a la protección de datos personales. Y es que, aunque los instrumentos tradicionales le han dispensado una cierta protección bajo el amparo del derecho a la intimidad, la naturaleza y especificidad de los derechos perjudicados demanda una mejor (y mayor) cobertura. A esta demanda han respondido el conjunto de directrices para la regulación de los archivos de datos personales informatizados, adoptadas por Resolución 45/95, de 14 de diciembre de 1990, de la Asamblea General de Naciones Unidas *(Directrices para la regulación de los archivos de datos personales informatizados)*.[106] En virtud de la misma, los procedimientos para aplicar las normas relativas a los archivos de datos personales informatizados se dejan a iniciativa de cada Estado, con sujeción a una serie de orientaciones, entre las que cabe destacar la relativa a ciertos principios que deberían observarse en las legislaciones nacionales: legalidad y lealtad, de exactitud, de especificación de la finalidad, de accesibilidad.

---

http://www.un.org/spanish/aboutun/hrights.htm.

105 «Pacto de Derechos Políticos de 1966», adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su Resolución 2200 A (XXI), de 16 de diciembre de 1966. Su contenido puede consultarse en: http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm.

106 Adoptada en la 68.ª sesión plenaria. Su contenido puede consultarse en: http://www.un.org/spanish/documents/ga/res/45/list45.htm.

2. Organización para la Cooperación y el Desarrollo Económico[107]

38. La adopción de recomendaciones elaboradas por organizaciones como la OCDE, especialmente en lo relativo a la creación de marcos internacionales que permitan impulsar el respeto al derecho a la protección de datos en el contexto de las transferencias internacionales de datos, supone un positivo avance de cara a lograr este objetivo.

Es de destacar la Recomendación de 23 de septiembre de 1980 del Consejo de la OCDE relativa a las líneas directrices concernientes a la protección de la intimidad y los flujos transfronterizos de datos de carácter personal, que introdujo importantes reformas en sus legislaciones estatales con el fin impedir el almacenamiento ilícito de datos personales y su revelación no autorizada. Esta situación provocó con el tiempo una lógica preocupación por proteger la intimidad de los ciudadanos, lo que dio lugar a un desarrollo asimétrico de normas nacionales y, por consiguiente, un inevitable obstáculo a la libre circulación transfronteriza de datos.

Por esta y otras razones, en el seno de la OCDE se han elaborado todo un conjunto de directrices que armonizan la normativa nacional relativa a la intimidad y tratan de impedir interrupciones en la circulación internacional de datos. Estas directrices son, en buena medida, resultado de los trabajos realizados por el subgrupo de la OCDE de

[107] Fundada en 1961, la OCDE agrupa a 34 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo. En la OCDE, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y colaborar a su desarrollo y al de los países no miembros.

Bancos de Datos en el Sector Público, el cual comenzó a articular soluciones políticas en este sentido, constituyendo, en 1978, un Grupo de Expertos encargado de estudiar esta problemática. Las directrices mencionadas se llevaron a cabo a través de tres instrumentos internacionales: *a)* la Recomendación de 23 de septiembre de 1980 en la se que insta a los Estados miembros a tener en cuenta en su legislación interna; *b)* las «Directrices sobre la protección de la intimidad y los flujos transfronterizos de datos de carácter personal»; y *c)* la Declaración de 11 de abril de 1985 «sobre flujos transfronterizos de datos». Las directrices recogidas en estas declaraciones y recomendaciones representan un consenso sobre principios básicos que en muchos casos se han incorporado a las legislaciones nacionales existentes, sirviendo de fundamento para aquellos países que todavía no disponen de este tipo de regulación. Entre estos principios destacan: el principio de limitación de la recogida de datos, el de calidad de datos, el de especificación del fin, de seguridad, transparencia, participación del individuo y el de responsabilidad. Todos ellos han sido reafirmados, si bien de forma implícita, en posteriores declaraciones e instrumentos internacionales realizados en el marco de la OCDE, como puede deducirse de la Recomendación relativa a las directrices de política criptográfica, adoptada por el Consejo de la OCDE el 2 de marzo de 1997, o la Declaración Ministerial relativa a la protección de la intimidad en las redes globales adoptado por el Grupo de Trabajo sobre Seguridad de la Información e Intimidad en Ottawa el 7 y 9 de octubre de 1998.

3. Conferencia Internacional de Autoridades de Protección y Privacidad[108]

39. Nos referimos a la denominada ***Resolución de Madrid*: *Estándares Internacionales sobre Datos Personales y Privacidad.*** Se trata de la Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales, aprobada en la 31.ª Conferencia internacional de Autoridades de protección de datos y privacidad, celebrada en Madrid, del 4 al 6 de noviembre de 2009.

Señala la *Resolución de Madrid* que debemos apostar por un enfoque común, por el diálogo transatlántico entre la conjunción privacidad-seguridad y optar por el establecimiento de unos estándares comunes; y, más aún en una sociedad como la actual, en la que el desarrollo de las herramientas que proporciona la sociedad de la información y las tecnologías de la información y las telecomunicaciones dan lugar a un marco enteramente globalizado, en el que son comunes los flujos de datos entre los distintos Estados, siendo dichos flujos necesarios para el funcionamiento de la sociedad tal y como es hoy concebida.

Eso sí, hasta tanto se desarrollen estas iniciativas es preciso atender con especial sensibilidad a los flujos internacionales de datos, para

---

[108] Reunión más importante a nivel mundial en los temas relacionados a la privacidad y a la protección de datos personales a la que acuden las Autoridades de Protección de Datos y Privacidad de diferentes países. Su principal objetivo es generar intercambios, compartir conocimientos e impulsar proyectos de normas y regulaciones a ser adoptadas para el trabajo cooperativo entre los Estados, un requisito indispensable con miras a una problemática de alcance global que no reconoce fronteras geográficas.

que se permitan su transferencia desde entornos geográficos con niveles de protección adecuados a otros que carezcan de ellos, garantizándose la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita.

40. La superación de fronteras físicas y temporales requiere, ineludiblemente, de un instrumento normativo común, con el que se logre el mayor consenso internacional posible. No se trata de abandonar los sistemas jurídicos tradicionales, ni la fuerza de las leyes, sino de adaptar el sistema para que su aplicación y control sean lo más inmediato y factible posible. Es, por tanto, una adaptación multirregional y multidisciplinar del Derecho en materia de transferencia internacional de datos.

Es necesaria, pues, cierta coordinación en el ámbito mundial en materia transferencia internacional de datos personales, con el fin último de garantizar la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal.

41. Así las cosas, en mi opinión, ***las iniciativas que emanan de organizaciones intergubernamentales de alcance global estudiadas son claramente insuficientes para garantizar el derecho a la protección de datos de carácter personal.*** Las normas emanadas de estas instancias internacionales o bien no son directamente invocables por los particulares (perjudicados) o bien carecen de una traducción adecuada al plano práctico. El titular del derecho a la protección de datos sigue encontrándose en una evidente situación de inferioridad jurídica, que le sitúa al borde de la desprotección.

II. ESTRUCTURAS DE CARÁCTER REGIONAL

42. A pesar de que las distintas organizaciones internacionales están englobadas bajo una misma rúbrica (estructuras de carácter regional) los niveles de integración son muy distintos.

Una vez abordadas las iniciativas en materia de protección de datos personales provenientes de la superestructura jurídica internacional, en este segundo apartado nos ocuparemos de *analizar* **los distintos intentos normativos de las organizaciones de integración regional que tienen como objetivo la protección del titular del derecho a la protección de datos de carácter personal**; en particular, los provenientes de: **1) la UE; 2) el Consejo de Europa; y 3) la APEC.**

1. Unión Europea[109]

43. La regulación del tratamiento de datos personales en los Estados miembros de la UE se ha caracterizado por el alto grado de homogeneidad entre las normas existentes sobre la materia en cada uno de dichos Estados —consecuencia lógica de la transposición de la Directiva 95/46/CE—. No obstante, no podemos olvidar que cada Estado miembro tiene un margen de maniobra en la materia y que, además, se verá influenciado por diferentes factores políticos, culturales y so-

[109] La UE es una comunidad política de Derecho constituida en régimen de organización internacional, *sui generis*, nacida para propiciar y acoger la integración y gobernanza en común de los Estados y los pueblos de Europa. Está compuesta por veintiocho Estados europeos y fue establecida con la entrada en vigor del Tratado de la Unión Europea (TUE), el 1 de noviembre de 1993.

ciológicos a nivel interno que provocarán pequeñas diferencias entre las legislaciones de unos y otros Estados.

El reconocimiento del derecho a la protección de datos de carácter personal, aunque es relativamente reciente en todos los Estados miembros de la UE, nos permite, hoy día, distinguir tres grandes grupos de Estados:

a) El grupo de aquellos Estados miembros en los que el texto constitucional reconoce expresamente un derecho a la protección de datos personales. Así ocurre en Suecia, Portugal, Eslovaquia, Eslovenia, Hungría y Polonia.[110]

b) El grupo de los Estados en los que el texto constitucional no reconoce expresamente un derecho a la protección de datos personales, pero sí contiene disposiciones sobre la materia que han permitido al Tribunal Constitucional reconocer dicho derecho fundamental. Este es el caso de España, Países Bajos, Finlandia y Lituania.[111]

c) El grupo de los Estados en los que en el texto constitucional no existe ninguna referencia a la protección de datos personales y el Tribunal Constitucional ha reconocido la existencia del derecho a la protección de datos personales como parte integrante, como

[110] El primer país en el que se reconoció este derecho fundamental en la Constitución fue Portugal, en 1976. Posteriormente, ante la importancia que está cobrando este derecho, el reconocimiento expreso en los textos constitucionales se produce cada vez más en los Estados miembros. Por regla general, en las Constituciones más recientes se ha decidido incluir el *derecho a la protección de datos personales*, como es el caso de las Constituciones de los países del Este, como la de Polonia; en otros casos, como está ocurriendo en los *länder* de Austria y de Alemania, por ejemplo, se han reformado sus Constituciones para incluir este derecho.

[111] *Vid.* art. 18.4 de la CE; art, 10 de la holandesa; art. 10 de la finesa, o el art. 22.3 de la lituana.

nuevo contenido, de otro derecho fundamental, sí reconocido expresamente en la Constitución, ya sea el derecho a la intimidad o a la vida privada, ya sea al libre desarrollo de la personalidad y la dignidad humana.[112]

44. Fue a partir de 1970 cuando los diferentes países europeos fueron abordando la tarea de regular el tratamiento de datos personales para tratar así de hacer frente a los potenciales peligros que los desarrollos tecnológicos representaban para la vida privada de las personas. Así, se han sucedido tres generaciones de leyes de protección de datos:

1) Las leyes de primera generación, surgidas tras la aprobación de la Ley del *Land* de Hesse, se caracterizaron por exigir una autorización previa para la creación de ficheros de datos y por crear autoridades de control encargadas de supervisar el tratamiento de datos.

2) Las leyes de segunda generación, elaboradas tras la aprobación del Convenio 108 sobre Protección de Datos del Consejo de Europa, se caracterizaron por una tendencia a la simplificación, por el abandono de los mecanismos previos de control y por la búsqueda de la autorregulación, de un equilibrio entre la protección de los derechos de los ciudadanos y el desarrollo de las nuevas tecnologías.

3) Tras la aprobación de la Directiva 95/46/CE —que nació con dos claros objetivos: evitar intromisiones ilegítimas en la vida de las personas y asegurar la consecución del mercado interior y la libre

[112] Así, se encuentran dentro de este tercer grupo la mayoría de los Estados miembros de la UE, como, por ejemplo, Italia, donde el derecho a la protección de datos personales no se encuentra reconocido constitucionalmente y han sido la jurisprudencia y la doctrina las que se han encargado de reconocerlo como parte integrante del *diritto a la riservatezza*.

circulación de datos sin restricciones injustificadas entre los Estados miembros (art. 1)—, las leyes de tercera generación se caracterizan por armonizar la libre circulación de datos y la defensa de los derechos de las personas, incrementando las medidas de seguridad; estas leyes, a diferencia de las anteriores, ya no se centran tanto en el uso de la informática como en la protección del individuo frente a la acumulación de datos personales.

45. La consolidación definitiva en la UE del derecho a la protección de los datos personales viene representada por la Carta de los Derechos Fundamentales de la UE,[113] que reconoce el «Respeto de la vida privada y familiar» (art. 7) y el derecho a la «Protección de datos de carácter personal» (art. 8), al dotar al derecho a la protección de datos de una configuración legal expresa.

El artículo 7 señala que «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones». Los derechos garantizados en el artículo 7 corresponden a los que garantiza el artículo 8 del CEDH. A fin de tener en cuenta la evolución técnica, se ha sustituido la palabra correspondencia por la de «comunicaciones». De conformidad con lo dispuesto en el apartado 3 del artículo 52, este derecho tiene el mismo sentido y alcance que el artículo correspondiente del CEDH.

El artículo 8 señala que «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a ac-

[113] *DOUE* C 303, de 14 de diciembre de 2007, y C 83, de 30 de marzo de 2010.

ceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente». Este artículo se basa en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE, así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El derecho a la protección de los datos de carácter personal se ejerce en las condiciones establecidas por la Directiva antes mencionada y puede limitarse en las condiciones establecidas por el artículo 52 de la Carta.[114]

46. La Carta distingue entre el tradicional derecho «al respecto de la propia vida privada y familiar» y el «derecho a la protección de datos personales». El primero está mencionado en el artículo 7, que en resumen reproduce el esquema del artículo 8 del Convenio Europeo de Derechos Humanos. El segundo, recogido en el artículo 8 de la Carta, consagra el carácter autónomo del derecho fundamental, distinto del derecho a la tutela de la vida privada. Y es importante resaltar que, caso único en el entero texto de la Constitución Europea, al derecho a la protección de datos personales se dedica un artículo específico también en la primera parte (art. 51). Este nuevo derecho fundamental no puede ser enmarcado en el esquema de *ser dejado solo*, sino que se

---

[114] *Vid.* M.ª Carmen GUERRERO PICÓ, *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 101-108; y, José MARTÍN Y PÉREZ DE NANCLARES, «Comentario al artículo 8. Protección de Datos de Carácter Personal», en *Carta de los Derechos Fundamentales de la Unión Europea*, Fundación BBVA, Madrid, 2008, pp. 223-243.

concreta en la atribución a cada uno del poder de *gobernar* la circulación de las informaciones que le conciernen. Se transforma así en elemento capital de la libertad del ciudadano en la sociedad de la información y de la comunicación.

47. Se ha individualizado, en su artículo 8, un novedoso derecho: el derecho a la protección de datos de carácter personal; que pasa a formar parte del orden público europeo y de los derechos de sus ciudadanos. Éste es uno de los derechos fundamentales que se explicitan con mayor amplitud y que aparece deslindado, con claridad meridiana, de otros como el respeto a la vida privada y familiar. Así, la privacidad ha entrado en la categoría de los derechos humanos en la medida que garantiza libertades ulteriores como la de obtener trabajo, un crédito o de optar o acceder a determinados servicios: en definitiva, devuelve al individuo (persona física)[115] el control sobre su entorno y garantiza la sostenibilidad del desarrollo.[116]

[115] Sin embargo, en determinados supuestos también las personas jurídicas, en tanto que destinatarias de las normas en materia de protección de datos, podrían ser titulares del derecho a la protección de datos. *Vid.* en el mismo sentido, José MARTÍN Y PÉREZ DE NANCLARES, «Comentario al..., *op. cit.*, pp. 231-232.

[116] Ya la STC 292/2000, de 30 de noviembre, indicaba el objeto y contenido propios del derecho fundamental a la privacidad —derecho fundamental que como tal es inherente a la persona e indisponible—. Protege un conjunto de datos de carácter personal, no necesariamente íntimos o incluso públicos, que, por su capacidad de ser tratados por medios informáticos, arrojan un perfil de la persona, y cuyo uso puede lesionar los derechos de los ciudadanos.

A. Iniciativas legislativas

48. Recientemente, el Parlamento Europeo y la Comisión han optado por una revisión de la Directiva 95/46/CE. Lo ha hecho a través de un Reglamento: ***Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos***,[117] norma general y directamente aplicable sin necesidad de transposición; el objetivo es claro: logar la uniformidad legislativa. Establece un conjunto de normas sobre protección de datos válido para toda la UE: control de los ciudadanos sobre sus datos personales, protección de datos adaptada al mercado único digital, y protección de datos en un contexto de mundialización. Ello deriva de la propia asunción de la figura del Reglamento como instrumento jurídico único.[118] Sin embargo, su base jurídica está, cuanto menos, en entredicho: reconocerle valor jurídico a la Carta de los Derechos Fundamentales no ha sido otra cosa que atribuirle valor normativo a aquello que ya se venía aplicando como principio general del Derecho. Pero es más, el artículo 6.1 del TFUE es muy claro: las «disposiciones de la Carta no ampliarán en modo alguno las competencias de la

[117] Reglamento General de Protección de Datos, de 25-01-2012. *COM (2012) 11 final.* Junto al nuevo Reglamento, la Comisión ha propuesto una Directiva que fija las normas sobre la protección de los datos personales tratados con fines de prevención, detección, investigación o persecución de delitos y para las actividades judiciales correspondientes.

[118] La aplicabilidad directa de un Reglamento reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos fundamentales de las personas y la contribución al funcionamiento del mercado interior.

Unión tal como se definen en los Tratados». La Comisión europea propone como fundamento el artículo 16.2 del TFUE, que parece atribuir una competencia específica al Parlamento Europeo y al Consejo que establecer «con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros». Aunque se trata de una atribución limitada al «ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos», ello explica que la Propuesta de Reglamento se acompañe de la Propuesta de una Directiva relativa al ámbito judicial y policial.

Se proporcionan refuerzos a las autoridades nacionales independientes de protección de datos para que efectúen una mejor aplicación de las normas de la UE en su territorio. Paralelamente, se acentúan sus atribuciones, al asumir con carácter general la potestad de multar a las empresas que quebranten las normas de protección de datos de la UE, sanciones que pueden suponer hasta un millón de euros o un 2% del volumen de negocios anual global de una empresa. A su vez, se eliminan requisitos administrativos innecesarios, como los de notificación a las empresas. En lugar de la disposición actual, que obliga a todas las empresas a notificar todas las actividades de protección de datos a los supervisores de protección de datos, el Reglamento intensifica la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesen datos personales. Por ejemplo, las empresas y organizaciones deberán notificar a la autoridad nacional de control toda violación de datos grave lo antes posible.

En cuanto al marco de protección de los ciudadanos, los principios normativos y los derechos Arco se refuerzan en tres sentidos:

1.º) Para los casos en que el tratamiento de los datos exija el consentimiento del interesado, deberá dejarse claro en la normativa nacional que dicho consentimiento ha de obtenerse explícitamente y no presuponerse. Se trata de una mejora necesaria respecto de la situación actual, en la que se permiten categorías de consentimiento cuya concurrencia no siempre es de fácil determinación. Así, y como ejemplo de ello, conforme a los artículos 6 y 7 de nuestra LOPD el consentimiento puede ser tácito o expreso, lo cual no deja de plantear problemas. Respecto del consentimiento tácito, por su difícil concreción, más aún si, como exige la LOPD de manera un tanto incongruente, ha de ser además de tácito, inequívoco. En cuanto al segundo, porque se distingue entre consentimiento expreso escrito y no escrito, subcategorías que, de nuevo, son de complicada definición.

2.º) Se regula el derecho a la portabilidad de los datos, es decir, se permite que los ciudadanos tengan un acceso más fácil a sus propios datos. Ello conlleva el poder transferir sus datos personales de un proveedor de servicios a otro con mayor facilidad, aspecto que aumenta además la competencia entre servicios.

3.º) Muy en boga en los últimos tiempos e íntimamente relacionado con el núcleo del derecho de protección de datos, esto es, la disponibilidad efectiva sobre los datos personales protegidos, se introduce el *derecho al olvido*. A través del mismo se pretende ayudar a los ciudadanos a gestionar mejor los riesgos inherentes a la protección de datos en línea, permitiendo a los usuarios borrar sus datos cuando no existan razones legítimas para conservarlos.

En lo relativo al ámbito geográfico de aplicación, deberán aplicarse las normas de la UE a toda empresa activa en el mercado de la UE que ofrezca sus servicios a ciudadanos de la Unión y procese datos perso-

nales en terceros países. Del mismo modo, los ciudadanos podrán dirigirse a la autoridad de protección de datos de su país, incluso cuando sus datos sean tratados por una empresa ubicada fuera de la UE.

49. Con respecto a la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita el futuro Reglamento plantea una novedad relevante: si bien el artículo 3 mantiene el criterio territorial vinculado al concepto *establecimiento* para responsables o encargados de tratamiento ubicados geográficamente en la UE, incluye un nuevo criterio de «tratamientos relacionados con oferta de bienes o servicios a ciudadanos de la UE» o destinados a «monitorizar su conducta» para responsables sin establecimiento en la UE. De esta forma, la protección de los datos de los ciudadanos deberá extenderse a la transferencia internacional de datos desde la UE a terceros Estados, con independencia de la ubicación geográfica de una empresa o de su centro de tratamiento de datos. En el contexto de globalización actual, se exige una mejora de los actuales mecanismos de transferencia internacional de datos a terceros Estados, a fin de facilitar el flujo transfronterizo de datos de carácter personal.

B. Cooperación de Autoridades

50. Cuando hablamos de Cooperación entre Autoridades nos estamos refiriendo a un caso concreto: el de las Normas o Reglas Corporativas Vinculantes (BCR –*Binding Corporate Rules*–). Su objetivo es claro: flexibilizar los flujos de datos entre empresas de grandes corporaciones multinacionales. Las empresas multinacionales necesitan que la información pueda fluir entre sus diferentes sedes. Para ello hay que

efectuar, en muchas ocasiones, una transferencia internacional de datos personales.

Se trata de códigos de buenas prácticas basados en las normas de protección de datos europeas y aprobadas al menos por una Autoridad de control, que dichas empresas multinacionales elaboran de manera voluntaria y suscriben a fin de asegurar las salvaguardias necesarias para determinadas categorías de transferencias internacionales de datos personales entre empresas que forman parte del mismo grupo de sociedades y están vinculadas por esas normas.[119]

51. Las BCR son un conjunto de normas o reglas de procedimiento interno que rigen las transferencias internacionales de datos de carácter personal en el seno de grupos multinacionales de empresas. Se trata de un instrumento potenciado por la UE, enfocado a remover los obstáculos a la libre circulación de datos personales entre países, y a flexibilizar los movimientos internacionales de datos personales entre un grupo de empresas multinacionales con filiales establecidas incluso fuera del EEE.

De esta manera, las normas corporativas vinculantes se configuran como un instrumento que permite a las empresas ofrecer garantías para poder llevar a cabo transferencias de datos hacía terceros países. En concreto, el Grupo de Trabajo del artículo 29, en su documento de trabajo *WP 108*, recoge un modelo de *checklist* para la aprobación de dichas normas corporativas vinculantes, y en otro documento de trabajo (*WP 107*), establece un procedimiento de cooperación para la emisión

---

[119] *Vid.* Comunicación de la Comisión al parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI*, Bruselas, 25 de enero de 2012. COM (2012) 9 final, pp. 12.

de posiciones comunes sobre las garantías proporcionadas por dichas reglas corporativas que permitan a las empresas transferir datos.

Las BCR, que constituyen un instrumento positivo, alternativa a las cláusulas contractuales tipo, responden a la lógica de los contratos, pero en un planteamiento multilateral que exige el establecimiento de mecanismos de cooperación internacional entre las Autoridades nacionales de protección implicadas. Se sigue un modelo, que podríamos denominar de *integración intermedia*. Supone la solicitud conjunta de las BCR ante una sola autoridad, pero la autorización debe ser emitida por cada una de las Autoridades nacionales de protección implicadas. Supone un grado de cooperación intermedio entre las Autoridades nacionales de protección.

El mecanismo es muy sencillo: *a)* uno de los miembros del grupo se erige en responsable de la solicitud y asume la iniciativa; *b)* este representante, que asume el liderazgo, debe presentar una sola solicitud de BCR a la Autoridad nacional de protección que considere la más adecuada *(leading authority)*; y, *c)* se presenta una sola solicitud que debe contener la mención de cada una de las Autoridades nacionales que debe prestar su autorización.[120]

El procedimiento de cooperación comienza en este momento: la autoridad nacional de protección directora del proceso reenvía las BCR a las otras Autoridades nacionales de protección implicadas para que realicen las alegaciones que estimen oportunas. Cuando éstas han sido realizadas, se comunica a la autoridad a cargo para que el grupo aporte las modificaciones necesarias; en ese caso, la versión inicial se consolida; aunque, como la última palabra la tiene cada una de las Auto-

[120] Por el momento, a 1 de enero de 2013, son 21 las Autoridades nacionales en materia de protección de datos que reconocen las BCR.

ridades implicadas, una puede estar conforme y otra exigir modificaciones para que las BCR se ajusten a su legislación nacional.

Este modelo presenta un atractivo frente a los contratos: sólo es necesario presentar las BCR para su aprobación ante una Autoridad nacional, mientras que los contratos deben ser presentados ante cada una de ellas, pero menos intenso, pues aunque las BCR se solicitan conjuntamente deben ser aprobadas por cada una de las Autoridades nacionales de protección implicadas.

Sin duda alguna, las BCR no sustituyen a las cláusulas contractuales tipo aprobadas por la Comisión Europea, puesto que cada instrumento tiene sus propios propósitos. No son sino una alternativa a las cláusulas contractuales tipo que pueden suscribirse entre exportador e importador para la regulación de una transferencia internacional, que suponga una cesión de datos, cuando el destinatario de los datos está ubicado en un país fuera de la UE y que no goza de un nivel de protección adecuado.

Deben ser vistas como un instrumento que facilite las transferencias internacionales de datos personales, garantice la aplicación de la normativa sobre protección de datos, y se convierta en un instrumento propicio para fomentar el desarrollo y aplicación de unos estándares internacionales comunes.

Las BCR constituyen una suerte de *safe haven* entre empresas de un mismo grupo. El elemento clave de las BCR es que las mismas son vinculantes, tanto hacia dentro como hacia fuera. Hacia *dentro* (obligatoriedad interna) requiere de mecanismos legales corporativos y psicología corporativa de cumplimiento que se garantiza con una formación adecuada del personal. Hacia *fuera* (obligatoriedad externa), es decir, que la política de privacidad de la compañía se dé a conocer con total transparencia y que se haga con un acto de publicidad por parte de la empresa.

52. El Grupo de Trabajo del artículo 29, en los últimos tiempos, se ha concentrado en la mejora de las autorizaciones basadas en las BCR,[121] habiéndose producido dos avances de interés:

- El primero de ellos tiene que ver con la aprobación por el Grupo de Trabajo del artículo 29 de tres Documentos de Trabajo (*WP153, 154* y *155*) que pretenden aclarar y complementar el régimen establecido por anteriores Documentos: en particular, por los *WP 74* y *108*.
- El segundo de los hitos destacados que merece una mención tiene que ver con la adopción de un acuerdo entre diversos Estados Miembros de la UE para el reconocimiento mutuo de sus decisiones en materia de BCR.[122] Este acuerdo surge como respuesta a las dificultades del procedimiento de coordinación existente. El problema que se pretende paliar es el largo tiempo que media entre que una empresa solicita la autorización de una BCR y el logro de la decisión final. El acuerdo supone que cuando una empresa solicite autorización para una BCR ante la *Leading authority*, la decisión que ésta adopte será aceptada por las demás Autoridades participantes. El mecanismo no se configura como un acuerdo de contenido jurídico, sino como un compromiso político, que no altera la necesidad de iniciar procedimientos nacionales de acuerdo con lo establecido por las diferentes legislaciones nacionales, ni

[121] Las BCR tienen su origen en la aprobación del documento de trabajo WP74, de 3 de junio de 2003, elaborado por el Grupo de Trabajo del artículo 29.

[122] El Grupo inicial de autoridades participantes estaba formado por Francia, Alemania (Agencia federal y autoridades de Estados federados), Irlanda, Italia, Letonia, Luxemburgo, Holanda, Reino Unido y España. A ellas se han unido posteriormente Noruega, Liechtenstein, Chipre, República Checa, Islandia, Malta y Eslovenia.

tampoco modifica la necesidad de que las BCR se ajusten a las especificidades que tales legislaciones puedan determinar.

En definitiva, las BCR se configuran, hoy día, como una alternativa contractual, de carácter multilateral, para la transferencia internacional de datos a terceros Estados. Se trata de reglas uniformes para el tratamiento de datos dentro de un grupo de empresas, aplicables a las sedes implicadas en la transferencia, que implica la cooperación entre las Autoridades nacionales de dichas sedes.[123]

53. Aunque el legislador europeo quiere darle un impulso a las BCR, convirtiéndolas en un instrumento habitual en todos los grupos multinacionales, y buena prueba de ello es que la Propuesta de Reglamento[124] pretende convertirlas en el estándar que empleen los grupos multinacionales en el futuro, la obligatoriedad externa que se predica de las BCR, en la práctica plantea (y seguirá planteando), a nuestro modo de ver, tres problemas capitales para la protección del titular del derecho a la protección de datos de carácter personal ante el tratamiento ilícito internacional de sus datos personales: *a)* su carácter vinculante;

[123] Sobre los presupuestos y ámbito de aplicación de las BCR, sus aspectos sustantivos más significativos y el procedimiento de cooperación establecido para conciliar el criterio de la solicitud única con el de la autoridad múltiple, *Vid.* Diana SANCHO VILLA, «Normas corporativas vinculantes *(binding corporate rules)*: aspectos sustantivos y de cooperación internacional de autoridades», en *Revista Española de Protección de Datos*, núm. 4. Enero-Junio 2008, pp. 35-60.

[124] *Vid.* Considerando 85.º de la Propuesta de Reglamento: «Todo grupo de sociedades debe poder hacer uso de normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo de empresas, siempre que tales normas corporativas incluyan principios esenciales y derechos aplicables con el fin de asegurar las garantías apropiadas para las transferencias o categorías de transferencias de datos de carácter personal».

b) el favorecimiento del *forum shopping*; y, sobre todo, *c)* la articulación de conflictos de competencia entre Autoridades de control. Veamos cada uno de ellos:

a) ***Su carácter vinculante:*** no podemos ocultar nuestras dudas sobre el carácter vinculante de las BCR, pues sólo son un mínimo nivel de protección: no son más que meras *declaraciones unilaterales de voluntad*; y es que, salvo algún caso aislado expresamente reconocido por la ley, la voluntad unilateral que se estima vinculante para quien la declara es la que va acompañada del consentimiento del que la recibe, por lo que en realidad se trata de un control unilateral, con obligaciones para una sola de las partes. Por eso, en la Ley española (RLOPD) se acepta la posibilidad de dar una autorización a solicitudes en que se aporte como garantía la existencia de unas normas corporativas vinculantes, pero siempre bajo el cumplimiento de unos requisitos concretos legalmente establecidos (art. 70.4 del RLOPD).

b) ***El favorecimiento del forum shopping***: las BCR implican que el grupo empresarial acepte que el posible perjudicado pueda elegir entre: *a)* la jurisdicción del Estado origen de la transferencia (lugar en que se encuentre el perjudicado); o, *b)* la del Estado en que se han delegado responsabilidades en protección de datos cometa —p. ej., el lugar donde se haya cometido la infracción— (WP 74, de 3 de junio de 2003), lo que, en la práctica, está favoreciendo el *forum shopping*.

El posible perjudicado (exportador o importador de los datos), consciente de que una misma situación privada internacional puede ser resuelta de manera distinta según sea planteada ante tribunales de un país o de otro país, podría acudir a las Autoridades de un país determinado con el fin de lograr un concreto resultado jurídico que fa-

vorezca sus intereses. Si las posibilidades del perjudicado se redujeran a una y sólo a una, cualquiera que sea el Estado miembro cuya autoridad deba pronunciarse al respecto, se evitarían evasiones de las legislaciones más restrictivas, no dando pie a prácticas de *forum shopping*, en caso de litigios derivados de la aplicación de una BCR, como consecuencia de un tratamiento ilícito internacional de datos de carácter personal.

c) ***La articulación de conflictos de competencia entre Autoridades de control:*** aunque la decisión de aceptación o no de las BCR será adoptada por consenso entre todas las Autoridades de control implicadas, no resulta posible la adopción de una decisión única al término del procedimiento de adopción de las BCR, al no caber el reconocimiento mutuo de las decisiones de las Autoridades. Se pueden plantear varios escenarios conflictuales: por un lado, uno, puede darse el caso de que una de las Autoridades de control participantes en el proceso de adopción de las BCR se declare competente en caso de incumplimiento de la misma, aún no siendo la Autoridad de control elegida en la BCR *(Leading authority)*; es más, puede darse el caso de que la autoridad de control llegue a extralimitarse en el ejercicio de sus funciones de control;[125] y, por

[125] Así, p. ej., a nuestro modo de ver, la Inspección de la AEPD realizada en Colombia, en julio de 2007, a dos empresas que prestaban sus servicios como centros de atención al cliente a dos empresas españolas del sector de las telecomunicaciones. La propia AEPD realizó la Inspección en Colombia, bajo el argumento de la existencia de un contrato entre el exportador de los datos (España) y el importador de los mismos (Colombia), donde se le atribuía competencia para la inspección a la AEPD (y la *amenaza* de que en caso de no permitir la inspección española se le retiraría a la empresa exportadora la autorización pertinente para realizar la transferencia internacional de datos). En nuestra opinión, fue un error gravísimo: las autoridades de control deben someterse al dictado del principio de

otro lado, dos, es posible la disparidad de criterios de las Autoridades de control de los Estados miembros; p. ej., a la hora de determinar cuándo un Estado tiene un *nivel de protección adecuado*, o, en su caso, que existan requisitos adicionales en cada país, como la notificación o diligencias administrativas, que habrá que cumplir también.[126]

2. Consejo de Europa[127]

54. El Consejo de Europa es una organización internacional de ámbito regional destinada a promover, mediante la cooperación de los Estados de Europa, la configuración de un espacio político y jurídico común en el continente, sustentado sobre los valores de la democracia, los derechos humanos y el imperio de la ley.

Tenemos como referente normativo el **Convenio 108/81/CE, del Consejo de Europa, de 28 de enero de 1981, para la *protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.**[128]

territorialidad, procediendo a efectuar las inspecciones que consideren oportunas a los efectos de verificar el cumplimiento de la normativa en protección de datos, en el marco de una transferencia internacional de datos, pero sólo en el país del exportador o en el país del importador, según el caso (la AEPD sería competente cuando el país de origen o el país de destino de los datos sea España).

126 Así, p. ej., el control *a posteriori* realizado por la AEPD, sobre la base del artículo 70.4 RLOPD.

127 Lo integran 47 países miembros, todos los de la Europa entendida en su más amplia concepción geográfica.

128 *BOE* núm. 274, de 15 de noviembre de 1985. Han ratificado el Convenio: Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Irlanda, Islandia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido y Suecia. Otros países han procedido sólo a la firma del Convenio, sin ratificarlo: Chipre, Eslovenia,

El Convenio 108/81/CE se presenta con un objetivo claro, que se establece en su artículo 1: garantizar a toda persona física el respeto de sus derechos y libertades fundamentales y en especial de su derecho a la intimidad, con relación al tratamiento automático de los datos de carácter personal que le conciernen (protección de datos).

La idea que subyace es buscar el equilibrio entre la protección de datos relativos a las personas y la libre circulación de las informaciones a través de las fronteras. El Convenio 108/81/CE «busca compatibilizar la protección del derecho a la intimidad personal con la liberalización de los flujos de datos entre los Estados parte *ius communicationis*»;[129] se trata de un instrumento jurídico que carece de aplicabilidad directa, ya que mientras un Estado firmante del mismo no dicte las normas de desarrollo oportunas, éste no podrá ser aplicado directamente por los Tribunales.[130] Además, se trata de una *norma de mínimos*, que opera a modo de *postulados generales*, pues permite, en su artículo 12, que los Estados parte en el mismo puedan llegar a tener un «Derecho distinto» sobre la materia, esto es, aunque la regla general es la «libre circulación de datos personales entre los Estados parte», estos pueden fijar limitaciones a la misma, mediante su normativa de desarrollo.[131,132]

Grecia, Hungría, Italia y Turquía. No han ratificado su Protocolo Adicional: Bélgica, Dinamarca, Grecia, Italia y Reino Unido.

129 Javier CARRASCOSA GONZÁLEZ, «Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado», en *Revista Española de Derecho Internacional,* vol. XLIV, núm. 2, 1992, p. 433.

130 *Vid.,* en el mismo sentido, STC 254/1993, de 20 de julio de 1993.

131 *Vid.,* en particular, Javier CARRASCOSA GONZÁLEZ, «Circulación internacional de datos personales informatizados y la Directiva 95/46/CE», en *Actualidad Civil*, núm. 23, 1997, pp. 512-513.

Son varios los principios sobre los que se sustenta el Convenio: *a)* el Principio del *consentimiento*, según el cual la finalidad justificativa de la creación de un fichero de datos debe estar definida y predeterminada antes de su puesta en funcionamiento; *b)* el Principio de *lealtad*, que implica que la recogida de datos debe realizarse de una forma lícita; *c)* el Principio de *calidad*, según el cual el responsable de los datos debe comprobar la exactitud de los datos recopilados y su actualización; *d)* el Principio de *publicidad*, que obliga a la existencia de un registro público de los ficheros automatizados; *e)* el Principio de *control*, que supone que cualquier persona tiene derecho a conocer si los datos que le conciernen son objeto de tratamiento informatizado y, si así fuera, a obtener copias de ellos, e incluso a su rectificación si fueran erróneos o inexactos; y, *f)* el Principio de *seguridad y confidencialidad en el tratamiento de los datos*, según el cual se debe establecer medidas de seguridad para que los ficheros de datos estén protegidos.

55. La relación existente entre la comentada revisión de la Directiva 95/46/CE y la del Convenio 108/81/CE, del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal es una realidad. Al cumplirse los 30 años de su adopción en 1981, se iniciaron los trabajos preparatorios de la revisión del Convenio 108 del Consejo de Europa, aunque ésta se lanzó formalmente a finales de 2010 con la

---

[132] *BOE* núm. 228, de 20 de septiembre de 2010. Son Estados Parte del Protocolo: Albania, Alemania, Andorra, Austria, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, España, Estonia, Eslovaquia, Francia, Hungría, Irlanda, Letonia, Macedonia, Liechtenstein, Lituania, Luxemburgo, Mónaco, Montenegro, Países Bajos, Polonia, Portugal, República Checa, Rumania, Serbia, Suecia, Suiza.

aprobación por el Comité de Ministros de una *Resolución sobre la Protección de Datos y la Privacidad en el Tercer Milenio*.

En 2011, el Consejo de Europa publicó una hoja de ruta con los hitos principales en lo relativo al proceso de modernización del Convenio 108. En noviembre de 2011, el Secretariado publicó una primera propuesta de texto articulado, para su presentación y primera discusión general en la reunión plenaria del Comité Consultivo de Protección de Datos (T-PD), que se celebró ese mismo mes de noviembre.

56. Existe un consenso unánime sobre la necesidad de que ambos procesos sean coherentes. Pero el hecho de que la propia Comisión haya manifestado su intención de negociar el texto del Convenio en ejercicio de las competencias de la UE en la materia (para lo que tendrá que pedir el correspondiente mandato al Consejo de la UE), parecen indicar que el proceso se verá ralentizado. Por otra parte, se da también la circunstancia de que el Consejo de Europa no se ha decantado aún por un instrumento de modificación de entre varias opciones posibles (protocolo adicional, protocolo de modificación o convenio revisado), lo que indudablemente influirá en el cumplimiento de los plazos marcados.

3. Foro de Cooperación Económica Asia-Pacífico[133]

57. La APEC se presenta como un Foro multilateral, creado en 1989, con el fin de consolidar el crecimiento y la prosperidad de los países del Pacífico, que trata temas relacionados con el intercambio comercial, coordinación económica y cooperación entre sus integrantes. El **Marco de Privacidad de APEC** promueve un acercamiento flexible a la protección de la privacidad de la información en las Economías miembro de APEC, evitando la creación de barreras innecesarias para los flujos de información (2005), fue desarrollado y aprobado en 2004, con unos objetivos claros: impulsar la apropiada protección de la información personal, prevenir la creación de barreras innecesarias al flujo de información, promover que empresas multinacionales utilicen métodos uniformes para recabar y procesar datos personales, y facilitar esfuerzos nacionales e internacionales para exigir la protección de datos personales.

58. Así las cosas, es evidente que los intentos de estas organizaciones de integración regional (UE, Consejo de Europa, APEC) no han logrado en la práctica una protección adecuada, eficaz y equilibrada del titular del derecho a la protección de datos de carácter personal ante un tratamiento ilícito internacional.

---

[133] Como mecanismo de cooperación y concertación económica, está orientado a la promoción y facilitación del comercio, las inversiones, la cooperación económica y técnica y al desarrollo económico regional de los países y territorios de la cuenca del océano Pacífico. La suma del Producto Nacional Bruto de las 21 economías que conforman el APEC equivale al 56% de la producción mundial, en tanto que en su conjunto representan el 46% del comercio global.

Los intentos de estas organizaciones de integración regional se enfrentan a una doble dificultad, generada por la naturaleza propiamente internacional del problema: por un lado, la capacidad para llegar a soluciones *ad intra* —armonizando (Directiva) o uniformizando (Reglamento) legislaciones—, o *ad extra* —procurando la coordinación de autoridades—; y, por otro lado, no puede prescindir del diálogo con otros sistemas. Un rearme proteccionista interior puede penalizar al mercado regional en el plano de la competencia internacional o generar el recurso a los paraísos de datos.

III. INICIATIVAS EN EL ESPACIO TRANSNACIONAL

59. Un último fenómeno normativo que puede alcanzar cierta importancia en la materia que nos ocupa son las iniciativas procedentes del denominado *Derecho transnacional*. En especial, el análisis se centrará en el protagonismo de las ***organizaciones creadas por los operadores del comercio internacional que codifican dicho ordenamiento jurídico espontáneo, profesional, cuyo objeto es regular las relaciones comerciales internacionales en el ámbito concreto de la protección del titular del derecho a la protección de datos.***

Tales iniciativas normativas vendrían protagonizadas por los siguientes organismos de carácter privado que se han ocupado específicamente del problema: ***1)*** **la CCI; y** ***2)*** **la ISO.**

1. Cámara de Comercio Internacional[134]

60. Debemos destacar una iniciativa: la **Propuesta de la CCI que pretende modificar la Decisión de la Comisión Europea 2002/16/CE, sobre *cláusulas contractuales tipo que amparan las transferencias a prestadores de servicios en terceros países*.**[135,136]

La Propuesta debe ser acogida favorablemente en la medida en que permite, con garantías, posibilitar que los prestadores de servicios puedan contratar a otras entidades para la ejecución de los servicios cuya prestación fue inicialmente asumida por ellos. Dicha Propuesta se dirige de forma prioritaria a permitir la subcontratación de servicios por parte de un encargado del tratamiento, entre empresas ubicadas en terceros países que no garanticen un nivel de protección adecuado. Lo que, en la práctica, puede suponer que los fenómenos de deslocalización de actividades empresariales desde Europa se incrementen.

Es por ello que, partiendo de las garantías que deben exigirse en las transferencias internacionales de datos de carácter personal a países que carecen de un nivel de protección adecuado, debemos formular una observación dirigida a mantener la neutralidad entre las em-

---

134 La CCI es una organización que se encarga de brindar protección a las empresas de los diferentes países del mundo en lo que confiere a las operaciones comerciales. Esta Cámara se creó en 1919 en Francia. Constituida con personalidad propia y naturaleza jurídica asociativa. Es la única organización empresarial que tiene el estatus de organismo de consulta ante las Naciones Unidas y sus organismos especializados.

135 *DO* 2002 l 6/52.

136 Hay propuestas de actualización no sólo por parte de la CCI sino también por otras partes interesadas: la *Japan Business Council in Europe* (JBCE), el *EU Committee of the American Chamber of Commerce in Belgium* (Amcham) y la *Federation of European Direct Marketing Associations* (FEDMA).

presas que operan en el ámbito de la UE y las ubicadas en terceros Estados, en relación con el fenómeno de la subcontratación.

A mi modo de ver, el documento presenta una omisión relevante puesto que se limita a incorporar cláusulas contractuales que garanticen la protección de datos personales cuando el prestador de servicios (importador de los datos en un tercer país), subcontrata a otra empresa ubicada asimismo en un país tercero y no da respuesta a la posibilidad de que un prestador de servicios ubicado en la UE pueda subcontratar con garantías adecuadas con entidades en terceros países. La citada omisión podría suponer, en la práctica, que los efectos de las modificaciones propuestas no sean neutrales al permitir una mayor flexibilidad al prestador de servicios establecido en un tercer país frente al establecido en la UE, teniendo en cuenta que en el primero de los casos los riesgos asociados al tratamiento de datos pueden ser superiores al prestarse todos los servicios contratados o subcontratados en países donde, salvo en virtud de las cláusulas contractuales tipo, no es de aplicación la Directiva 95/46/CE.

Por tanto, esta falta de neutralidad puede incentivar fenómenos de deslocalización de actividades empresariales en la UE más intensivos de los que resultarían si se contemplaran unas cláusulas contractuales tipo que permitieran, al menos, que la actividad del primer prestador de servicios contratado por el responsable del tratamiento que subcontrata a empresas en un tercer país, estuviera ubicada en la UE. En tal caso, las modificaciones de la Decisión 2002/16/CE propuestas por la CCI, como concreción del sistema de garantías de la Directiva 95/46/CE, operarían como un instrumento normativo discriminatorio en contra de actividades empresariales en la UE, quedando, en última instancia, en cierto modo, desprotegido el titular del derecho a la protección de datos de carácter personal ante el tratamiento ilícito internacional de sus datos de carácter personal.

2. Organización Internacional de Normalización[137]

61. La Organización Internacional de Normalización o ISO es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

Las normas que, actualmente, están siendo elaboradas por el nuevo grupo de trabajo de la ISO son tres: ***1)*** **la norma ISO 24760-1:2011** («marco para que la gestión de información sobre la identidad se realice de manera segura, fiable y respetuosa de la privacidad»), que define los términos para la gestión de identidades y especifica los conceptos básicos de la identidad y la gestión de la identidad y sus relaciones;[138] ***2)*** **la norma ISO 29100:2011** («marco sobre privacidad que define los requisitos de privacidad para el procesamiento de información de carácter personal en cualquier sistema de información de cualquier jurisdicción»), que proporciona un marco de privacidad al especificar una terminología común sobre la privacidad, definir los actores y sus roles en el procesamiento de información personal identificable, describir las consideraciones de privacidad salvaguardar, y

[137] La ISO es una red de los institutos de normas nacionales de 161 países, sobre la base de un miembro por país. Las normas desarrolladas por ISO son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país.

[138] Es aplicable a cualquier sistema de información que procesa la información de identidad. Se proporciona una bibliografía de los documentos que describen distintos aspectos de la gestión de la información de identidad.

proporcionar referencias a los principios de privacidad conocidos de tecnología de la información;[139] y *3)* **la norma ISO 29101:2013** («marco de referencia sobre la privacidad que establece las mejores prácticas para la implementación técnica uniforme de los principios de privacidad»), que define un marco de arquitectura de privacidad que especifica la preocupación por los sistemas (TIC) que procesan la información de identificación personal de la información y tecnología de comunicación, las listas de componentes para la aplicación de estos sistemas, y ofrece vistas arquitectónicas contextualizar estos componentes.[140]

62. Las ***iniciativas en el espacio transnacional (CCI, ISO)*** son, en principio positivas, pero no son ***suficientes, desde la perspectiva tuitiva, para la protección del titular del derecho a la protección de datos.*** Tienen como destinatarios a las empresas de la industria de tratamiento internacional de datos (causantes del daño en un tratamiento ilícito internacional de datos). Consecuentemente, el perjudicado no tiene posibilidad de invocarlas.

[139] Es aplicable a las personas físicas y organizaciones que participan en la especificación, el reclutamiento, la arquitectura de diseño, desarrollo, pruebas, mantenimiento, administración y operación de sistemas y servicios de información y tecnología de comunicación que se requieren controles de privacidad para el procesamiento de información de identificación personal.

[140] Es aplicable a las entidades que participan en la especificación, el reclutamiento, la arquitectura de diseñar, probar, mantener, administrar y sistemas TIC operativo que procesan información de identificación personal.

IV. BALANCE FINAL

63. Cualquier economía moderna tiene la necesidad de poder transmitir datos de carácter personal hacia el exterior. Si bien el perjudicado por un tratamiento ilícito internacional de sus datos se encuentra en una clara situación de inferioridad jurídica, que le sitúa al borde de la desprotección, la solución no puede venir por el bloqueo radical de los datos personales del perjudicado hacia el exterior.

Los retos que plantea la mundialización requieren herramientas y mecanismos flexibles que garanticen una protección adecuada, equilibrada y eficaz, sin fisuras jurídicas de los datos personales. Desde la superestructura jurídica internacional y las estructuras de carácter regional se deben promover la adopción de unas normas de protección de datos exigentes e interoperables en todo el mundo.[141]

64. El estudio de los mecanismos y reglas de protección vigentes en los distintos niveles de producción normativa —superestructura jurídica internacional, sistemas de integración regional, realizaciones del denominado *derecho transnacional*—, arroja un balance claro: el marco jurídico existente es a todas luces insuficiente para garantizar el derecho fundamental a la protección de datos ante un tratamiento ilícito internacional.

Las normas emanadas de las instancias internacionales y de las organizaciones de integración regional, a pesar de que han establecido límites a las transferencias internacionales de datos para evitar que la

[141] *Vid.* Comunicación de la Comisión al parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI*, Bruselas, 25 de enero de 2012. COM (2012) 9 final.

legislación interna de un país en la materia pueda ser burlada mediante la transferencia a otro país en donde la legislación sea menos exigente (o incluso que no exista legislación alguna en este campo), no tienen como objetivo principal la protección del titular del derecho a la protección de datos de carácter personal, sino cumplir con los objetivos de sus tratados. Por lo general, no son normas directamente invocables por los particulares, sino que son normas dirigidas a los Estados.

Otro tanto cabe decir de las posibles soluciones que provengan del espacio transnacional: o bien se trata de códigos de conducta, recomendaciones, instrumentos de *soft law*, que tienen como destinatarios a las empresas de la industria de tratamiento internacional de datos; o bien ofrecen mecanismos alternativos de resolución de controversias pensados desde y para la defensa de los intereses de esas misma empresas.

65. Lo deseable sería la aprobación de una normativa que permita esclarecer responsabilidades en los flujos internacionales de datos derivados de las necesidades empresariales, reducir los costes de cumplimiento con la normativa, facilitar a los titulares del derecho a la protección de datos instrumentos efectivos de protección de sus derechos, y dotar de mayor eficacia a los reguladores y minimizar las cargas administrativas.

Mientras eso llega, a día de hoy, la normativa de Derecho internacional privado es, de lejos, la más sencilla y manifiestamente mejorable desde un punto de vista tuitivo. En efecto, como veremos en el **capítulo III**, con un mínimo coste nomogenético, tanto la posible interpretación creativa de las normas vigentes cuanto la eventual elaboración de nuevas reglas arrojan resultados mucho más equilibrados, efectivos y adecuados, desde la perspectiva del titular del derecho a la protección de datos de carácter personal, ante un tratamiento ilícito internacional de sus datos.

Capítulo III.

Mecanismos de resolución de controversias para la protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita: mecanismos alternativos o jurisdiccionales de resolución de controversias

66. Una vez definido, deslindado y perfilado el objeto de estudio en el **capítulo** I, y estudiadas, en el **capítulo** II, las normas que se proyectan sobre el supuesto tipo, en este **capítulo** III vamos a: en primer lugar, descartar los diferentes mecanismos alternativos de resolución de controversias a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, para obtener una tutela adecuada, equilibrada y efectiva (I); para, en segundo lugar, estudiar la posible satisfacción de los problemas derivados del supuesto típico, desde la perspectiva del Derecho internacional privado, centrándose en el sector de la resolución judicial de controversias (II).

I. MECANISMOS ALTERNATIVOS DE RESOLUCIÓN DE CONTROVERSIAS

67. Una vez definido, deslindado y perfilado el objeto de estudio en el **capítulo** I, y estudiadas, en el **capítulo** II, las normas que se proyectan sobre el supuesto tipo, en este **primer apartado del capítulo** III vamos

a analizar los diferentes mecanismos alternativos de resolución de controversias a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, para obtener una tutela adecuada, equilibrada y efectiva. De esta forma, nos ocuparemos del recurso a las distintas modalidades de arbitraje (**1**), del eventual recurso a la mediación (**2**), para, en última instancia, valorar sí los mecanismos de alternativos de resolución de controversias ante un litigio derivado de una transferencia internacional de datos personales ilícitos nos ofrecen esa tutela demandada (**3**).

1. Recurso a las distintas modalidades de arbitraje

68. Es un hecho incontestable que el arbitraje se ha consolidado como un sistema rápido, seguro y eficaz para resolver las controversias que puedan surgir en el tráfico mercantil, tanto interno como internacional, y con las necesarias garantías de confidencialidad y especialización. Facilita, así, el desarrollo fluido de los intercambios comerciales y económicos al ajustarse a las nuevas y más complejas características, que están presentes en las transacciones que se producen en el nuevo entorno configurado por la mundialización de la economía y la nueva Sociedad de la Información.

Sin duda, los litigios derivados de transferencias internacionales de datos exigen soluciones rápidas; y, éstas, hoy en día, fundamentalmente, dado la secular lentitud de la justicia ordinaria, pueden venir de la mano de procedimientos de resolución extrajudicial de litigios.[142]

[142] Así lo han señalado, entre otros textos normativos, la Directiva sobre comercio electrónico, la LSSI, la Resolución del Consejo de 25 de mayo de 2000 relativa a una red comunitaria de órganos nacionales responsables de la solución extrajudicial de los litigios en materia de consumo (*DO* 2000 C 155/1), y la Recomenda-

El tráfico mercantil internacional de hoy –y más el peculiar contexto de las situaciones privadas derivadas de Internet– supone una celeridad tal en los negocios, que mal podría desconocerse la necesidad de asegurar con la misma rapidez, la protección jurídica de los intervinientes en el mercado. Así, se ha pensado, desde hace ya varios años, y, como resultado, se ha diseñado un sistema alternativo de resolución de conflictos en el que si bien se decide en Derecho o en equidad, excluye parcialmente a los tribunales de actuar en la resolución de conflictos, por cuanto, bajo este esquema, son ahora los particulares –los árbitros– los llamados a solucionar las disputas surgidas entre otros particulares.

69. Si bien el recurso a la jurisdicción ordinaria es la regla general en materia de conflictos derivados de una transferencia internacional de datos de carácter personal (sobre todo, en aquellos derivados de un contrato *interpartes)*, quizás, pudiera apuntarse la conveniencia de utilizar la tendencia hacia la llamada desjudicialización de las controversias. Sin duda, la accesibilidad, rapidez, eficacia, confidencialidad, especialización en la materia, bajo coste, trazabilidad y seguimiento, flexibilidad y ejecutabilidad son argumentos más que suficientes, a favor del arbitraje como alternativa a la solución judicial.[143] El recurso al arbitraje convencional de un tercero imparcial, con plenas facultades para dirimir el conflicto, en materia de transferencia internacional de datos, entre el perjudicado y el causante del daño, y para repartir

---

ción 98/257/CEE, de 30 de marzo de 1998, relativa a los principios aplicables a los órganos responsables de la solución extrajudicial de los litigios en materia de contratos de consumo (*DO* 1998 L 115/31).

[143] *Vid.*, en el mismo sentido, V*VID.*AA., *Factbook Comercio Electrónico*, 3.ª ed., Aranzadi, Elcano (Navarra), 2004, pp. 817-818.

los gastos que el mismo pudiera ocasionar, podría acabar con la unilateralidad propia del arreglo judicial de controversias.

70. El recurso a los ADR ***(Alternative Dispute Resolution)***, como mecanismo de resolución de litigios del mundo analógico, o bien para resolver controversias generadas en el mundo virtual, aunque es sumamente ventajoso para los particulares e incluso para las empresas —ya que se convierte en un sello de calidad empresarial, es un sistema que permite evitar mayores problemas, y ofrece una imagen positiva del producto—.[144] Sin embargo, no nos parece un mecanismo adecuado para resolver una controversia derivada de una transferencia internacional de datos personales extracontractual ilícita en la medida en que nos encontramos ante un supuesto en que las posiciones son muy distintas, en función de los intereses concurrentes.

71. No obstante, la resolución extrajudicial de conflictos requiere tanto de un apoyo o previsión legal y de un amplio reconocimiento legislativo, que permita garantizar a las partes la existencia de unos principios por los que se rija, cuanto de un apoyo por parte de los poderes públicos; de forma que se fomente su utilización, y se genere la suficiente confianza en ellos. Sin ninguna duda, Internet es un medio con un potencial extraordinario en el ámbito de la resolución de controversias. La autonomía de la voluntad de las partes en la construcción de su sistema de arbitraje se traduce en la existencia de libertad para

[144] *Vid.*, en el mismo sentido, en relación con las ventajas que comporta el Sistema Arbitral de Consumo, Robert CORTADAS ARBAT, «Luces y sombras del sistema arbitral de consumo: el sistema arbitral desde la óptica empresarial», en Carles E. FLORENSA I TOMÁS (Ed.), *El arbitraje de consumo*, Tirant lo Blanch, Valencia, 2004, pp. 181-184.

pactar el empleo de medios electrónicos en su procedimiento arbitral. Por tanto, cabe la posibilidad de utilizar Internet en algunas o en todas las fases del procedimiento arbitral, pero el recurso al arbitraje telemático o en línea, esto es, la que todas las fases del procedimiento se desarrollen en Internet, hoy en día, no sólo en materia de transferencia internacional de datos, sino, en general, en cualquier ámbito material, pensamos que es improbable y de difícil aplicación, por los problemas procesales que plantea (entre otros, digitalización de ciertos medios de prueba, garantizar la confidencialidad del procedimiento, o acreditar que las notificaciones se han realizado fehacientemente, etc.)[145]

72. La resolución de un litigio a través de Internet, mediante la correspondiente conexión *on line* entre los litigantes y el tercero imparcial constituye un ODR ***(Online Dispute Resolution Systems)***. El arbitraje *on line* o telemático constituye una variante de los ADR que consiste en aprovecharse de los medios tecnológicos para la resolución arbitral del litigio. De esta forma, el uso de las comunicaciones electrónicas y las nuevas tecnologías se convierten en aliados para la resolución extrajudicial de los conflictos planteados.

Son características propias de los ODR: *a)* su especialidad, ya que se celebra por vía electrónica; *b)* el consentimiento mutuo de las partes manifestado electrónicamente; *c)* su ámbito de aplicación ilimitado; *d)* la idoneidad para resolver las controversias derivadas de la contratación electrónica; y, *e)* la fuerza vinculante del laudo dictado por el árbitro.

---

[145] *Vid.*, en el mismo sentido, Pedro De Miguel Asensio, *Derecho privado de Internet*, 4.ª ed., Civitas, Cizur Menor (Navarra), 2011, p. 489-495.

Son diversos los sistemas de arbitraje *on line* existentes hoy en día, desarrollados no sólo en el panorama internacional y en el ámbito comunitario, sino también a nivel nacional.[146]

73. Los ODR son sistemas que sólo operan a través de Internet, pensados exclusivamente para ser utilizados en un entorno electrónico, si

---

[146] Experiencias españolas en el ámbito del comercio electrónico como las articuladas por la Asociación Española de Arbitraje Tecnológico (Arbitec), por la empresa Arbitraje y Mediación (Aryme), por la Asociación Española de Normalización y Certificación (Aenor), por la Asociación Comunitaria de Arbitraje y Mediación (ACAM), o por el Tribunal de resolución Extrajudicial de Conflictos de la Asociación Andaluza de Comercio Electrónico; o, en materia de protección de consumidores, iniciativas como las del propio Instituto Nacional de Consumo —a través del programa SITAR—, o de la Conselleria de Industria, Comercio y Turismo valenciana —a través del proyecto *Arbitraje Virtual de Consumo*—[146]. No son escasas las iniciativas surgidas en el seno de la UE, tales como los proyectos «Ecodir» (*Electronic Consumer Dispute Resolution Platform*), «E-Arbitration-T», «Eurochambers», y «Webtrader»; o, la Red Eje-Net. En el ámbito internacional, además de los centros de arbitraje de la OMPI o de la Cámara de Comercio Internacional, debemos mencionar algunas iniciativas que nos llevan a reflexionar sobre la conveniencia en apostar por los ODR: como, p. ej., el sistema *SquareTrade* (la compañía Squaretrade, situada en San Francisco, CA, ofrece un sistema de negociación, mediación y arbitraje por medio de Internet. Sus principales clientes son los participantes en disputas sobre productos vendidos en remates *on line*, tanto como conflictos originados en la falta de cumplimiento contractual entre proveedores de servicios y compañías), el *Cybersettle.com* (organización que usa un método propio para arbitrar disputas concernientes a asuntos financieros, en particular las sumas a otorgar en compensación por daños asegurados; los métodos puramente automatizados están diseñados de tal manera que ofrecen un proceso basado en una fórmula matemática), o el *Magistrado Virtual —Virtual Magistrate Project—* (sistema de arbitraje virtual, organizado para casos de conflictos por uso indebido de material protegido por leyes de propiedad intelectual, con el objeto de proveer de un sistema rápido y de bajo costo para decidir temas de protección de derechos de propiedad intelectual *on line*).

bien cabe señalar que los mismos todavía se encuentran en una fase inicial que requiere de un desarrollo efectivo y adecuado mediante el apoyo legal necesario para que los mismos lleguen a ser plenamente operativos.

74. El mundo virtual presenta dos características que convierten a los métodos clásicos de resolución de controversias en menos eficientes: *a)* su rapidez; y, *b)* el bajo coste. El primer aspecto es el de la rapidez en las transacciones *on line*, que demanda una respuesta igualmente rápida a los problemas encontrados. El segundo aspecto es el muy reducido coste de acceso al mundo cibernético: este coste invita la participación en el comercio y en la política *on line*, de entidades pequeñas e individuos que no podrían tener entrada de otro modo en los mercados tradicionales o en las arenas políticas. Cuando los costes de los sistemas de resolución de controversias, en tiempo y dinero, superan el valor de la disputa, esto significa que las víctimas no van a poder encontrar solución accesible a sus disputas, y entonces los actores deberán enfrentarse a costes de litigio que cancelan las ventajas de sus ofertas de bienes y servicios en el mercado electrónico.

75. Sin ninguna duda, los ODR parece que son todo ventajas, ya que permite la conexión, a golpe de ratón, entre partes que están ubicadas en distintos lugares del mundo—, comodidad —pues evita el desplazamiento de las partes—, eliminación de horarios —ya que Internet está abierto 24 horas—, su bajo coste —las facilidades de comunicación por Internet y el hecho de que las partes no tengan que desplazarse suponen una reducción considerable del coste económico del procedimiento arbitral— y, su trazabilidad y seguimiento —ya que las nuevas tecnologías permiten verificar, controlar y tutelar en línea y en

tiempo real el estado de las actuaciones, lo que facilita una posición de los litigantes en el pleito más activa—.

Ahora bien, si queremos impulsar los ODR como mecanismos de resolución extrajudicial de controversias derivadas de una transferencia internacional de datos ilícita debemos partir de cinco grandes premisas: primera, la extensión de estos sistemas no debe comportar una mayor burocratización, esto es, los sistemas deben seguir siendo directos, rápidos, ágiles y comprensibles; segunda, debemos apostar por una mayor cualificación de los árbitros, mediadores, negociadores y conciliadores; tercera, debe fomentarse el criterio del Derecho frente al de la equidad, y en aquellas materias en las que el Derecho vaya detrás de la realidad social, y sólo en esos caso, apostar por el criterio de equidad; cuarta, debe potenciarse e incrementarse la información acerca de la existencia de estos mecanismos extrajudiciales de resolución de conflictos; y, quinto, han de implantarse las nuevas tecnologías, sobre todo, para facilitar los procedimientos de comunicación.

76. Además, de nuevo debemos hacer la misma reflexión: difícilmente perjudicado y causante del daño, en la práctica, van a someter su controversia a un ODR: la necesidad de garantizar la confidencialidad de las partes y la seguridad —técnica y jurídica— del procedimiento arbitral, la familiaridad y el conocimiento de las nuevas tecnologías y, la perdida de los componentes físicos y visuales de la comunicación en persona.[147]

[147] *Vid.* Ana Montesinos García, «Los retos..., *op. cit.*, pp. 243-246.

2. Eventual recurso a la mediación

77. La ***mediación*** es un mecanismo de resolución alternativa de controversias que ayuda a resolver, de forma pacífica, diferentes tipos de conflictos[148]. Es una instancia voluntaria que tiene como objetivo el acercamiento entre las personas que presentan una posición controvertida, El mediador a cargo del proceso, con su habilidad, ayuda a que se clarifiquen e identifiquen esos intereses en conflicto y que se llegue a un acuerdo satisfactorio, sin tener que recurrir al órgano jurisdiccional de turno;[149] el mediador, contrariamente a lo que hace el árbitro en el arbitraje, no impone ninguna solución a las partes, sino que son ellas mismas quienes generan el acuerdo.

---

148 *Vid.*, en general, Alexander H BEVAN, Alternative dispute resolution: a lawyer's guide to mediation and other forms of dispute resolution, Sweet & Maxwell, 1992; Dennis CAMPBELL y Peter SUMMERFIELD, Effective Dispute Resolution for the International Commercial Lawyer, Kluwer Law and Taxation Publishers, Deventer, 1987; y, en material de consume, Marta CAPDEVILA I NOGUÉ, «Mediació en matèria de consum», en Carles E. FLORENSA I TOMÁS (Ed.), El arbitraje..., *op. cit.*, pp. 121-132.

149 *Vid.*, en general sobre la mediación como un mecanismo propicio para la resolución de conflictos, Stephen B. GOLDBERG, Eric D. GREEN, y Frank E. A. SANDER, *Dispute Resolution*, Little, Brown & Company,..., *op. cit.*, pp. 99-147; Stephen B. GOLDBERG, Eric D. GREEN y Frank E. A. SANDER, *Dispute Resolution. 1987 Supplement with Exercises in Negotiation, Mediation, and Mini-Trials*,..., *op. cit.*, pp. 39-64; y, Helena SOLETO MUÑOZ y Milagros M.ª OTERO PARGA (Coords.), *Mediación y solución de conflictos. Habilidades para una necesidad emergente*, Tecnos, Madrid, 2007; y, en particular, sobre las principales habilidades que se debe potenciar para ser un buen mediador, Julio GARCÍA RAMÍREZ, y Sergio ORTAS GIGORRO, «Principales habilidades del negociador en el ámbito jurídico», en *Economist & Jurist*, núm. 112, julio-agosto 2008, Difusión Jurídica, Madrid, 2008, pp. 130-132.

78. La mediación no es un método o una técnica de resolución extrajudicial de conflictos nueva en España. Lo que es nuevo es el impulso que le ha dado el legislador.[150]

Se trata de un sistema de negociación asistida (las partes actúan, negocian y proponen las soluciones por sí mismas); voluntario (las partes deciden participar o no en el proceso de mediación y ponerle fin en cualquier momento y no están obligadas a llegar a un acuerdo), dirigido (es un proceso que tiende al acuerdo y/o a la reparación); que se basa en el principio ganar/ganar (no tiende a la competencia); en el que el mediador utiliza una estructura ya pautada y técnicas específicas para alcanzar los objetivos; basado en el principio de confidencialidad (el mediador y las partes no pueden revelar lo sucedido en las sesiones; salvo con la autorización de las partes); y, no sujeto a reglas procesales, ya que el procedimiento es absolutamente informal y flexible.

79. La mediación es un ADR flexible y confidencial, que consta de 5 etapas: *a)* Introducción —explicación a las partes por parte del mediador de las reglas del procedimiento y de su papel en la mediación—; *b)* Sesión común —las partes exponen su conflicto, guiadas por el mediador, y planteamiento de sus pretensiones—; *c)* Sesiones separadas o *caucus* —se realizan cuando el mediador percibe, a través del relato de las partes, que hay asuntos confidenciales que no se pueden debatir en la sesión conjunta, y que pueden entorpecer el procedimiento si no se tratan adecuadamente—; *d)* Cierre —el mediador hace un resumen

[150] *Vid.* Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles. *BOE núm.* 162, de 7 de julio de 2012; y Real Decreto 980/2013, de 13 de diciembre, por el que se desarrollan determinados aspectos de la Ley 5/2012, de 6 de julio, de mediación en asuntos civiles y mercantiles. *BOE núm.* 310, de 27 de diciembre de 2013.

de los acuerdos alcanzados, parciales o totales, y redacta el acuerdo de mediación—; y, *e)* Formalización del acuerdo —la mediación termina con el contrato redactado y firmado por las partes en el mismo acto de cierre de la sesión—.[151]

80. La mediación, como alternativa para la resolución de conflictos, **preserva la relación entre las personas** involucradas en la disputa. En la mediación, la decisión a la que lleguen las partes será elaborada por ellas mismas y no por el mediador. Se reafirma así la capacidad de la mediación de devolverle el poder a las partes para que sean ellas mismas las protagonistas de la decisión, y no el mediador.

Constituye una manera diferente de resolver nuestros conflictos, ya que permite que seamos nosotros mismos los que resolvamos nuestras diferencias con la otra parte, esto se consigue con la ayuda de un mediador (que ni es juez ni parte), de manera objetiva, neutral e imparcial, reconduce la comunicación para que los participantes puedan volver a escucharse y hablarse.

81. Pues bien, en mi opinión, será muy difícil vemos capaces de llegar a un acuerdo extrajudicial a las partes litigantes: perjudicado y causante del daño, que se encuentran en una posición de desequilibrio tal que precisa de la intervención de una autoridad pública con potestad

[151] *Vid.*, en relación con las características y fases de la mediación, Joan SALA, «La mediación, una alternativa para la resolución de conflictos», en *Revista IURIS. Actualidad y Práctica del Derecho*, núm. 120, octubre 2007, Barcelona, pp. 25-27.

resolutoria, que ponga fin al conflicto *interpartes* y cuya resolución sea vinculante para ambas partes.[152]

3. Balance final

82. *Los **obstáculos a la aplicación de estos mecanismos de resolución extrajudicial de conflictos son dos***: por un lado, la falta de confianza y de conocimiento de estas alternativas por parte de los particulares; y, por otro lado, su alto coste para los litigantes y los pocos «incentivos» para el cumplimiento del veredicto. En mi opinión, estos mecanismos no son los adecuados para solucionar este tipo de controversias, que requieren de costes reducidos, agilidad y escasa formalidad.

83. Si queremos promover el desarrollo de mecanismos alternativos de resolución de controversias *on line* para resolver los litigios derivados de una transferencia internacional de datos ilícita deberíamos trabajar en tres dimensiones: primera, alentando el desarrollo de criterios apropiados para el mundo virtual; segunda, desarrollando la infraestructura tecnológica necesaria para asegurar que los mecanismos de resolución de disputas sean de bajo coste; y, tercera, implicando a todos los sujetos participantes en Internet.

Además, no hay, a día de hoy, órganos internacionales de resolución extrajudicial de controversias, ya que los ADR o los ODR tienen

[152] La mediación entre empresas es un éxito incontestable en otros países europeos, como p. ej., Francia o Reino Unido, donde los litigios se reducen en un porcentaje considerable. Esta práctica es aún mayor en EE.UU., donde más de un tercio de los conflictos no se judicializan. Pero, en España como la mediación es voluntaria, tanto para los jueces como para las partes, cuesta abrir camino.

un ámbito nacional y, son los acuerdos entre ellos, a nivel internacional, los que permiten el desarrollo de la autorregulación con un alcance global. El principio que inspira esa actividad de autodisciplina global, cuando nos encontramos ante controversias transfronterizas, no es otro sino el reconocimiento recíproco; y, que es realmente eficaz cuando se desarrolla por entidades de autorregulación de carácter internacional, integrados por organizaciones de autodisciplina nacionales.

84. Así las cosas, como veremos a continuación, a día de hoy, para obtener una legítima compensación ante la violación de un derecho fundamental, el Derecho internacional privado se presenta como el sistema normativo más sencilla y manifiestamente mejorable; ya sea reinterpretando a favor del perjudicado las normas vigentes de competencia judicial internacional y derecho aplicable; ya sea reformando en sentido tuitivo dicha normativa.

El recurso a la resolución judicial de controversias se presenta, *a priori*, como la solución más factible para procurar una protección adecuada, equilibrada y eficaz del perjudicado por una transferencia internacional ilícita de información personal sensible.

II. MECANISMOS JURISDICCIONALES DE RESOLUCIÓN DE CONTROVERSIAS

85. Una vez definido, deslindado y perfilado el objeto de estudio en el **capítulo I**, estudiadas, en el **capítulo II**, las normas que se proyectan sobre el supuesto tipo; y en el **primer apartado de este capítulo III** analizados los diferentes mecanismos alternativos de resolución de

controversias a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, para obtener una tutela adecuada, equilibrada y efectiva; en este **segundo apartado de este capítulo III** me ocuparé del recurso a la resolución judicial de controversias ante la reclamación del perjudicado, titular del derecho a la protección de datos, por un tratamiento ilícito internacional de sus datos de carácter personal: estudio de la normativa para la determinación del tribunal internacionalmente competente en materia de transferencias internacionales de datos de carácter personal (**1**), de la prórroga de la competencia (**2**), de los litigios derivados de una transferencia internacional de datos de carácter personal ilícita en ausencia de pactos entre las partes (**3**), del *forum delicti commissi* como alternativa al foro general del domicilio del demandado (**4**), de la solicitud de medidas cautelares o provisionales en litigios derivados de una transferencia internacional de datos de carácter personal ilícita (**5**), y de la LOPJ como regla subsidiaria para los supuestos no contemplados ni por el régimen institucional ni por el régimen convencional en materia de transferencia internacional de datos de carácter personal ilícita (**6**). Así las cosas, veremos como el recurso a la resolución judicial de controversias se presenta, *a priori*, como la solución más factible para procurar una protección adecuada, equilibrada y eficaz del perjudicado por una transferencia internacional ilícita de información personal sensible (**7**).

1. Determinación del tribunal internacionalmente competente en materia de transferencias internacionales de datos de carácter personal ilícitas

86. Dos son las cuestiones que debemos abordar con carácter previo al estudio de los criterios atributivos de competencia judicial internacional ante un litigio derivado de una transferencia internacional de datos de carácter personal ilícita: *1)* la calificación jurídica del supuesto de hecho: la lesión del derecho a la protección de datos derivada de una transferencia internacional de datos; y *2)* el marco normativo español regulador para la determinación del tribunal internacionalmente competente.

1. Tratamiento ilícito de datos de carácter personal, derecho a indemnización, y su calificación en Derecho internacional privado

87. Son varias las cuestiones que debemos abordar en este apartado: ***a)*** la importancia que desde la perspectiva del Derecho internacional privado tienen las transferencias internacionales de datos personales; ***b)*** los supuestos en función de que la persona afectada se dirija contra el responsable promotor/exportador y/o contra el responsable receptor/importador de los datos de carácter personal; ***c)*** la exigencia de responsabilidad civil objetiva extracontractual, derivándose el derecho a indemnización del afectado por el tratamiento de sus datos, al que le han provocado daño o lesión del tratamiento ilícito de sus datos; ***d)*** la identificación de los dos tipos de litigios que se pueden plantear atendiendo a las partes intervinientes: perjudicado y exportador/importador de datos; y ***e)*** la calificación de la pretensión.

a. Transferencias internacionales de datos de carácter personal y Derecho internacional privado

88. Las combinaciones son múltiples. Las nuevas tecnologías han multiplicado en los últimos años la transferencia de datos de carácter personal de un país a otro, donde son objeto de tratamiento, para posteriormente ser devueltos al país de origen o vendidos a empresas que operan en otros países. Es frecuente que los datos personales circulen de un país a otro con el objetivo de *escapar* a la aplicación de determinadas Leyes nacionales más estrictas en lo que afecta a su tratamiento.

89. A pesar de la actualidad e importancia práctica del tema, por el contrario, falta en la doctrina un estudio completo de los numerosos problemas que plantean las transferencias internacionales de datos de carácter personal desde la perspectiva del Derecho internacional privado.[153] En particular, un trabajo que responda a la siguiente pregunta: ¿el régimen de competencia judicial internacional garantiza la tutela del afectado ante un tratamiento ilícito internacional de datos de carácter personal?

[153] Podemos destacar tan sólo un par de estudios específicos sobre las operaciones de tratamiento internacional de datos personales y sobre el régimen jurídico aplicable a la transferencia internacional de datos de carácter personal: Vicente GUASCH PORTAS, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, 2014; Diana SANCHO VILLA, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010; y Diana SANCHO VILLA, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003.

b. Aplicación territorial del procedimiento de tutela que administra la AEPD: el artículo 18 de la LOPD

90. Una transferencia internacional de datos de carácter personal típica presenta tres operaciones de tratamiento: *1)* la que supone la puesta disposición de los datos por el primer empresario, siempre responsable del tratamiento (p. ej., la captación de los datos); *2)* la que implica el acto de transmisión de esos datos al extranjero por el promotor/exportador; y, también, *3)* el tratamiento de los mismos que realiza el empresario receptor/importador en su establecimiento en el extranjero. El legislador español utiliza los términos de *exportador/importador* para referirse a los empresarios en el contexto de una transferencia internacional de datos a un tercer Estado. Cuando la transmisión se produce dentro de la UE, el término genérico es *responsable* para referirse al que promueve una cesión de datos personales respecto de otro responsable o celebra un contrato de acceso con un encargado. Así, independientemente del destino geográfico de la transferencia internacional de datos (dentro o fuera de la UE), utilizaremos los términos de «responsable promotor o exportador» y «responsable receptor o importador».

91. En cuanto al ámbito de aplicación territorial del procedimiento de tutela que administra la AEPD en el artículo 18.2 de la LOPD, podemos distinguir tres supuestos, en función de que la persona afectada se dirija contra el responsable promotor/exportador y/o contra el responsable receptor/importador de los datos de carácter personal:

– ***Supuesto 1:*** Exportador de los datos, que en el marco de una transferencia internacional de datos, impide el ejercicio de los derechos de acceso, rectificación, cancelación y oposición: el afecta-

do podrá iniciar el procedimiento de tutela ante la autoridad de protección de datos correspondiente de ese Estado.

- ***Supuesto 2:*** Tutela contra el receptor/importador de los datos establecido en la UE o en un tercer Estado con un nivel de protección adecuado: el afectado deberá solicitar tutela ante la autoridad de protección de datos correspondiente de ese Estado miembro de la UE. En este segundo supuesto (tercer Estado con un nivel de protección adecuado) el procedimiento de tutela será el que administre la autoridad garante competente en el país extranjero.
- ***Supuesto 3:*** Reclamación contra el receptor/importador de los datos establecido en un tercer Estado: el afectado deberá solicitar tutela ante la autoridad de protección de datos correspondiente de ese tercer Estado.

c. Derecho a indemnización: el artículo 19 de la LOPD

92. El punto de partida es la realización de un tratamiento ilícito de datos. Consecuentemente, existirá daño y, por tanto, posible reclamación si se verifica que se ha producido un tratamiento ilícito internacional de datos de carácter personal. De esta forma, la vulneración del derecho a la protección de datos, en los supuestos de transferencia internacional de datos trae como resultado la exigencia de responsabilidad civil objetiva extracontractual, derivándose el derecho a indemnización del afectado por el tratamiento de sus datos, al que le han provocado daño o lesión del tratamiento ilícito de sus datos.[154] Desde

[154] Derecho a indemnización calificado de «sorprendente» por algún sector doctrinal muy autorizado en la materia. *Vid.* Javier APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 2.ª ed., Aranzadi, Elcano (Navarra), 2002, p. 167.

un punto de vista sustantivo, según establece el artículo 19.1 de la LOPD[155] —*ex* art. 17.3.º de la LORTAD—, «los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley [Orgánica de Protección de Datos de carácter Personal] por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados».[156] Es más, en virtud del *ex* artículo 3.2 del Real Decreto 1332/1994, en caso de incumplimiento, el cedente (exportador) y el cesionario (importador) de los datos responderán solidariamente.[157]

---

155 Este precepto viene a coger la responsabilidad civil extracontractual o aquiliana de los artículos 1902 y 1903 de nuestro Código Civil. Este tipo de responsabilidad es de aplicación cuando el daño se haya producido por los ficheros de titularidad privada, en aquellos supuestos en los que no existe una relación entre los interesados, perjudicado y responsable, sino que se trata de «dos personas entre las que nace el derecho y obligación de indemnizar como consecuencia de actos del responsable en los que no ha intervenido la voluntad del perjudicado». Javier APARICIO SALOM, *Estudio...*, *op. cit.*, p. 167; «ya que en aquellos supuestos en los que exista una previa relación jurídica entre el interesado y el responsable o encargado, la obligación de indemnizar dimanará del propio contrato, en cuanto se hayan incumplido las obligaciones en él estipuladas». Lucrecio REBOLLO DELGADO y M.ª Mercedes SERRANO PÉREZ, *Introducción a la protección de datos*, Dykinson, Madrid, 2006, p. 52.

156 El artículo 19 de la LOPD es el *heredero directo* de los artículos 22 y 23 de la Directiva 95/46/CE. *Vid.* sobre la exégesis de los mencionados artículos, Enrique COLLADO GARCÍA-LAJARA, *Protección de datos de carácter personal. Legislación, Comentarios, Concordancias y Jurisprudencia*, Dykinson, Madrid, 2000, pp. 49-52; Manuel HEREDERO HIGUERAS, *La directiva comunitaria de protección de los datos de carácter personal: Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos*, Aranzadi, Pamplona, 1997, pp. 181-183; y Antonio RUIZ CARRILLO, *La protección de los datos de carácter personal*, Bosch, Barcelona, 2001, pp. 107-113.

157 La articulación de la responsabilidad solidaria cedente-cesionario plantea algunos problemas: *a)* de índole legal, al articularse esta responsabilidad cuasi-

El artículo 19 de la LOPD, aunque es heredero del artículo 23 de la Directiva 95/46/CE, no recoge la indicación contenida en el apartado 2 del mencionado artículo 23 de la Directiva 95/46/CE, donde se establece que el «responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño».[158]

La lectura del propio artículo 23 de la de la Directiva 95/46/CE induce a confusión: ¿el legislador comunitario ha optado por introducir un sistema de responsabilidad objetiva o subjetiva? Parece que deja a los Estados miembros a que apliquen sus propias reglas de Derecho común en la materia,[159] lo que, en el caso español, se traduce en la exigencia de responsabilidad civil objetiva extracontractual que prevé el artículo 19 de la LOPD.

93. Los requisitos para que se pueda exigir esta responsabilidad civil obteniendo la reparación de los daños morales y patrimoniales son: *1)* que se acredite el incumplimiento del contenido de la LOPD; y *2)* que

objetiva en una norma de rango reglamentario; *b)* de índole jurídico, ante el ejercicio de la acción de responsabilidad del afectado contra el cesionario, que se encuentre en un país extranjero; y, *c)* de índole práctico, cuando se pretenda determinar la responsabilidad del cedente cuando el incumplimiento deriva de la conducta del cesionario. *Vid.,* en el mismo sentido, Miguel VIZCAÍNO CALDERÓN, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001, p. 371.

158 *Vid.* Diana SANCHO VILLA, *Transferencia internacional...*, op. cit., p. 221.

159 Tal y como se deduce, a nuestro modo de ver, del Considerando 55.º de la propia Directiva 95/46/CE, cuando señala que el responsable «sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor». *Vid.*, en el mismo sentido, Diana SANCHO VILLA, *Transferencia internacional...*, *op. cit.*, p. 222.

no concurra una causa de exoneración de la responsabilidad, se vincule el incumplimiento con el daño o lesión sufrió en los bienes o derechos, el daño o lesión se evalúe, la actuación o la falta de actuación generadora del daño no represente la materialización de los elementos de un tipo penal, pues entonces estaríamos ante la comisión de un delito y no frente a un ilícito penal.[160]

Para que el perjudicado por una transferencia internacional de datos ilícita exija una indemnización por daños y perjuicios se deben aunar, entonces, tres elementos: *a)* la existencia de un daño moral y/o económico, como consecuencia de la lesión del derecho fundamental a la protección de datos de una persona física en los supuestos de transferencia internacional de datos; *b)* que se haya producido un incumplimiento de la ley aplicable en materia de protección de datos de carácter personal; y, *c)* que no exista relación entre los interesados, responsable y afectado, sino que se trate de dos personas entre las que nace el derecho y obligación de indemnizar, como consecuencia de actos del responsable/s en los que no ha intervenido la voluntad del afectado.[161]

---

[160] *Vid.* Rafael VELÁZQUEZ BAUTISTA, *100 interrog@ntes...*, *op. cit.*, p. 37; además, en general, en relación sobre la responsabilidad civil contractual y extracontractual, *Vid.* Mariano YZQUIERDO TOLSADA, *Sistema de responsabilidad civil contractual y extracontractual*, Dykinson, Madrid, 2001; y, en particular, sobre la acción de responsabilidad civil derivada de un tratamiento automatizado de datos de carácter personal (jurisdicción, legitimación, *petitum*, prescripción y caducidad), *Vid.* Pedro GRIMALT SERVERA, *La Responsabilidad civil en el tratamiento automatizado de datos personales*, Comares, Granada, 1999; y, María E. ROVIRA SUEIRO, *La Responsabilidad civil derivada de los daños ocasionados al derecho al honor, a la intimidad personal y familiar y a la propia imagen*, Cedecs, Barcelona, 1999.

[161] En el caso de que entre el afectado y el/los responsable/s exista alguna relación jurídica, de cuyo incumplimiento se deriven los perjuicios, la obligación de in-

d. Supuestos

94. La determinación del tribunal internacionalmente competente para conocer de un litigio privado derivado de la vulneración del derecho a la protección de datos en supuestos de transferencia internacional de datos promovida desde España existirá, desde la posición procesal del afectado, e, independientemente de que se produzca entre dos responsables del tratamiento de datos de carácter personal (p. ej., en casos de transferencia internacional de datos entre empresas de un mismo grupo con destino último a la sede central del grupo) o aquel en que la transferencia se desarrolla entre un responsable y un encargado establecido en el extranjero (p. ej., en operaciones de marketing o de gestión de ficheros). Generalmente, se pueden plantear dos tipos de litigios, atendiendo a las partes intervinientes: perjudicado y exportador/importador de datos: *a) **reclamación del perjudicado contra el promotor/exportador de datos de carácter personal;*** y, *b) **reclamación del perjudicado contra el receptor/importador de datos de carácter personal.***[162]

e. Calificación de la pretensión

95. El daño derivado de la intromisión ilegítima en el derecho a la protección de datos, manifestado en el uso indebido o ilegítimo de los datos de una persona física, como consecuencia de una transferencia internacional de datos, como ya se ha señalado en el capítulo anterior,

---

demnizar tendrá carácter contractual, derivada del incumplimiento de lo pactado. *Vid.* Javier APARICIO SALOM, *Estudio sobre..., op. cit.*, p. 167.

[162] *Vid.* Diana SANCHO VILLA, *Transferencia internacional...*, op. cit., p. 224.

puede recibir una calificación *contractual*, o *extracontractual*, sobre la base de la existencia o no de una vinculación jurídica entre el transmitente y el afectado. Evidentemente, nos encontraremos en el ámbito de la responsabilidad civil contractual cuando entre el autor y la víctima hubiere existido una previa relación contractual y se hubiere producido un incumplimiento de lo pactado; mientras que la ausencia de vínculo contractual traerá como consecuencia la asunción de la responsabilidad civil extracontractual, materializada en la exigencia de una indemnización por los daños y perjuicios ocasionados. En el presente trabajo sólo nos ocuparemos de los daños derivados de intromisiones ilegítimas en el derecho a la protección de datos que integran supuestos generadores de responsabilidad civil extracontractual.

2. Marco normativo regulador en competencia judicial internacional y determinación del tribunal internacionalmente competente en transferencias internacionales de datos de carácter personal

96. Entre los resultados de la armonización internacional en el ámbito de la protección de datos no se incluye la formulación de reglas sobre competencia judicial internacional. De esta forma, la determinación de la competencia judicial internacional en materia de reclamaciones por la vulneración del derecho a la protección de datos derivadas de una transferencia internacional de datos de carácter personal conduce a un laberinto normativo, de intrínseca complejidad, ya que se acumulan fuentes de origen diverso –institucional o comunitario,[163] convencio-

[163] Nos referimos, hoy día, al Derecho de la UE.

nal y autónomo— a las que debemos acudir: *1.º)* al *limitado*[164] Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Bruselas, el 27 de septiembre de 1968 (en lo sucesivo, CB); *2.º)* a su paralelo, el Convenio de «Lugano II», de 30 de octubre de 2007, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil[165] (en lo sucesivo, CL II), sustituto directo del Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Lugano, el 16 de septiembre de 1988;[166] *3.º)* al Tratado bilateral entre el Reino de España y la República de El Salvador sobre competencia judicial, reconocimiento y ejecución de sentencias en materia civil y mercantil (en adelante, Tratado España-República de El Salvador);[167] *4.º)* al Reglamento (CE) núm. 44/2001, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil —Reglamento «Bruselas I»— (a partir de ahora, RB);[168,169] o, *5.º)* a la Ley Orgánica 6/1985, de 1 de

[164] El CB se aplica, en la actualidad, únicamente con relación a los Territorios Franceses de Ultramar y a las Antillas holandesas.

[165] *DOUE* L 339, de 21 de diciembre de 2007. Este texto convencional entró en vigor el 01/01/2010. Son Estados parte: los Estados miembros de la UE, incluido Dinamarca (desde el 01/01/2010), Noruega (desde el 01/01/2010), Suiza (desde el 01/01/2011), e Islandia (desde el 01/05/2011). El CL II es de aplicación a los países del territorio «Bruselas I», y a los de la AELC no pertenecientes a la UE, excluyendo a Liechtenstein.

[166] *BOE* núm. 243, de 10 de octubre de 1979.

[167] *BOE* núm. 256, de 25 de octubre de 2001.

[168] *DOCE* 2001 L 12/1. El ámbito de aplicación del RB incluye a los Estados miembros de la UE.

[169] Modificado por el Reglamento (UE) núm. 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el

julio, del Poder Judicial (en adelante, LOPJ).[170] La aplicación de un instrumento jurídico u otro dependerá fundamentalmente del domicilio del demandado.

97. Los foros de competencia judicial internacional se concretan a partir de la naturaleza jurídica de la acción y partiendo del criterio del domicilio. De tal manera que existen foros que no tienen en cuenta el domicilio de las partes y foros que tienen en cuenta tal domicilio (en particular, el del demandado) para la aplicación de estos instrumentos normativos de determinación de la competencia judicial internacional.

La estructura de los foros de competencia judicial internacional del CB, del CL 11, del Tratado España-República de El Salvador, y del RB,[171] se construye sobre tres niveles jerarquizados: *a)* el primer nivel está constituido por las denominadas «competencias exclusivas», previstas en los artículos 22 del RB/CL 11,[172] 16 del CB o 3 del Tratado España-República de El Salvador. En determinadas materias, este precepto atribuye competencia única y exclusiva a los tribunales de un Estado, excluyendo absolutamente la posibilidad de que conozcan cualesquiera otros tribunales. Si se trata de una de las materias previs-

reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil —Reglamento «Bruselas 1 bis»— (*DOUE* L 351/1 de 20/12/2012), que será aplicable a partir del 10 de enero de 2015; modificado por el Reglamento (UE) núm. 542/2014 del Parlamento y del Consejo, de 15 de mayo de 2014, por el que se modifica el Reglamento (UE) núm. 1215/2012 en lo relativo a las normas que deben aplicarse por lo que respecta al Tribunal Unificado de Patentes y al Tribunal de Justicia del Benelux (*DOUE* L 163 de 29/05/2014).

170 *BOE núm.* 157, de 2 de julio de 1985.

171 Y del Reglamento «Bruselas 1 bis».

172 Art. 24 en el Reglamento «Bruselas 1 bis».

tas en los artículos 22 del RB/CL II,[173] 16 del CB o 3 del Tratado España-República de El Salvador, el tribunal del Estado competente de oficio controlará su competencia, excluyendo la posibilidad de que otros tribunales pudieran declararse competentes para conocer del mismo litigio; *b)* si no se trata de una de las materias previstas en el artículo 22 del RB/CL II,[174] 16 del CB o 3 del Tratado España-República de El Salvador, es preciso recurrir al segundo escalón en el orden jerárquico: al principio de autonomía de la voluntad. La voluntad de las partes, prevista en el artículo 23 del RB/CL II,[175] 17 del CB o 5.2 del Tratado España-República de El Salvador atribuye competencia exclusiva a los tribunales designados por las partes («sumisión expresa»). No obstante, el acuerdo de sumisión a los tribunales de un Estado siempre puede ser modificado, tácitamente, mediante la «sumisión tácita» por ambas partes a otros tribunales (arts. 24 del RB/CL II,[176] 18 del CB o 5.1 del Tratado España-República de El Salvador); y, finalmente, *c)* el tercer escalón jerárquico de las reglas de competencia judicial internacional opera en defecto de sumisión expresa o tácita por las partes, y siempre que no se trate de una de las materias objeto de competencias exclusivas. En tales casos, serán competentes, indistintamente, los tribunales del «domicilio del demandado» (art. 2 del RB/CL II,[177] del CB o 2 del Tratado España-República de El Salvador); y/o, los designados por los foros especiales de competencia («compe-

[173] Art. 24 en el Reglamento «Bruselas I bis».
[174] Art 24 en el Reglamento «Bruselas I bis».
[175] Art 25 en el Reglamento «Bruselas I bis».
[176] Art 26 en el Reglamento «Bruselas I bis».
[177] Art 4 en el Reglamento «Bruselas I bis».

tencias especiales») previstos en el artículo 5 del RB/CL II,[178] del CB o 4 del Tratado España-República de El Salvador.

Por último, debemos acudir a la LOPJ, que, en su artículo 22, recoge las normas de competencia judicial internacional aplicables para que un órgano jurisdiccional español se declare competente, ante la imposibilidad de aplicación del RB/CL II[179], del CB o del Tratado España-República de El Salvador. La LOPJ recoge en su artículo 22.1, en primer término, una serie de foros de competencia que presentan «carácter exclusivo» y que se inspiran y coinciden en buena medida con los previstos en el artículo 16 del CB/CL o 3 del Tratado España-República de El Salvador. El artículo 22.2 recoge dos foros generales que atribuyen competencia a los órganos jurisdiccionales, cualquiera que sea la materia afectada: sumisión a los Juzgados o Tribunales españoles y domicilio del demandado en España. Por último, el artículo 22.3 recoge diversos foros de competencia, que nos recuerdan a las «competencias especiales» del artículo 5 del RB/CL II y del CB.

98. En el presente trabajo, como ya se ha indicado, nos centraremos en el siguiente supuesto de hecho: la reclamación por daños y perjuicios por la persona afectada (titular del derecho a la protección de datos) ante el tratamiento ilícito internacional de sus datos de carácter personal.

Una vez determinado el domicilio del demandado, en aplicación del RB,[180] del CL II, del CB o del Tratado España-República de El Salvador, los criterios atributivos de competencia serían los siguientes: *a)*

---

178 Art 7 en el Reglamento «Bruselas I bis».

179 Y del Reglamento «Bruselas I bis».

180 Modificado por el Reglamento «Bruselas I bis».

el foro de la sumisión, expresa o tácita, que nos permite concentrar los litigios a los que las partes se refieran, bajo el conocimiento de los tribunales de un solo país; *b)* el foro del domicilio del demandado, esto es, los tribunales del país donde esté domiciliado el «presunto vulnerador-demandado» conocerá de todas las pretensiones que se deduzcan contra él, independientemente del país o países en los que se haya producido el hecho dañoso; y/o, *c)* el foro del lugar del hecho dañoso, que atribuye competencia a los tribunales del «lugar donde se hubiere producido o pudiere producirse el hecho dañoso» del que nace la responsabilidad extracontractual, pudiendo considerarse como «país donde ocurre el hecho dañoso» tanto el país donde ocurre el hecho causal como el país donde se verifica el resultado lesivo, esto es, en nuestro caso, el país donde radica el fichero de datos de carácter personal.

2. Litigios derivados de una transferencia internacional de datos de carácter personal ilícita: prórroga de la competencia (sumisión expresa o tácita)

99. Debemos comenzar el estudio de los foros de competencia judicial internacional prestando especial atención a la prórroga de la competencia judicial internacional. Así, en primer lugar, me ocuparé de la sumisión expresa de las partes a favor de los tribunales de un determinado Estado (A); para, en segundo lugar, referirme a la sumisión tácita de las partes a favor de los tribunales de un determinado Estado para la resolución de un litigio derivado de una transferencia internacional de datos de carácter personal ilícita (B).

A. Sumisión expresa de las partes a favor de los tribunales de un determinado Estado

100. El acuerdo de sumisión es un pacto entre las partes de una relación jurídica en cuya virtud éstas determinan el órgano jurisdiccional que será competente para conocer de los litigios que eventualmente pudieran surgir como consecuencia de ciertas obligaciones asumidas por las partes.

La sumisión puede realizarse mediante acuerdo expreso (arts. 23 del RB/CL II,[181] 17 del CB o 5.2 del Tratado España-República de El Salvador) o, como veremos más adelante, mediante acuerdo tácito: la realización de ciertas prácticas que denotan la voluntad de las partes de someterse a los tribunales de un determinado país (arts. 24 del RB/CL II,[182] 18 del CB o 5.1 del Tratado España-República de El Salvador).

101. Si bien este foro de competencia constituye una alternativa a considerar de forma muy positiva ya que presenta grandes ventajas pues ofrece un elevado nivel de previsibilidad, seguridad jurídica y confianza a las partes. También favorece los intereses del comercio internacional, pues fomenta, lógicamente, las transferencias internacionales de datos de carácter personal, en la medida en que: *a)* por un lado, las cláusulas de elección de foro permiten a las partes someter sus controversias a los tribunales que se adaptan mejor a sus intereses; y, *b)* por otro, incrementan la seguridad jurídica que reclaman las transacciones comerciales internacionales: eliminan la incertidumbre

[181] Art 25 en el Reglamento «Bruselas I bis».

[182] Art 26 en el Reglamento «Bruselas I bis».

sobre la jurisdicción competente que se origina por la conexión de una relación jurídica internacional con varios ordenamientos; la importancia de este foro de competencia judicial internacional en el ámbito de la responsabilidad extracontractual (en particular, en los litigios consecuencia de la lesión del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita) en la práctica es muy limitada, pues, normalmente, las partes implicadas en litigios de este tipo no acuerdan dónde litigar.

La razón fundamental se encuentra, precisamente, en la dificultad en alcanzar un acuerdo entre las partes en esta cuestión, no sólo una vez surgido el litigio —*a posteriori*— sino mucho menos antes de que surja la posible controversia —*a priori*—. En la medida que, por definición, la responsabilidad civil extracontractual surge sin que previamente exista una relación entre las partes. Es claro el limitado juego de la sumisión expresa como fuero de competencia internacional cuando la responsabilidad es extracontractual, aunque no puede descartarse la incidencia de un posible acuerdo tácito (que, como sabemos, prevalece en cualquier caso sobre la sumisión expresa).

102. Aunque en los supuestos de transferencias internacionales de datos de carácter personal desde España al extranjero el requisito de la domiciliación en un Estado miembro de al menos una de las partes se da en la gran mayoría de los casos, en breve este requisito dejará de ser un *posible problema* ya que el Reglamento «Bruselas I bis», en su artículo 25.1, elimina la exigencia, prevista en el artículo 23.1 del RB como presupuesto de su aplicación, de que al menos una de las partes tuviere su domicilio en un Estado miembro, lo que va unido también a la supresión del párrafo 3 del mencionado artículo 23; tras la modificación no resultará necesario prever un tratamiento diferenciado para los casos en los que ninguna de las partes que han cele-

brado el acuerdo esté domiciliada en un Estado miembro. En consecuencia, en el marco del nuevo Reglamento la eficacia atributiva de competencia (al tribunal o tribunales del Estado miembro designado) y la eficacia derogatoria de la competencia (de los tribunales de los Estados miembros no designados) derivada del artículo 25 se proyecta sobre los acuerdos de prórroga de competencia incluso si ninguna de las partes está domiciliada en un Estado miembro.[183]

Sin embargo, no se exigirá, con carácter general, que entre el país al que pertenece el Estado elegido por las partes y la relación de la que deriva el litigio exista un vínculo concreto o un elemento objetivo de conexión, lo que permite a las partes elegir un foro neutral o una mayor experiencia en reclamaciones derivadas de la lesión del derecho a la protección de datos.

103. Con el Reglamento «Bruselas I bis» la cuestión de si un acuerdo de sumisión expresa en favor de los órganos jurisdiccionales, o de un concreto órgano jurisdiccional, de un Estado miembro es nulo de pleno derecho en cuanto a su validez material se decidirá de acuerdo con el Derecho del Estado del órgano, u órganos, jurisdiccional designados en el acuerdo, incluidas las normas de conflictos de dicho Estado miembro.[184] El nuevo artículo 25.1 del Reglamento incorpora una regla de conflicto uniforme, según la cual la validez material de los

---

183 *Vid.* Pedro A. De Miguel Asensio, «El nuevo Reglamento sobre competencia judicial y reconocimiento y ejecución de resoluciones», en *Diario La Ley*, núm. 8013, Sección Tribuna, 31 de enero de 2013, Año XXXIII, editorial La Ley, p. 6.

184 Considerando 20.º del 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.

acuerdos de prórroga de competencia se rige por la ley del Estado miembro designado.[185]

104. La validez de ese acuerdo atributivo de competencia exige la prueba del consentimiento efectivo entre las partes sobre el caso concreto: la sumisión debe hacerse por escrito;[186] en este sentido, el RB[187] (y el CL 11/CB, o el Tratado España-República de El Salvador) sensible con su adaptación al entorno de Internet, admite la formalización de la sumisión expresa por medios electrónicos; esto es, la elección *on line* del tribunal competente, siempre que se encuentre en el territorio cubierto por la aplicación del RB[188] (o, del CL 11/CB); y, se garantice la existencia del consentimiento de las partes en orden a la elección del tribunal competente. Así, p. ej., en el marco de una transferencia internacional de datos de carácter personal, la elección del mismo podrá efectuarse, según el caso, mediante intercambio de emails.

a. Cláusulas de elección de foro a favor de tercero: Decisiones de la Comisión Europea y Binding Corporate Rules

105. Las cláusulas de elección a favor de tercero serán válidas únicamente en litigios por vulneración del derecho a la protección de datos derivado de una transferencia internacional de datos de carácter personal ilícita siempre que sean de origen contractual. Por tanto, en

---

185 *Vid.* Pedro A. De Miguel Asensio, «El nuevo Reglamento...», *op. cit.*, p. 6.

186 *Vid.*, en general sobre la validez de las cláusulas atributivas de competencia en el comercio electrónico, Pedro A. De Miguel Asensio, *Derecho privado de Internet*, 3.ª ed., Civitas, Madrid, 2002, pp. 448-455.

187 Y del Reglamento «Bruselas I bis».

188 Y del Reglamento «Bruselas I bis».

reclamaciones extracontractuales difícilmente podemos recurrir al artículo 23 del RB/CL ll, al artículo 17 del CB o al artículo 5.2 del Tratado España-República de El Salvador.

Los acuerdos de elección de foro en este ámbito tienen un claro reflejo en las cuatro Decisiones dictadas por la Comisión Europea dictadas hasta la fecha, tendentes a clarificar el clausulado contractual en esta materia.[189] Podemos establecer dos grupos, en función de la clase de competencia judicial internacional que establecen: *a)* las que establecen una Competencia judicial internacional *indirecta* (las Decisiones 2001/497/CE y 2004/915/CE) y *b)* las que establecen Competencia judicial internacional *directa* (las Decisiones 2002/16/CE y 2010/87/UE). Veamos cada una de ellas:

*a) **Competencia judicial internacional indirecta:*** las Decisiones 2001/497/CE y 2004/915/CE:

i) **Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE:**[190]

> V. Resolución de conflictos con los interesados o con la autoridad
> [...]
> *c)* Cada una de las partes se compromete a acatar cualquier decisión de los *tribunales competentes* o de la autoridad *del país de establecimiento del exportador de datos* cuyas decisiones sean finales y contra la que no pueda entablarse recurso alguno.

---

189 *Vid.,* en relación con el régimen aplicable a la posición del interesado en el contrato que reglamenta una transferencia internacional de datos y las cláusulas tipo existentes a nivel comunitario y autónomo, Diana SANCHO VILLA, *Transferencia internacional..., op. cit.*, pp. 230-236.

190 *DOCE* L 181/19, de 4 de julio de 2001.

ii) **Decisión 2004/915/CE de la Comisión, de 27 de diciembre, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países:**[191]

> V. Resolución de conflictos con los interesados o con la autoridad
> [...]
> *c)* Cada una de las partes se compromete a acatar cualquier decisión de los *tribunales competentes* o de la autoridad *del país de establecimiento del exportador de datos* cuyas decisiones sean finales y contra la que no pueda entablarse recurso alguno.

b) Competencia judicial internacional directa: las Decisiones 2002/16/CE y 2010/87/UE.

iii) **Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE:**[192]

> Cláusula 7. Mediación y jurisdicción
> 1. El importador de datos acuerda que si el interesado invoca en su contra derechos de tercero beneficiario y/o reclama una indemnización por daños y perjuicios con arreglo a las cláusulas, aceptará la decisión del interesado de:
> [...]
> *b)* someter el conflicto a los *tribunales del Estado de establecimiento del exportador de datos*.

[191] *DOCE* L 385/74, de 29 de diciembre de 2004.

[192] *DOCE* L 6/52, de 10 de enero de 2002.

iv) **Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo:**[193]

> Cláusula 7
> **Mediación y jurisdicción**
> 1. El importador de datos acuerda que, si el interesado invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios con arreglo a las cláusulas, aceptará la decisión del interesado de:
> *a)* someter el conflicto a mediación por parte de una persona independiente o, si procede, por parte de la autoridad de control;
> b) *someter el conflicto a los tribunales del Estado de establecimiento del exportador de datos.*
> 2. Las partes acuerdan que las opciones del interesado no obstaculizarán sus derechos sustantivos o procedimentales a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.

La apuesta de las BCR por el recurso a la vía jurisdiccional como mecanismo de resolución de controversias (***Competencia judicial internacional directa)*** es también clara (y circunscrita sólo al ámbito de la responsabilidad contractual). Vamos a comprobarlo:

i) **WP 74 (11639/02/EN):**

> ***5.6. Rule on jurisdiction.***
>
> *As explained above in chapter 5.5.2., the corporate group must also accept that data subjects would be entitled to take action against the corporate group, as well as to choose the jurisdiction:*

[193] *DOCE* L 39/5, de 12 de febrero de 2010.

a) either in the jurisdiction of the member that is at the origin of the transfer, *or*

b) in the jurisdiction of the European headquarters or the jurisdiction of the European member with delegated data protection responsibilities.

Assuming the proper functioning of the system which implies a good level of compliance throughout the group, regular audits, efficient complaint handling, cooperation with data protection authorities, etc. the involvement of the courts seems unlikely, but in any case cannot be excluded. Having said that, only experience with these instruments will tell us if such forecast is right.

ii) WP 154 (1271-00-01/08/EN):

18. Third party beneficiary rights.

A clear statement that the BCR grant rights to data subjects to enforce the rules as third-party beneficiaries. The rights should cover the judicial remedies for any breach of the rights guaranteed and the right to receive compensation (see articles 22 and 23 of the EU Directive).

A statement that the data subjects can choose to lodge claims before:

– The jurisdiction of the data exporter located in the EU, *or*
– The jurisdiction of the EU headquarters/the EU Member with delegated responsibilities, *or*
– *Before the competent Data Protection Authorities.*

A commitment that all data subjects beneficiating from the third party beneficiary rights should also have easy access to this clause.

Como vemos, se puede optar por darle la competencia judicial internacional a los tribunales del Estado de establecimiento del *origen de la transferencia internacional de datos* o dejarla en manos de los tribunales del Estado del lugar donde radique la *European headquarters* (Autoridad Europea Supervisora de la BCR).

Además, en una transferencia internacional de datos contractual promovida desde España (exportador domiciliado en España) y existiendo sumisión a los tribunales de un Estado miembro (españoles) los efectos son tanto prorrogatorio cuanto derogatorio. Si el terce-

ro/afectado platea su demanda ante los tribunales españoles, en virtud de la cláusula, estos serán competentes (efecto prorrogatorio) y otros no podrán conocer el litigio en cuestión (efecto derogatorio). Sin embargo, si el mismo presenta la demanda ante otros tribunales, estos serán, en principio, competentes sin que se pueda hacer valer por promotor/exportador y receptor/importador el acuerdo de sumisión.

b. Cláusulas atributivas de competencia en transferencias internacionales de datos entre responsables del tratamiento o a un encargado

106. Los contratos que documentan transferencias internacionales de datos de carácter personal son susceptibles de incorporar, con carácter facultativo, cláusulas atributivas de competencia judicial internacional para resolver las reclamaciones que el interesado desee interponer contra los empresarios implicados donde solicite la reparación de un daño causado (vulneración del derecho a la protección de datos derivado de una transferencia internacional de datos de carácter personal ilícita).[194]

Conviene distinguir dos supuestos:

a) Transferencias internacionales de datos de carácter personal entre responsables del tratamiento: en estos casos el afectado (titular del derecho a la protección de datos vulnerado derivado de una transferencia internacional de datos de carácter personal ilícita) para ser resarcido como tercero beneficiario por cualquier incumplimiento estipulado en el contrato en el que hubieran incurrido estos (si ambos acuerdan ser responsables solidarios) puede

[194] *Vid.* Diana SANCHO VILLA, *Transferencia internacional...*, *op. cit.,* pp. 239-242.

dirigirse indistintamente contra el exportador establecido en un Estado miembro (en las transferencias de España al extranjero, en España), contra el importador de los datos establecido en un tercer Estado, o contra ambos, frente a los tribunales españoles.

b) Transferencias internacionales de datos de carácter personal a un encargado: lo usual es que el afectado (titular del derecho a la protección de datos vulnerado derivado de una transferencia internacional de datos de carácter personal ilícita) se dirija contra el responsable del tratamiento de sus datos de carácter personal (exportador). No obstante, si las expectativas de protección del afectado se ven truncadas al desaparecer de hecho, dejado de existir o ser insolvente el responsable, aquel podrá dirigir su acción contra el importador de sus datos personales, frente a los tribunales españoles. Así, p. ej., si un afectado reclamara una indemnización por los daños sufridos por el tratamiento de sus datos por el importador que ha realizado en su establecimiento en EE.UU., ante los tribunales españoles, existen tres vías para asegurar este resultado: tratar de fundamentar la competencia (como veremos) en los criterios del artículo 22.3 de la LOPJ; intentar la vía de la acumulación de acciones contra el importador y el exportador de sus datos en el domicilio del exportador en un Estado miembro (cuando se dé, como veremos, las condiciones de aplicación del foro de competencia judicial internacional de la pluralidad de demandados), o bien, mediante una cláusula atributiva de competencia a favor de los tribunales del exportador a favor de tercero incluida en el oportuno contrato.[195]

---

[195] *Vid.* Diana SANCHO VILLA, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010, pp. 240-242.

107. En principio, los efectos de los acuerdos atributivos de jurisdicción válidamente celebrados en el marco de litigio por vulneración del derecho a la protección de datos derivado de una transferencia internacional de datos de carácter personal ilícita, son *inter* partes. En virtud del acuerdo de sumisión *interpartes* se atribuye competencia judicial internacional a los tribunales elegidos, que serán los únicos competentes para conocer de la cuestión, lo que excluye, en principio, la competencia de los tribunales de los demás Estados parte; además, mediante el acuerdo de sumisión se excluye la competencia judicial internacional de cualquier otro tribunal que pudiera ser competente de no existir el acuerdo expreso de sumisión; en fin, la competencia judicial internacional determinada mediante el acuerdo de sumisión es *obligatoria* para las partes, salvo que un eventual y mutuo acuerdo posterior lo derogue.

108. Las reclamaciones que el afectado dirija contra el importador de sus datos que queden cubiertas por la cláusula atributiva de competencia existente *interpartes* fundamentaría su competencia judicial internacional en los foros generales. Eso sí, dicha cláusula atributiva de competencia a favor de tercero (afectado) no cubre las posibles reclamaciones que se dirijan entre sí exportador e importador de los datos personales del afectado; esto es, el exportador no podrá utilizar esta cláusula atributiva de competencia judicial internacional para demandar al importador ante los tribunales del Estado donde tenga su establecimiento.[196]

[196] *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.,* pp. 242-243.

109. No obstante, hay que tener presente que la sumisión expresa (y la tácita, que después examinaremos), aunque perfectamente disponible para las partes en los litigios que estamos examinando, es un foro muy poco utilizado, en supuestos de responsabilidad extracontractual, con carácter general. Y ello básicamente porque es muy difícil en la práctica que el afectado y el responsable alcancen un acuerdo de esta naturaleza, cuando se discute este tipo de supuestos, y aún menos de modo previo a la aparición de la controversia. Será poco habitual que las partes (autor y víctima de la lesión del derecho a la protección de datos) en los litigios derivados de una transferencia internacional de datos de carácter personal ilícita, se sometan a unos concretos tribunales y, lógicamente, menores serán las posibilidades de que esa sumisión sea expresa.

B. Sumisión tácita de las partes a favor de los tribunales de un determinado Estado

110. Se considera que existe *sumisión tácita*,[197] de acuerdo con el artículo 24 del RB/CL ll,[198] el artículo 18 del CB o el artículo 5.1 del Tratado España-República de El Salvador, la siguiente conducta pro-

[197] El foro del acuerdo de *sumisión tácita* para la determinación del Tribunal internacionalmente competente permite el ahorro de costes procesales y (al igual que con la *sumisión expresa)* que las partes decidan ante qué tribunal quieren litigar. *Vid*., en general, sobre el concepto, límites y requisitos de la sumisión tácita como foro de competencia judicial internacional, Alfonso-Luis Calvo Caravaca y Javier Carrascosa González, «La sumisión tácita como foro de competencia judicial internacional y el artículo 24 del Reglamento 44/2001, de 22 de diciembre 2000», en Alfonso-Luis Calvo Caravaca y Santiago Areal Ludeña, *Cuestiones actuales del Derecho mercantil internacional*. Madrid, 2005, pp. 203-215.

[198] Art. 26 en el Reglamento «Bruselas I bis».

cesal de las partes: cuando el demandante (afectado) presenta una demanda ante el tribunal de un Estado y la comparecencia del demandado (causante del daños) ante ese tribunal no tiene por objeto impugnar su competencia judicial. En tal caso, debe entenderse que las partes aceptan tácitamente someter el litigio a ese tribunal.

111. Si se presentara la demanda ante un tribunal, y el demandado compareciera y realizara cualquier acción que no fuera la impugnación de la competencia,[199] este tribunal sería competente con independencia del domicilio de las partes, siempre que la materia no fuera objeto de una competencia exclusiva.

112. La voluntad de las partes (afectado y exportador o importador) sometiéndose tácitamente a un tribunal de un Estado, al amparo del artículo 24 del RB/CL II,[200] del 18 del CB o 5.1 del Tratado España-República de El Salvador, prevalece sobre los acuerdos atributivos de jurisdicción concluidos al amparo del artículo 23 del RB/CL II,[201] 17 del CB o 5.2 del Tratado España-República de El Salvador. En cualquier caso, ante la existencia de un acuerdo de esta naturaleza, el alcance de esta elección tendrá los condicionamientos generales, sin especialidades, de forma que habrá de estar a cada caso concreto y

---

199 Para que no exista *sumisión tácita*, la impugnación de la competencia judicial internacional debe realizarse de acuerdo con las normas de Derecho procesal del Estado del foro (en el caso español, sería preciso interponer la declinatoria internacional de jurisdicción a que se refiere los artículos 63 y 64 de nuestra LEC), aunque se realice de forma subsidiaria una defensa sobre el fondo del asunto, siempre que ésta se presente al mismo tiempo o en un momento posterior a la declinatoria.

200 Art. 26 en el Reglamento «Bruselas I bis».

201 Art. 25 en el Reglamento «Bruselas I bis».

valorar el comportamiento del demandado en el proceso para afirmar si efectivamente existe una voluntad de someterse a esa jurisdicción estatal particular ante la que el demandante (titular del derecho a la protección de datos de carácter personal) ha presentado su demanda.

C. Recapitulación

113. Las vigentes normas de competencia judicial internacional, elaboradas en los distintos niveles normativos (institucional, convencional y autónomo), no sólo son claramente inadecuadas para proteger a la víctima de un tratamiento ilícito internacional de sus datos, sino que pueden incluso conducir a resultados contraproducentes. En primer lugar, el recurso a la autonomía de la voluntad resulta peligroso ante una situación de desequilibrio entre las partes; tal y como se pone de manifiesto en la existencia de foros de protección (contratos individuales de trabajo, contratos de seguro y contratos celebrados por consumidores) en los diferentes sistemas de Derecho internacional privado comparado. La posibilidad de que se produzca un supuesto de sumisión tácita (regulada en el artículo 24 del RB/CL ll, 18 del CB, 5.1 del Tratado España-República de El Salvador o 22.2 de la LOPJ) es difícilmente verificable en la práctica: primero, porque el damnificado tendrá una tendencia lógica a demandar ante los tribunales del lugar de su residencia (con ello se cumpliría el primer requisito para que se produzca la prorrogación tácita de fuero, es decir, plantear la demanda ante un tribunal que de otra forma no sería competente); segundo, porque parece evidente que el causante del daño, más que someterse a dichos tribunales, lo que haría sería impugnar su competencia, para no resultar enjuiciado por los tribunales de la contraparte.

114. En cualquier caso, si se produce la sumisión tácita es de suponer que el demandante (perjudicado) habrá realizado un cálculo previo de las posibilidades de éxito de su reclamación. Suposición que, dadas las características de los afectados y del conocimiento especializado que requiere el tratamiento de las situaciones privadas internacionales, dista mucho de coincidir con el estudio de campo realizado respecto de estas infracciones. La prorrogación expresa de fuero será, cuando menos, igual de difícilmente verificable que el supuesto de la sumisión tácita y, además, ciertamente peligroso para el perjudicado, dada la situación de desigual *bargaining power* en el que se encuentran las partes enfrentadas.

3. Litigios derivados de una transferencia internacional de datos de carácter personal ilícita en ausencia de pactos entre las partes

115. El recurso al principio de la autonomía de la voluntad es difícilmente verificable en la práctica. En ausencia de pactos entre las partes habrá que recurrir, en primer lugar, al foro general del domicilio del demandado. La primera cuestión que debemos clarificar es identificar al responsable del perjuicio: promotor o receptor de los datos de carácter personal objeto de una transferencia internacional (A); para, a partir de ahí, ocuparme de la determinación de su domicilio (B), resolver el problema de la pluralidad de demandados (C) y de las transferencias internacionales de datos de carácter personal realizadas por sucursales (D).

A. Identificación del responsable: promotor *vs.* receptor de datos de carácter personal

116. El domicilio del demandado en los litigios que estamos examinando puede configurarse como una nueva forma de ataque del demandante, una solución fácil, neutra y práctica. No obstante, esta atribución de competencia plantea algunas dificultades: en primer lugar, el recurso al foro general situaría al demandante (afectado) en la nada cómoda situación de tener que litigar en casa de su contraparte (exportador o importador), con lo que ello supone: desconocimiento del idioma, aumento de los costes, desconocimiento de las normas procesales aplicables, etc.; en segundo lugar, este foro general conduce a la designación de la jurisdicción competente en términos genéricos: tribunales españoles, alemanes, suizos, belgas, etc.; y, a partir de ahí, serán las normas de reparto territorial de la organización jurisdiccional correspondiente quienes deban designar el órgano jurisdiccional concreto ante el cual plantear la reclamación; y, finalmente, es un foro poco adecuado en los casos en que el presunto responsable (exportador o importador) actúa desde países lejanos o exóticos, de modo que el demandante (afectado) no conoce o puede no averiguar fácilmente el domicilio del demandado (exportador o importador).

117. El recurso al foro general del domicilio del demandado plantea tres problemas particulares:

– El primer problema surge, en numerosas ocasiones, cuando el afectado desconoce al causante del daño (da igual que sea el exportador o el importador de los datos personales), le resulta imposible saber quién es y menos en qué país está domiciliado. En estos casos, evidentemente, poco podemos hacer.

- El segundo problema añadido del foro del domicilio del demandado es más complejo y se produce cuando el exportador o el importador de los datos personales (demandado) se ha identificado con un *domicilio aparente*, diferente a su *domicilio real*. Ante este riesgo de confusión creado por el causante del daño (demandado) la solución debería pasar, en nuestra opinión, por permitir al afectado (demandante) demandar tanto ante los tribunales del Estado del *domicilio aparente*, cuanto del Estado del *domicilio real*.
- El tercer problema viene derivado de que el domicilio del demandado sólo opera en el momento de presentación de la demanda. Por ello, este foro puede facilitar ciertos comportamientos oportunistas del demandado: p. ej., *huir* de la UE evitando el foro del domicilio del demandado en un Estado participante del RB.[202] En estos casos, el demandante no tendría que venir obligado, única y exclusivamente, ante los tribunales del Estado extranjero donde tiene su domicilio el demandado, sino que podrían entrar en juego otros foros de competencia: el lugar de cumplimiento de la obligación litigiosa, los tribunales pactados previamente, o el domicilio del propio demandante.

B. DETERMINACIÓN DEL DOMICILIO DEL DEMANDADO.

118. En función del demandado ante quien presentemos la reclamación podemos diferenciar dos supuestos: por un lado, la reclamación contra el promotor de una transferencia internacional de datos de carácter personal; y, por otro lado, la reclamación contra el receptor de una transferencia internacional de datos de carácter personal.

[202] Y del Reglamento «Bruselas I bis».

a. Reclamación contra el promotor de una transferencia internacional de datos de carácter personal

119. Toda reclamación presentada por el afectado (establecido en España) contra el responsable promotor de una transferencia internacional de datos de carácter personal recaerá en los tribunales españoles del domicilio del responsable promotor. Así, p. ej., cuando éste transmitió los datos sin el consentimiento del afectado provocando un daño, o bien, lo hizo con su consentimiento pero no atendió su petición de rectificación de alguna información causándole un daño.[203]

120. La persona afectada podrá demandar al responsable del tratamiento establecido en nuestro país y promotor de una transferencia internacional de datos de carácter personal (exportador) por el foro general del domicilio del demandado en España (art. 2 del RB/CL 11/CB/[204] Tratado España-República de El Salvador) en la generalidad de los supuestos de transferencias internacionales de datos de carácter personal de España al extranjero, tanto si se trata de una transferencia internacional a un responsable del tratamiento cuanto si se trata de una transferencia internacional a un encargado, y con independencia de que el empresario receptor de los datos esté establecido en un tercer Estado o no.

La competencia recaerá en el tribunal español del domicilio del responsable promotor/exportador de los datos, p. ej., cuando éste transmitió los datos personales *a)* sin el consentimiento del afectado provocando el daño, o *b)* lo hizo con su consentimiento, pero no

---

[203] *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.,* p. 226.

[204] Art. 4 en el Reglamento «Bruselas I bis».

atendió su petición de rectificación de alguna información causándole un daño.

b. Reclamación contra el receptor de una transferencia internacional de datos de carácter personal

121. Cuando la reclamación contra el promotor de la transferencia internacional de datos de carácter personal en España es planteada por el responsable o encargado receptor/importador de los datos: la competencia corresponderá a los tribunales del Estado del domicilio del demandado (art. 2 del RB/CL 11/CB/[205] Tratado España-República de El Salvador).

El receptor (importador) de una transferencia internacional de datos de carácter personal, sea éste un responsable o un encargado, podrá ser demandado ante los tribunales del Estado miembro de su domicilio, conforme al artículo 2 del RB/CL 11/CB/[206] Tratado España-República de El Salvador. En las transferencias internacionales de datos de carácter personal dirigidas a países cuyo nivel de protección sea adecuado debemos distinguir, a su vez, dos supuestos: primero, si el receptor/importador se encuentra domiciliado en un Estado miembro de la UE, en un Estado parte del EEE o en Suiza, en cuyo caso el tribunal podrá declararse competente, de acuerdo a la regla general del domicilio del demandado (art. 2 del RB/CL 11/CB/[207] Tratado España-República de El Salvador); y, segundo, en el resto de supuestos, en los que habrá que acudir a la LOPJ para determinar sí/no la competencia

[205] Art. 4 en el Reglamento «Bruselas I bis».

[206] Art. 4 en el Reglamento «Bruselas I bis».

[207] Art. 4 en el Reglamento «Bruselas I bis».

judicial internacional de los tribunales españoles. La misma solución (LOPJ) se aplicará a las reclamaciones contra los importadores establecidos en cualquier otro Estado distinto de los anteriores.[208]

En definitiva, la protección del afectado (establecido en España) queda limitada ante una demanda contra el responsable o encargado receptor/importador de los datos. Para intentar atraer la competencia judicial internacional de los tribunales españoles tendremos que o bien, atraer el litigio al ámbito de la competencia de los tribunales del promotor/exportador de los datos; consultar si se han introducido una cláusula de elección de foro a favor de tercero; o bien, como veremos, fundamentar sus pretensiones en los criterios atributivos de competencia judicial internacional del artículo 22.3 y 4 de la LOPJ.[209]

C. Pluralidad de demandados: promotor y receptor de una transferencia internacional de datos de carácter personal

122. Ante una pluralidad de demandados[210] el afectado puede presentar la demanda ante el tribunal correspondiente al domicilio de cualquiera de ellos (art. 6.1 del RB/CL II/CB,[211] o 4.6 del Tratado España-República de El Salvador). Este artículo 6.1 presenta un gran interés en los litigios por vulneración del derecho a la protección de datos derivado de una transferencia internacional de datos de carácter personal ilícita, debido a la frecuencia con que el tratamiento ilícito in-

---

208 *Vid.* Diana Sancho Villa, *Negocios Internacionales..., op. cit.,* p. 227.

209 *Vid.* Diana Sancho Villa, *Transferencia internacional...*, *op. cit.,* p. 228.

210 Con carácter general sobre el fuero de la pluralidad de demandados, *Vid.* Iván Heredia Cervantes, *Proceso internacional y pluralidad de partes,* Comares, Granada, 2002.

211 Art. 6.1 en el Reglamento «Bruselas I bis».

ternacional de datos de carácter personal es cometido de manera coordinada por personas domiciliadas en distintos Estados (p. ej., exportador e importador de los datos).

123. Es una opción interesante a considerar, ya que el afectado adquiere la capacidad de acercar el litigio a su círculo de intereses (los tribunales del Estado del domicilio del promotor/exportador). No obstante, la solución del artículo 6.1 en la materia que nos ocupa es francamente defectuosa, ya que se obliga al afectado a presentar tantas demandas como Estados en los que se ha infringido su derecho a la protección de datos de carácter personal. Esto conlleva un grave menoscabo en la tutela efectiva del titular del derecho a la protección de datos del afectado.

Una protección eficaz del afectado exige una interpretación extensiva del requisito de «resoluciones inconciliables» del referido artículo 6.1 del RB/CL II/CB[212] o 4.6 del Tratado España-República de El Salvador. En caso de pluralidad de demandados, cuando estos estén vinculados entre sí, la demanda podría interponerse ante el tribunal del lugar del domicilio del demandado que presente una mayor vinculación con el litigio, siempre que existiera peligro de resultados contradictorios, si los asuntos fueran enjuiciados separadamente. Se trata de una solución que salvaguarda el equilibrio entre todos los intereses en presencia. Además, se trataría de una solución que responde a criterios de proximidad y que evita el *forum shopping*.

124. El conocimiento por el tribunal de un Estado miembro/contratante de la vulneración del derecho a la protección de datos

[212] Art. 6.1 en el Reglamento «Bruselas I bis».

derivada de una transferencia internacional de datos ilícita, protegido por las leyes de varios Estados miembros/contratantes, serviría para garantizar la aplicación uniforme de la proyectada legislación sobre la materia en protección de datos;[213] y, en el caso de duda acerca de la interpretación a otorgar a una de esas normas, siempre se podría acudir al TJUE.

D. Transferencias internacionales de datos de carácter personal realizadas por sucursales

125. En ocasiones, el promotor/exportador establecido en un tercer Estado utiliza para su tratamiento de datos «medios en España» (art. 2.1.c de la LOPD). Si el medio es un centro de explotación, su sede de explotación, su sede de administración o su sede estatutaria (sucursal, agencia o establecimiento) el afectado dispone del foro de la sucursal ya mencionado, previsto en el artículo 5.5 del RB/CL 11/CB[214] o 4.5 del Tratado España-República de El Salvador. Este foro de competencia cubre los litigios relativos a las actividades de dicha «sucursal» consistentes en la realización de tratamientos de datos en España en nombre de la sociedad de la que depende, en el marco de los litigios relativos a la explotación de estos establecimientos, y siempre que aquella sociedad esté domiciliada en un Estado parte del RB/CL 11/CB.[215,216,217]

---

213 En este sentido, el hecho de que las legislaciones nacionales de los Estados miembros no reglamenten el derecho a la protección de datos de carácter personal de la misma manera no debería impedir la aplicación de este foro de competencia judicial internacional.

214 Art. 7.5 en el Reglamento «Bruselas I bis».

215 Y del Reglamento «Bruselas I bis».

216 *Vid.* Diana Sancho Villa, *Transferencia internacional...*, *op. cit.*, pp. 244-245.

E. Recapitulación

126. El juego del foro general del domicilio del demandado en la práctica también suele ser más bien reducido por dos razones capitales: por un lado, porque *litigar fuera de casa* puede llevar aparejados elevados costes para el sujeto afectado, que puede no estar en disposición de asumir; y, por otro lado, porque, como hemos señalado, puede convertirse en *misión imposible* la determinación del domicilio del responsable (demandado).

127. En defecto de elección de tribunales competentes, la opción del foro general ofrece al damnificado una alternativa favorable a sus intereses. El foro general del domicilio del demandado resulta evidentemente perjudicial para la víctima: *a)* porque, generalmente, tendrá que correr con el coste de internacionalización del proceso; y, *b)* porque la sitúa tan lejos de su ámbito de desarrollo social y personal como cerca del centro de intereses del causante del daño.

4. Litigios derivados de una transferencia internacional de datos de carácter personal ilícita: el *forum delicti commissi* como alternativa al foro general del domicilio del demandado

128. En defecto de elección de tribunales competentes, junto a la opción del foro general del domicilio del demandado opera, en concu-

---

[217] En todo caso, en otro orden de cosas, a los efectos del cumplimiento de las normas imperativas españolas, el responsable exportador deberá cumplir con la obligación de nombrar a un representante en España (art. 5 de la LOPD).

rrencia, el *forum delicti commissi*. Se trata de darle la competencia a los tribunales del «lugar donde se hubiere producido o pudiere producirse el hecho dañoso». Me ocuparé de los problemas en la interpretación del «lugar donde se hubiere producido o pudiere producirse el hecho dañoso» en transferencias internacionales de datos de carácter personal (A): disociación entre país de origen y país de verificación del perjuicio ocasionado al titular del derecho a la protección de datos de carácter personal; y multiplicación de los países en los que se verifica el perjuicio ocasionado al titular del derecho a la protección de datos de carácter personal (a); de qué ocurre cuando el titular del derecho a la protección de datos de carácter personal presenta la demanda ante los tribunales del lugar donde se localiza la acción que causa directamente el daño (b) o cuando el titular del derecho a la protección de datos de carácter personal presenta la demanda ante los tribunales donde se materializa el daño directo para él y producido de manera inmediata (c).

Concluiré este apartado con dos propuestas: por un lado, la necesidad de una regla especial para las transferencias internacionales de datos de carácter personal realizadas a través de Internet: el lugar del «centro de intereses del presunto perjudicado» (B); y, por otro lado, con una propuesta de *lege ferenda*: la residencia del afectado por la transferencia internacional de datos de carácter personal como foro de competencia: potenciación del *favor actoris* (C).

A. Determinación del Juez internacionalmente competente: el *forum delicti commissi*

129. Fuera de los supuestos indicados anteriormente, la competencia judicial internacional puede corresponder a los tribunales del lugar donde se haya producido o pudiere producirse el hecho dañoso *(forum*

delicti commissi). Indica el artículo 5.3 del RB/CL II/CL/CB[218] que «las personas domiciliadas en un Estado podrán ser demandadas en otro Estado (....) 3) En materia delictual o cuasidelictual, ante el tribunal del lugar donde se hubiere producido o pudiere producirse el hecho dañoso.»[219,220]

130. Ante la vulneración del derecho a la protección de datos derivado de una transferencia internacional de datos de carácter personal ilícita «lo habitual es que el hecho dañoso se produzca en el país donde radica el fichero de datos personales, aunque no tiene por qué ser siempre así»,[221] ya que, el lugar donde se ha producido el hecho dañoso puede ser, efectivamente, el país o países (si se han producido transferencias de datos sucesivas, y sólo para los perjuicios causados en cada uno de esos territorios) donde se han transferido los datos (que en las transferencias de datos de España al extranjero, ese lugar será España, por aplicación del artículo 2.1 de la LOPD), así como, el

218 Art. 7.3 en el Reglamento «Bruselas I bis».

219 A este respecto el propio TJUE en su sentencia de 27 de septiembre de 1988, asunto *Kalfelis* (189/87, Rec. p. 5565), en su apartado 18 definió el concepto de materia delictual o cuasidelictual en el sentido del número 3 del art. 5 como un concepto autónomo que abarca todas las demandas dirigidas a exigir la responsabilidad de un demandado y que no están relacionadas con la materia contractual en el sentido del núm. 1 del art. 5. De acuerdo con esta doctrina, el artículo 5.3 del RB/CL II/CB tiene carácter residual, pues siempre va a aplicarse cuando la obligación no esté incluida en el art. 5.1 del RB/CL II/CB.

220 En iguales términos se expresa el art. 4.3 del Tratado España-República de El Salvador (En materia de responsabilidad extracontractual, serán competentes los tribunales del lugar de que se hubiere producido el hecho que la genera).

221 Alfonso-Luis Calvo Caravaca y Javier Carrascosa González *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001, p. 153.

país donde se haya manifestado el daño por el tratamiento de datos realizado en ese lugar, por parte del que recibió los datos.[222]

a. Problemas en la interpretación del «lugar donde se hubiere producido o pudiere producirse el hecho dañoso» en transferencias internacionales de datos de carácter personal

131. El artículo 5.3 del RB/CL II/CB[223] o 4.3 del Tratado España-República de El Salvador utiliza como criterio de atribución de competencia judicial internacional el *locus delicti commissi*, o lugar del daño.

Para que el lugar de recepción de los datos sea considerado como lugar del daño (en el que éste se produce) resulta preciso que en ese concreto Estado esté presente el interés que resulta lesionado: el derecho a la protección de datos menoscabado.

Los problemas que pueden surgir en la determinación de esta norma son de diversa índole y van desde la posible disociación territorial entre el lugar donde se realiza el hecho causal (lugar de origen) y donde finalmente se materializa el daño (lugar de resultado) hasta la multiplicación de los lugares de origen y de resultado (daños plurilocalizados).

i) Disociación entre país de origen y país de verificación del daño

132. La expresión «lugar donde se hubiere producido el hecho dañoso» comprende tanto el lugar donde se produce el hecho causal como el lugar donde sobreviene el daño o resultado lesivo. Cabe, siguiendo esta doctrina, que la víctima pueda elegir cualquiera de los dos fueros:

---

222 *Vid.* Diana SANCHO VILLA, *Transferencia internacional...*, *op. cit.,* pp. 251-252.

223 Ap. 3 del art. 7 en el Reglamento «Bruselas I bis».

a) lugar donde el daño se materializó (lugar de resultado o *locus damni*) —lugar de recepción de los datos de carácter personal— o *b)* lugar donde tuvo lugar el acontecimiento del que se deriva el daño (lugar de origen o *locus delicti)* —lugar de emisión de los datos de carácter personal—, siempre que no coincida el lugar de la acción dañosa y el del resultado dañoso, y responda al objetivo de buena administración de justicia.

Si el afectado presenta la demanda ante los tribunales del lugar donde se localiza la acción que causa directamente el daño, en un buen número de supuestos nos va a conducir a estimar internacionalmente competente al tribunal del domicilio del responsable del daño y resulta que tal tribunal es ya competente en virtud del foro general del Estado del domicilio del demandado.

133. A efectos de determinar el evento causal lo que debe contar es el *lugar donde se sitúa la acción que origina directamente el daño*». El origen del hecho dañoso se sitúa, con carácter general, en el lugar donde se encuentra el promotor/exportador de los datos personales del afectado. Así, p. ej., el tratamiento de datos personales que realiza un sujeto como encargado por cuenta de otro no tendría la suficiente entidad para integrar el criterio de competencia judicial internacional del evento causal cuando aquellos fueran preparatorios del tratamiento de este último. Igualmente, esta regla no sería de aplicación cuando el encargado se extralimite en sus funciones y realice actuaciones que supongan la disposición propia de los datos personales del afectado.[224]

[224] *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.,* pp. 234-235.

ii) Multiplicación de los países en los que se verifica el daño

134. El supuesto típico de multiplicación de los países en los que se verifica el daño es el siguiente: una cadena de tratamientos de datos sin el consentimiento del afectado entre un responsable y varios encargados y subencargados. En estos casos, el afectado podría reclamar ante los tribunales del lugar donde radique el responsable (primero en la cadena) como lugar de origen del daño. Ahora bien, sólo le serían imputables los daños que estén dentro de la esfera de control del causante del daño (lo que pueda razonablemente prever) y no cualquier daño que pueda producirse en la cadena de tratamientos de datos de carácter personal del afectado.[225]

En cadenas de responsables del tratamiento de datos de carácter personal del afectado debemos entender que habrá tantos lugares de origen del daño como unidades de tratamientos de datos personales realizados.[226]

b. El titular del derecho a la protección de datos de carácter personal presenta la demanda ante los tribunales del lugar donde se localiza la acción que causa directamente el daño

135. El lugar del resultado dañoso es aquél en el que se produce el *perjuicio material directo* para la *víctima directa*. Dicho lugar se habría de localizar en el Estado donde se hubieran recibido los datos de carácter personal, y, consecuentemente, el contenido ilícito fuera accesible. Se trata de lugar en el que el hecho generador despliega sus *efec-*

---

225 *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.,* pp. 235-236.

226 *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.,* p. 236.

tos perjudiciales, es decir, el lugar donde el perjuicio ocasionado se manifiesta de forma concreta.[227]

En estos casos, los tribunales del Estado donde se ha verificado el daño sólo serían competentes para conocer de las demandas basadas en los daños ocurridos en el territorio de dicho Estado, mientras que si el afectado opta por los tribunales del Estado donde radica el *origen del daño* (lugar donde se localiza la acción que causa directamente el daño) pueden conocer de todas las consecuencias derivadas del mismo, sea cual fuere el Estado en el que se cerifique el daño (reparación de la integridad de los daños derivados del supuesto de responsabilidad extracontractual).

En todo caso, si el afectado presenta la demanda ante los tribunales donde se materializa el daño directo para él y producido de manera inmediata, en un buen número de supuestos, va a coincidir con el lugar donde el afectado se encuentra domiciliado, fomentando, de esta forma, el *favor actoris*, y potenciando la posición de la presunta víctima *(favor leasi)*.

c. El titular del derecho a la protección de datos de carácter personal presenta la demanda ante los tribunales donde se materializa el daño directo para él y producido de manera inmediata

136. Cuando el afectado sufre daños en varios Estados derivados de un mismo acto la competencia judicial internacional en cada uno de

---

[227] STJUE de 16 de julio de 2009, C-189/08, *Zuid-Chemie BV*, FD 27 y 28). *Vid.* Natividad GOÑI URRIZA, «La concreción del lugar donde se ha producido el hecho dañoso en el art. 5.3 del Reglamento 44/2001: nota a la STJCE de 16 de julio de 2009», en *Cuadernos de Derecho Transnacional* (Marzo 2011), Vol. 3, núm. 1, pp. 290-295.

esos Estados se limitará al daño sufrido en ese Estado (art. 5.3 del RB/CL II/CB[228] o 4.3 del Tratado España-República de El Salvador). Pero, ¿dónde se sufren las consecuencias directas e inmediatas de una vulneración del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita? Quizás el criterio de la residencia habitual del titular del derecho a la protección de datos de carácter personal se pueda traducir en el *centro de intereses del afectado*. Eso sí, siempre que el derecho a la protección de datos haya sido vulnerado en el Estado de residencia del afectado, y no cuando el daño presente una nota de proximidad con otro lugar. Así, p. ej., si se aplican condiciones de crédito desfavorables a un sujeto con residencia en Alemania en base a una información incorrecta sobre su solvencia a la que accede una empresa española, a nuestro entender, el perjuicio a efectos del artículo 5.3 del RB/CL II/CB[229] o del 4.3 del Tratado España-República de El Salvador se produce de manera directa e inmediata en España (mercado donde el sujeto sufre las condiciones de crédito perjudiciales) y no tanto en Alemania (lugar de residencia del sujeto).[230]

[228] Ap. 3 del art. 7 en el Reglamento «Bruselas I bis».

[229] Ap. 3 del art. 7 en el Reglamento «Bruselas I bis».

[230] *Vid.* Diana SANCHO VILLA, *Negocios Internacionales...*, *op. cit.,* pp. 236-237.

B. Excesiva fragmentación y necesidad de una regla especial para las transferencias internacionales de datos de carácter personal realizadas a través de Internet: el lugar del *centro de intereses del presunto perjudicado*

137. La expresión «lugar donde se hubiere producido o pudiere producirse el hecho dañoso», utilizada en el número 3 del artículo 5 del RB/CL II/CB[231] o del 4.3 del Tratado España-República de El Salvador debería interpretarse, en caso de vulneración del derecho a la protección de datos, mediante información difundida en varios Estados miembros a través de Internet, en el sentido de que el titular del derecho a la protección de datos personales vulnerado por el tratamiento ilícito internacional de sus datos. Puede entablar una acción de reparación: ante los órganos jurisdiccionales del Estado donde se localice el *centro de gravedad del conflicto* entre los bienes e intereses en juego, dotados así de competencia para reparar la integridad de los daños derivados de la vulneración del derecho a la protección de datos. Se entiende por Estado donde se localiza el centro de gravedad del conflicto aquel en cuyo territorio la información litigiosa resulta objetiva y particularmente relevante y donde, al mismo tiempo, el titular del derecho a la protección de datos de carácter personal tiene su *centro de intereses*.

138. Las conclusiones presentadas ante el Tribunal de Justicia de la Unión Europea por el Abogado General Cruz Villalón en dos asuntos acumulados —*eDate Advertising* (C-509/09) y *Martínez y Martínez*

[231] Art. 7.3 en el Reglamento «Bruselas I bis».

(C-161/10)—[232,233] permiten esbozar un criterio adicional para la determinación de la competencia judicial internacional en litigios relativos a la responsabilidad extracontractual derivada de actividades desarrolladas en Internet.[234] En concreto, las cuestiones prejudiciales tie-

---

[232] *Vid.* STJUE (Gran Sala) de 25 de octubre de 2011. En los asuntos acumulados C-509/09 y C-161/10, que tienen por objeto dos peticiones de decisión prejudicial presentadas, con arreglo al artículo 267 TFUE, por el *Bundesgerichtshof* (Alemania) (asunto C-509/09) y por el *Tribunal de grande instance* de Paris (Francia) (asunto C-161/10), mediante sendas resoluciones de 10 de noviembre de 2009 y 29 de marzo de 2010, recibidas en el Tribunal de Justicia, respectivamente, el 9 de diciembre de 2009 y el 6 de abril de 2010. *Vid.*, Clara Isabel CORDERO ÁLVAREZ, «Asuntos acumulado eDate Advertising y Martínez y Martínez (STJUE de 25 de octubre)», en *Foro, Nueva época*, núm. 14/2011, 267-268; y Isabel LORENTE MARTÍNEZ, «Lugar del hecho dañoso y obligaciones extracontractuales. La Sentencia del TJUE de 25 octubre 2011 y el coste de la litigación internacional en Internet», en *Cuadernos de Derecho Transnacional* (Marzo 2012), Vol. 4, núm. 1, pp. 277-301.

[233] *Vid.*, en el mismo sentido, STJUE de 18 de octubre de 2012, «Football Dataco ll» que planteó la siguiente problemática: el envío por una persona, a través de un servidor web situado en un Estado miembro A (Alemania), de datos previamente obtenidos por esta persona a partir de una base de datos a otra persona establecida en un Estado miembro B (Inglaterra), a solicitud de esta última, para ser almacenados en la memoria de este ordenador y ser visualizados en su pantalla, constituye un acto de «reutilización» de dichos datos por parte de la persona que ha realizado tal envío. Debe considerarse que este acto ha tenido lugar, al menos en el Estado miembro B cuando existan indicios que permitan concluir que tal acto pone de manifiesto la intención de su autor de dirigirse a los miembros del público establecidos en este Estado miembro, extremo éste que corresponde verificar al órgano jurisdiccional nacional.

[234] *Vid.*, en relación con los aspectos de dicha sentencia relativos a la interpretación del artículo 5.3 del RB y los perfiles que dicha decisión dedica al artículo 3 de la Directiva sobre el comercio electrónico (Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior). Elisa TORRALBA MENDIOLA, «La difama-

nen como objeto determinar en qué medida o con qué adaptaciones la interpretación del fuero del lugar del hecho dañoso del artículo 5.3 del RB[235] (y del CL 11/CB) o del artículo 4.3 del Tratado España-República de El Salvador llevada a cabo por el TJUE en su célebre Sentencia *Shevill* son aplicables a los supuestos en los que supuestamente se viola un derecho de la personalidad (como, p. ej., el derecho a la protección de datos) se ha difundido a través de Internet, si bien la respuesta a tal cuestión está llamada a condicionar también el tratamiento de la competencia judicial internacional en otras categorías de ilícitos cometidos a través de Internet. La propuesta del Abogado General contempla la evolución de la jurisprudencia *Shevill* previendo respecto de las actividades desarrolladas en Internet que pueda operar un criterio adicional de conexión como determinante de la atribución de competencia judicial internacional, el ***«centro de gravedad del conflicto»,*** al tiempo que rechaza la mera accesibilidad de la información en un país como fundamento para la atribución de competencia a sus tribunales.

El fundamento del planteamiento del Abogado General y de su propuesta de complementar los criterios establecidos en la Sentencia *Shevill* se encuentra en la transformación introducida por Internet en este ámbito: su alcance global menoscaba que la fragmentación de órganos competentes a la que conduce la Sentencia *Shevill* pueda fundamentarse realmente en la garantía de una buena administración de justicia, la dificultad de medición del grado de difusión de los medios en Internet o la necesidad de favorecer un planteamiento que

---

ción en la era de las comunicaciones: ¿Nuevas? perspectivas de Derecho Internacional Privado Europeo», en *Revista inDret*, núm. 1/2012, disponible en http://www.indret.com.

235 Art. 7.3 en el Reglamento «Bruselas I bis».

permita una protección más eficaz de los derechos fundamentales en presencia, típicamente el derecho fundamental a la libertad de información y el derecho a la vida privada con expresa mención de los artículos 7 y 11 de la Carta de Derechos Fundamentales de la UE.

A partir de esos elementos el Abogado General justifica su propuesta de completar los «criterios de conexión de la sentencia Shevill» de modo que permita también atribuir competencia para conocer de la totalidad de los daños alegados a la jurisdicción que «esté en mejor situación para analizar la tensión de los intereses en juego», mediante la previsión de una situación intermedia a las dos ya existentes, que permita al titular del derecho de la personalidad lesionado litigar en un foro donde se encuentre su centro de intereses. Por lo tanto, en este planteamiento resulta clave cómo se concreta el ***centro de gravedad del conflicto.*** Para el Abogado General tal lugar «sería aquel donde una jurisdicción puede efectuar, en las condiciones más favorables, el enjuiciamiento de un conflicto entre la libertad informativa y el derecho a la propia imagen», lo que considera que tiene lugar en el Estado «donde se visualice o manifieste con mayor intensidad la potencialidad de un atentado al derecho a la propia reputación o intimidad y el valor inherente a la comunicación de una determinada información u opinión, según el caso», de modo que es la jurisdicción que se encuentra en una mejor posición para «permitir una aprehensión integral del conflicto entre los intereses en juego». Además, para salvaguardar la posición del demandado y garantizar la previsibilidad, el Abogado General aclara que ese lugar será el territorio donde el medio habría podido prever que dicha lesión pudiera eventualmente producirse, y en consecuencia, que exista el riesgo de ser allí demandado.

Las conclusiones destacan que para concretar el lugar donde se manifiesta el ***centro de gravedad del conflicto*** deben identificarse dos elementos: *a)* en primer lugar, que tal *centro de gravedad* se ubi-

que donde el perjudicado tenga su *centro de intereses*; a saber, el lugar «en el que el particular afectado en el goce de sus derechos de la personalidad desarrolla esencialmente su proyecto vital, siempre y cuando éste exista»; y, *b)* concretar dicho centro de gravedad. El Abogado General considera que «la información litigiosa debe estar expresada de tal manera que permita razonablemente prever que dicha información es objetivamente relevante en un determinado espacio territorial», es decir que esa información «debe expresarse en unos términos que, a la vista de las circunstancias que rodean la noticia, constituyan una información que suscite interés en un territorio y, en consecuencia, incite activamente a los lectores en dicho territorio a acceder a ella.». Con respecto a este segundo elemento, aclara que no cabe acudir a criterios subjetivos de intencionalidad y que no debe confundirse con una exigencia de que el medio dirija específicamente la información a ese país, que se considera contraria al texto literal del artículo 5.3 del RB[236] (y del CL 11/CB) o del 4.3 del Tratado España-República de El Salvador. Como aspectos a tener en cuenta al valorar si concurre este segundo requisito —que la información sea objetivamente relevante para el país al que se atribuye la competencia—, el Abogado General parte precisamente del contenido de la información que puede ser clave al interpretar el criterio de relevancia objetiva de la información de que se trate, en función de su *interés noticiable* con respecto a un concreto territorio. Como indicios complementarios para determinar el territorio donde la información es objetivamente relevante, las Conclusiones hacen referencia al nombre de dominio de primer nivel de la página en la que se difunde la información (si bien la importancia práctica de ese elemento en este contexto parece ser

[236] Art. 7.3 en el Reglamento «Bruselas I bis».

limitada), a la lengua en que se difunde, a los registros de acceso a una página y a la sección en la que se incluye para su difusión.

Aunque algunos de sus elementos, como los indicios a considerar para apreciar el centro de gravedad, pueden generar algunas dudas y exigir aclaraciones adicionales, el criterio adoptado por el Abogado General proporciona un modelo apropiado en caso de que el TJUE comparta su criterio acerca de la necesidad de adaptación de la Sentencia *Shevill* a las actividades desarrolladas a través de Internet. Otros aspectos de la interpretación del artículo 5.3 del RB[237] al contexto de Internet parecen quedar abiertos, en particular el *recordatorio* de que conforme a la Sentencia *Shevill* tienen competencia con respecto a la integridad de los daños «los tribunales del lugar de establecimiento del editor de la publicación». Si bien se trata de un criterio derivado del artículo 5.3 del RB[238] (y del CL 11/CB) o del 4.3 del Tratado España-República de El Salvador; y, por lo tanto, diferenciado del fuero general del domicilio del demandado del artículo 2 del RB[239] (y del CL 11/CB/ Tratado España-República de El Salvador) cabe en la práctica con frecuencia se desactiva al localizarse en el mismo lugar que éste, cabe considerar que resultarán de utilidad en el futuro precisiones adicionales en relación con la información difundida a través de Internet para la que el concepto de «lugar de establecimiento del editor de la publicación» no resulte una realidad tan homogénea como era propio del marco de los medios de comunicación impresos antes de la aparición de Internet.

---

237 Art. 7.3 en el Reglamento «Bruselas I bis».

238 Art. 7.3 en el Reglamento «Bruselas I bis».

239 Art. 4 en el Reglamento «Bruselas I bis».

Esta interpretación del TJUE favorece en la práctica la posición del afectado que ha visto lesionado su derecho a la protección de datos de carácter personal, en la medida en que pone a su disposición un fuero distinto al domicilio del demandado. La solución aquí retenida presenta, no obstante, un inconveniente: supone dar entrada a un *forum actoris,* alterando con eso el punto esencial de partida del RB (y del CL II/CB/ Tratado España-República de El Salvador) (que lo admite solo en los casos en que existe un desequilibrio entre partes contractualmente relacionadas: seguros, consumo y, con matices, trabajo, y en los supuestos en que el demandado está domiciliado fuera de la UE como consecuencia de lo previsto en su artículo 4.[240] No obstante, frente a este argumento cabe oponer que se trata de un foro previsible para el responsable y contemplado para un supuesto en el que quien está en situación de evitar el daño y su internacionalidad es exclusivamente al autor del mismo, sin que la víctima, por las propias características de los supuestos extracontractuales pueda actuar *a priori* en evitación de la situación.[241]

Resulta por lo tanto fundamental concretar cuál es el *centro de intereses* de la víctima ***(centro de gravedad del conflicto)***. Parece evidente que tal lugar coincidirá con la residencia habitual de la víctima, pero una persona puede tener su centro de intereses también en otro Estado en el que no resida habitualmente, en la medida en que otros indicios, como el ejercicio de una actividad profesional, permitan establecer la existencia de un vínculo particularmente estrecho con ese

---

[240] En contra de un criterio competencial que sea un *forum actoris*: SSTJUE de 11 de enero de 1990, C-220/88, FJ 19.º; de 19 de septiembre de 1995, C-364/93, FJ 13.º; de 27 de octubre de 1998, C-51/97, FJ 34.º y de 10 de junio de 2004, C-168/2002, FJ 20.º.

[241] *Vid.*, en particular, Elisa TORRALBA MENDIOLA, «La difamación..., *op. cit.*, pp. 19-21.

Estado. Por tanto, «resultará clave para concretar el Estado en el que se encuentra el 'centro de intereses' de la víctima la existencia de un vínculo particularmente estrecho entre la víctima y ese Estado el que determina que sus Tribunales sean los mejor situados para apreciar la lesión a los derechos de la personalidad de la supuesta víctima y que al supuesto responsable le resulte fácilmente previsible conocer dónde puede ser demandado».[242]

C. Balance final y propuesta de *lege ferenda*: la residencia del afectado por la transferencia internacional de datos de carácter personal como foro de competencia: potenciación del *favor actoris*

a. La residencia del afectado por la transferencia internacional de datos de carácter personal como foro de competencia

139. La multiplicación de los tribunales estatales competentes en supuestos conectados con multitud de países (como es el caso de los litigios derivados de un tratamiento ilícito internacional de datos de carácter personal) quiebra la tan necesitada seguridad jurídica en el tráfico privado internacional y provoca que pueda estimarse que los efectos lesivos de un acto ilícito se puedan manifestar en todos los países del mundo desde donde fuera accesible la información lesiva (los datos de carácter personal del afectado).[243] La pluralidad de foros

[242] Pedro A. De Miguel Asensio, «Competencia judicial y protección de los derechos de la personalidad en Internet», en *Diario La Ley*, núm. 7787, Sección Tribuna, 31 de enero de 2012, Año XXXIII, editorial La Ley, pp. 3-4.

[243] En efecto, en principio, los lugares/países donde se produce el hecho dañoso serán *todos los del mundo*, dado que Internet presenta un alcance planetario.

de competencia que ofrecen los diferentes regímenes de competencia judicial internacional propicia la utilización del denominado *forum shopping* por parte del sujeto afectado, quien podrá optar por plantear la demanda de responsabilidad extracontractual ante aquellos tribunales cuyas normas de conflicto designen como aplicable una ley que prevea un régimen de responsabilidad extracontractual más favorable para sus propios intereses.

Cuanto mayor es el número de Estados en el que se ha cometido la violación del derecho a la protección de datos, como consecuencia de una transferencia internacional de datos de carácter personal ilícita las alternativas se multiplican para el *forum shopper*. No obstante, las posibilidades de ataque nos pueden llevar en la práctica a la utilización de un foro realmente exorbitante en los que se aprecia una falta de vinculación real del litigio con la esfera española y que requieren una reducción teleológica a través del denominado *forum non conveniens*. Así, cuando el foro previsto en la norma de competencia judicial internacional otorga competencia a jueces de países que de ningún modo podían ser previstos por el demandado como competentes, dicho foro debe ser inaplicado.[244]

140. Así las cosas, a nuestro modo de ver, en esta materia, para evitar el *forum shopping* debemos acudir al *principio de proximidad*. El *principio de proximidad* se configura como un principio esencial que obliga necesariamente a establecer la competencia judicial internacional de aquellos tribunales que tengan una conexión o vínculo importante con el litigio para poder garantizar la necesaria previsibilidad del fuero para el demandado. La exclusión de la competencia judicial interna-

[244] *Vid.*, *ibídem,* p. 108.

cional de dichos tribunales es la solución más coherente con la tesis de la competencia limitada del tribunal del daño establecida por *Fiona Shevill (*y suscrita por *eDate Advertising)*. Si se entiende que el daño inicial y el sobrevenido son distintos a los efectos de reconocer la competencia judicial internacional, el tribunal del daño inicial sólo podrá conocer de éste y no de los daños posteriores sobrevenidos (sus consecuencias posteriores), salvo que se hayan producido en su mismo territorio. De igual manera, los tribunales donde se hayan sufrido dichas consecuencias sólo podrán conocer de éstas y no del daño inicial —si se produjo en otro Estado—.

Son obvias las eventuales consecuencias prácticas a las que esta aproximación conduciría: es posible que el segundo tribunal (el de los daños sobrevenidos) reconozca la existencia de responsabilidad y, en su virtud, conceda la reparación por esos perjuicios posteriores, mientras que el primer tribunal (el del daño inicial) establezca la no existencia de responsabilidad por concurrencia de alguna causa que exonera al demandado, por lo que no otorga ningún resarcimiento. Además, en la generalidad de ordenamientos jurídicos nacionales al reglamentar la responsabilidad extracontractual únicamente los daños indirectos o sobrevenidos tienen sentido si se prueba la existencia (o se presume) de un daño inicial. Y esto es consecuencia directa de la propia causalidad de los daños sobrevenidos o indirectos. Esto es, los daños sobrevenidos no son más que el efecto de un daño inicial y los indirectos se derivan del daño producido de forma directa a otro sujeto. Esto permite afirmar que entre ellos existe una cadena causal, indisociable, que no permite la disociación tanto desde el punto de vista de la estructura material de este tipo de daños como desde el punto de vista de la competencia limitada del *foro damni.*

Es más, desde la perspectiva del *principio de acumulación de acciones* tampoco puede admitirse la competencia de estos tribunales.

Pues si se otorgara competencia a todos y cada uno de los tribunales donde aparezca un daño sobrevenido o indirecto, además de al del daño inicial, la consecuencia más inmediata sería la multiplicación de tribunales competentes. Y frente a esta situación lo más evidente es el peligro de sentencias contradictorias que tendrían serios problemas en sede de reconocimiento y ejecución en otros Estados.

141. En el momento de aplicar el criterio de competencia del artículo 5.3 del RB (y del CL 11/CB) o 4.3 del Tratado España-República de El Salvador podría entrar en juego el principio de protección del afectado. Los tribunales españoles podrían tener en consideración el principio *favor laesi* como un principio informador del sistema de competencia.

A pesar de todos los argumentos anteriores podría eventualmente aducirse el principio del *favor laesi* para sustentar una solución contraria a la expuesta —pero que no tiene reflejo en la doctrina de TJUE—. Pues obviamente otorgar competencia a estos tribunales solo podría obedecer al objetivo de proteger a la víctima. Pero la cuestión es si este principio tiene suficiente fuerza para justificar que aquellos tribunales tengan competencia. Aunque, *a priori*, la respuesta parece clara: la protección del afectado no puede primar sobre otros principios fundamentales para la buena administración de justicia. El principio de protección del afectado no puede alegarse por ser contrario a los principios de proximidad y de concentración de acciones; en nuestra opinión, en aras a la protección del titular del derecho a la protección de datos de carácter personal vulnerado como consecuencia de una transferencia internacional de datos de carácter personal ilícita sí deberíamos posibilitar el *forum actoris*, aunque su operatividad no está contemplada en ninguno de los dos instrumentos europeos, y lo más importante, no exista ninguna manifestación favorable por parte de TJUE que permitiera esta aproximación.

142. La posición predominante del autor del daño, cuando éste es fuerte y conocedor de los riesgos que su actividad conlleva, y por tanto, con medios suficientes para afrontar las posibles responsabilidades en las que incurra, incluso si el litigio se lleva a cabo en el extranjero. Lo que se contrapone a la posición del afectado que estaría en situación de inferioridad, pues generalmente se tratarían de personas privadas sin conocimientos en la materia ni recursos especiales para litigar en el extranjero y que, raramente, pudo prever la agresión y adoptar los medios para su defensa.

143. Para evitarle inconvenientes al afectado y asegurarle una opción real de competencia a *favor damni* podrían haberse considerado competentes los tribunales de uno de los lugares donde se ha manifestado el hecho dañoso, también respecto a los daños sufridos en los otros dos Estados, en razón a que todos ellos están conectados a un mismo hecho generador. La relación de causalidad entre el hecho y el daño que no es de origen geográfico, sino jurídico, justificaría tanto la competencia global del lugar del hecho como la de cualquiera de los lugares del daño. El problema de fondo es que la flexibilización del foro del mencionado artículo 5.3 del RB/CL II/CB[245] o 4.3 del Tratado España-República de El Salvador mediante la opción entre el *lugar del hecho causal* y los del *lugar del hecho dañoso* puede resultar artificioso en los ilícitos contra el derecho a la protección de datos de carácter personal derivado de una transferencia internacional de datos de carácter personal, por la dificultad de determinar los lugares del hecho y del daño.

[245] Art. 7.3 en el Reglamento «Bruselas I bis».

b. Potenciación del favor actoris

144. En este contexto, y para los litigios derivados de una transferencia internacional de datos de carácter personal ilícita, la instauración del *forum actoris* que otorga la competencia a los tribunales del Estado de residencia habitual o principal establecimiento del afectado-demandante,[246] esto es, del afectado/perjudicado/víctima por la lesión de su derecho a la protección de datos, consecuencia de una transferencia internacional ilícita de datos («lugar donde la víctima sufre el daño, sin tener en cuenta la separación entre el hecho causal y el daño, puesto que es donde la víctima sufre el daño»).

La justificación de esta nueva posibilidad de ataque a favor de la víctima «puede encontrarse en el hecho de que nos encontramos ante un derecho de naturaleza personalísima que presenta un aspecto inmanente en virtud del cual puede entenderse producida la lesión en el lugar en el que el titular del derecho fundamental siente el perjuicio que es aquel en que tiene su residencia [...]. Si se adopta el fuero del domicilio del demandante la víctima tiene mayores facilidades para

[246] *Vid.* Carlos GÓMEZ MARTÍNEZ, «El ejercicio de acciones civiles de protección de la intimidad del usuario de Internet. Aspectos procesales», en Carlos GÓMEZ MARTÍNEZ (Dir.), *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2004, pp. 159-161; Raquel XALABARDER PLANTADA, «Cuestiones de derecho internacional privado: jurisdicción competente y ley aplicable», *op. cit.*, p. 487; y, la misma solución plantea Suquet Capdevila en materia de infracciones de derecho de propiedad industrial en Internet, *Vid.* Josep SUQUET CAPDEVILA, «Internet, marcas y competencia judicial internacional: ¿O la superación de la regla *forum loci delicti commissi*?...», *op. cit.*, p. 7; y, Fuentes Camacho, salvando las distancias, en materia de tráfico ilícito internacional de bienes culturales, *Vid.* Víctor FUENTES CAMACHO, *El tráfico ilícito internacional de bienes culturales*, Ediciones Beramar, EUROLEX, Madrid, 1993, pp. 173-177.

acceder a la justicia aunque el tribunal tiene mayores dificultades para la correcta apreciación del alcance del daño, dificultades que disminuyen cuando nos hallamos ante un derecho de la personalidad de carácter, en principio, universal, pero que, desde luego, existen y se manifiestan no sólo por la distancia en kilómetros sino, también, por la distancia de culturas y de sistema jurídicos»,[247] pero, eso sí, este nuevo *foro de necesidad* a favor de la residencia habitual o principal establecimiento del afectado-demandante, debería matizarse, de forma que quede circunscrito tan sólo al Estado donde se producen los daños principales al afectado; y, por supuesto, debería quedar a salvo la opción del afectado de litigar ante los tribunales del Estado de origen o destino de la transferencia internacional de datos personales ilícita objeto del litigio.

No obstante, para reducir el juego del *forum actoris* en estos casos y buscar el principio de igualdad de armas entre demandante y demandado, se puede reinterpretar el mencionado artículo 5.3 del RB/CL II/CB[248] o 4.3 del Tratado España-República de El Salvador y entender que *el lugar donde se hubiere producido o pudiere producirse el hecho dañoso* (lugar en el que se manifiestan todos los elementos constitutivos de la responsabilidad) sería el domicilio del perjudicado; y, eso sí, aplicando los siguientes correctivos:[249] primero, el *loci delicti* debe entenderse como el lugar donde se encuentre el interés de la víctima y donde se hayan manifestado los intereses esenciales; y,

---

247 *Vid.*, *ibídem,* p. 160.

248 Art. 7.3 en el Reglamento «Bruselas I bis».

249 *Vid.* Guillermo PALAO MORENO, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», en Javier PLAZA PENADÉS, *Cuestiones actuales de derecho y Tecnologías de la Información y Comunicación (TICs)*, Editorial Aranzadi, Cizur Menor (Navarra), 2006, pp. 293-296.

segundo, la interpretación del *loci delicti* debería ser corregida en aquellos casos en los que nos llevara a una respuesta inadecuada, fortuita o poco conectada con el litigio.

145. Se trataría de una posibilidad de *lege ferenda*[250] que tiende a proteger a la víctima que ha visto lesionado su derecho a la protección de datos, consecuencia de una transferencia internacional de datos de carácter personal ilícita, ya que le evita hacer frente a elevados costes al tener que interponer su demanda ante tribunales alejados, al coincidir con frecuencia el lugar donde se manifiesta el daño con aquel donde el demandante está domiciliado[251] (lugar donde la persona sufra la violación de su intimidad, esto es, el lugar de su domicilio). Para no provocar un desequilibrio demandante-demandado, al *favor actoris*, como criterio de determinación de la competencia judicial internacional, podemos aplicarle algún correctivo (y compensar, así, al demandado): uno, el daño podríamos entender que se ha producido sólo donde efectivamente se ha derivado un perjuicio directo para el derecho vulnerado; y, dos, recurrir a la Sentencia *Fiona Shevill*: mientras los tribunales del Estado de origen del perjuicio serían competentes para conocer de todos los daños que pudieran ocasionarse, los tribunales del lugar donde se ha producido el resultado lesivo tan sólo lo serían por los daños allí producidos.

---

[250] Se trata de una posibilidad que ya contempla nuestro ordenamiento jurídico, cuando, p. ej., en materia de protección de los derechos de los consumidores, el artículo 52.16 de la LEC admite la acción de cesación, en el caso de que el causante del daño no tenga establecimiento ni domicilio en territorio nacional.

[251] *Vid.*, en el mismo sentido, en relación con los supuestos de responsabilidad producidos a través de Internet, Guillermo PALAO MORENO, «Competencia..., *op. cit.*, pp. 283-284.

5. Solicitud de medidas cautelares o provisionales en litigios derivados de una transferencia internacional de datos de carácter personal ilícita

146. A continuación, me ocuparé concepto y régimen jurídico (A) y alcance (B) de las medidas cautelares o provisionales en litigios entre particulares en materia de transferencias internacionales de datos de carácter personal ilícitas.

A. Concepto y régimen jurídico de las medidas cautelares o provisionales en litigios entre particulares en materia de transferencias internacionales de datos de carácter personal ilícitas

147. La adopción de medidas cautelares o provisionales es bastante usual en los procedimientos por lesión de los derechos de la personalidad (derecho a la protección de datos de carácter personal). Este tipo de medidas resultan de gran importancia en este ámbito, ya que permiten al titular del derecho lesionado defender sus intereses de manera cautelar sin tener que esperar a la resolución sobre el fondo del asunto, evitando, al mismo tiempo, que los daños que puedan producirse puedan llegar a ser irreparables.

148. Las medidas cautelares o provisionales, como bien señala el propio TJUE, en aplicación del RB/CL 11/CB/[252] Tratado España-República de El Salvador, son aquellas que «van dirigidas a mantener una situación de hecho o de Derecho para salvaguardar los derechos cuyo reconocimien-

[252] Y del Reglamento «Bruselas I bis».

to se solicita, además, al juez que conoce del fondo del asunto».[253] Cualquier otra medida que persiga un fin distinto al señalado o que no encaje dentro de esta definición no podrá calificarse de *cautelares* o *provisionales* a los efectos del RBI/CL 11/CB/ Tratado España-República de El Salvador y, por tanto, el tribunal que se haya declarado competente para conocer del litigio derivado de la lesión del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita no podrá acudir a este fuero específico para fundamentar su competencia judicial internacional.

149. La modificación del RB[254] ha traído consigo la introducción de algunas novedades a la hora de que un tribunal pueda declararse competente para la adopción de medidas cautelares o provisionales:

a) El concepto de medidas cautelares y provisionales incluye, entre otras, las destinadas a obtener información o a conservar pruebas. No incluyen las medidas que no sean de naturaleza cautelar, como las que ordenan la audiencia de un testigo, lo que no impide la aplicación del Reglamento (CE) núm. 1206/2001 sobre obtención de pruebas.[255]

b) Se garantiza la libre circulación de las medidas cautelares y provisionales ordenadas por un órgano jurisdiccional competente en cuanto al fondo del asunto, siempre que el demandado haya sido citado antes de su adopción, o que la resolución que contenga la

---

253 STJUE de 26 de marzo de 1992, *Reichert y Kockler*, C-261/90, Rec. p. I-2149.

254 Art. 35 en el Reglamento «Bruselas I bis».

255 Considerando 25.º del 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 —Reglamento «Bruselas I bis»— (*DOUE* de 20/12/2012).

> medida le haya sido notificada antes de su ejecución. Lo anterior no impide su reconocimiento y ejecutividad de acuerdo con el Derecho nacional del Estado requerido. Cuando las medidas provisionales y cautelares sean ordenadas por un órgano jurisdiccional de un Estado miembro que no es competente en cuanto al fondo del asunto, su efecto se circunscribirse al territorio de ese Estado.[256]

150. La competencia para la adopción de las medidas cautelares o provisionales en materia civil y mercantil se traduce en la práctica en dos posibilidades: *1.ª)* basar la competencia en el propio sistema de foros de competencia judicial internacional previstos en el RB/CL 11/CB[257] o *2.ª)* puede basarse en el fuero cautelar específico del artículo 31 del RB/CL 11/CB,[258] en conexión con las diferentes reglas nacionales sobre competencia en materia de medidas cautelares o provisionales.

La que nos interesa es la primera de las opciones: el perjudicado puede solicitar las medidas directamente ante el tribunal que conoce del fondo del asunto (sobre la base de los fueros de los artículos 2 al 24 del RB/CL 11/CB),[259] lo que en estos litigios podría ser aquél que sea considerado como *lugar del hecho dañoso*. La adopción de tales medidas, sobre la base del artículo 5.3 del RB/CL 11/CB,[260] le correspondería tanto los tribunales del lugar donde la futura actividad tendría lugar

---

256 Considerando 33.º del 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 —Reglamento «Bruselas I bis»— (*DOUE* de 20/12/2012).

257 Y en el Reglamento «Bruselas I bis».

258 Art. 35 en el Reglamento «Bruselas I bis».

259 Art. 4 al 26 en el Reglamento «Bruselas I bis».

260 Art. 7.3 en el Reglamento «Bruselas I bis».

(futuro Estado de origen) como los tribunales del lugar donde finalmente se materializaría el futuro/s daño/s (futuro *loci damni)*, siguiendo la doctrina del TJUE: *Shevill* y posteriormente *eDate Advertising*.

151. Las medidas concretas que pueden solicitarse a tal fin puede hacerse con carácter cautelar o provisional o como medidas finales —de fondo o definitivas—. Esta calificación va a condicionar tanto la ley rectora de la medida, como el posible fuero de competencia del tribunal para adoptarlas. Si se trata de una medida definitiva (generalmente coetánea al ejercicio del derecho de reparación), será la ley aplicable al fondo la que concrete cuándo y cómo deben solicitarse, y cuáles. Si por el contrario es de carácter cautelar o provisional (aunque su adopción dependerá del Derecho del fondo: pues si según éste no existe ilícito, correlativamente no existirá justificación para adoptar la medida), deberá ser conforme con la ley procesal del Estado donde se solicita la tutela cautelar.

Y desde el punto de vista de la competencia judicial internacional —en el sistema RB/CL 11/CB—[261] esta condición también es esencial. Pues si es de fondo la medida tendrá que solicitarse ante aquellos tribunales que tengan reconocida competencia en función de los fueros generales o a la luz del fuero especial del artículo 5.3 del RB/CL 11/CB;[262] pero si es cautelar, además de la posible adopción sobre la base del fuero sobre el fondo, se prevé expresamente el fuero cautelar del artículo 31 RB/CL 11/CB.[263]

[261] Y Reglamento «Bruselas 1 bis».

[262] Art. 7.3 en el Reglamento «Bruselas 1 bis».

[263] Art. 35 en el Reglamento «Bruselas 1 bis».

Un dato relevante en aras a la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita es que cualquier Estado miembro podrá adoptar estas u otras medidas (siempre que sea compatibles con su Derecho interno) aunque el fondo del asunto esté siendo seguido en otro Estado (y regido por otro Derecho material), lo que le permitiría al Estado de origen de la transferencia internacional de datos de carácter personal ilícita adoptar las correspondientes medidas cautelares o provisionales a petición del afectado.

No obstante, debemos estar atentos dado que alguna de estas medidas conllevan la restricción de otros derechos (del causante del daño) que pueden ser considerados como fundamentales, para el caso de una supuesta validez extraterritorial de la medida más allá del territorio del foro pueden darse eventuales problemas por incidencia del orden público del tribunal del Estado requerido; además, en su caso, del posible alcance limitado connatural de estas medidas cautelares.

B. Alcance de las medidas cautelares o provisionales en litigios entre particulares en materia de transferencias internacionales de datos de carácter personal ilícitas

152. En cuanto al alcance de las medidas cautelares o provisionales frente lesiones al derecho a la protección de datos de carácter personal consecuencia de un tratamiento ilícito internacional debemos señalar que pueden solicitarse con independencia del medio utilizado, si bien la eficacia de la medida sí que puede estar condicionada por el medio utilizado.

El limitado alcance espacial de estas medidas no viene determinado por la naturaleza cautelar del fuero en el que se fundamenta el tribunal para su adopción sino que los mismos problemas va a plan-

tear estas medidas específicas cuando se hubieran adoptado con base en alguno de los fueros de competencia de fondo (art. 5.3 o art. 2 RB/CL II/CB[264] o art. 4.3 o art. 2 del Tratado España-República de El Salvador). El alcance espacial de la prohibición de actividad (p. ej., el tratamiento de los datos personales del afectado) está vinculado a la competencia judicial de base: la atribución de competencia judicial internacional vía artículos 5.3 o 2 del RB/CL II/CB[265] (o artículos 4.3 o 2 del Tratado España-República de El Salvador) permite obtener una cesación para cualquier Estado en los que puedan producirse efectos dañosos y, correlativamente, una competencia territorialmente limitada, como la del fuero del lugar del daño del art. 5.3, sólo puede ordenar la cesación respecto de los daños producidos en la jurisdicción del foro.[266]

153. El tribunal puede adoptar medidas cautelares o provisionales siempre que existan indicios racionales de carácter fáctico de que la lesión al derecho a la protección de datos de carácter personal se ha producido realmente, pero no en relación a hipotéticos hechos futuros. Es decir, previamente a la presentación de demanda preceptiva para la protección de su derecho a la protección de datos de carácter personal, aquella persona que cree vulnerado el mismo, ante ese mismo tribunal, podrá solicitar la adopción de medidas provisionales o cautelares como consecuencia de unos hechos anteriores y *denunciados* con antelación. En este contexto, para el caso de que el tribunal

---

[264] Art. 7.3 o 4 en el Reglamento «Bruselas I bis».

[265] Art. 7.3 en el Reglamento «Bruselas I bis».

[266] Este razonamiento se deriva de la doctrina *Shevill* en relación con las acciones indemnizatorias y de *eDate Advertising,* que ha extendido esta lógica a un litigio en el que también se había planteado una acción de cesación.

entienda que exista indicio de buen derecho a favor del actor —*fumus boni iuris*—, o si considera que el tiempo que puede transcurrir hasta la resolución del caso —*periculum in mora*—, puede poner en peligro, hasta el punto de hacer ineficaz, la posible sentencia favorable que recaiga, podrá adoptar una medida cautelar o provisional consistente en obligar al causante del daño a que cese en la intromisión. Por lo tanto, las medidas únicamente pueden solicitarse —y consecuentemente concederse— una vez que se haya consumado el ilícito (tratamiento ilícito internacional de datos de carácter personal).

6. La LOPJ como regla subsidiaria para los supuestos no contemplados ni por el régimen institucional ni por el régimen convencional en materia de transferencia internacional de datos de carácter personal ilícita

154. Tal y como prevé el artículo 4.1 del RB/CL II/CB,[267] cuando el demandado —el causante de la lesión del derecho a la protección de datos derivado de una transferencia internacional de datos de carácter personal— carece de domicilio en el *territorio Bruselas I* (RB), en el *territorio Lugano II* (CL II), o en el *territorio Bruselas* (CB), la competencia judicial internacional se debe determinar conforme a las normas del sistema autónomo del tribunal ante el cual se plantea la demanda, entrando en juego las disposiciones de la LOPJ; por tanto, el análisis se circunscribe a la respuesta que, desde el foro español, se ofrece a la evaluación prospectiva de la sede objetivamente competente para la resolución de controversias: por un lado, la sumisión expresa o tácita

[267] Art. 6.1 en el Reglamento «Bruselas I bis».

de las partes a los tribunales españoles: el artículo 22.2 de la LOPJ (A); y, por otro lado, el foro especial en responsabilidad civil extracontractual: el artículo 22.3 de la LOPJ (B).

A. Sumisión expresa o tácita de las partes a los tribunales españoles: el artículo 22.2 de la LOPJ

155. El régimen que establece el sistema de normas de conflicto español en la LOPJ es similar al que contienen los instrumentos institucionales y convencionales antes citados. Así, con carácter general, dispone la LOPJ que serán competentes los Tribunales españoles *cuando las partes así lo hayan pactado, expresa o tácitamente* (art. 22.2).

156. El artículo 22.2 de la LOPJ afirma que los tribunales españoles serán competentes «cuando las partes se hayan sometido expresa o tácitamente a los Juzgados o Tribunales españoles». El *acuerdo de sumisión* es un pacto entre las partes de una relación jurídica en cuya virtud éstas determinan el órgano jurisdiccional competente para conocer de los litigios que eventualmente pudieran surgir entre las partes. Tal sumisión puede realizarse mediante acuerdo *expreso* o mediante ciertas prácticas que denotan la voluntad de las partes de someterse a un órgano jurisdiccional: es la sumisión *tácita*.

Debido al carácter supletorio de la LOPJ frente a la normativa de origen no interno, la aplicación de aquélla se determinará por exclusión de la segunda; esto es, mediante una lectura a contrario de las disposiciones que establecen el ámbito de aplicación del RB/CL II/CB/[268] Tratado España-República de El Salvador. Bastará con

[268] Y del Reglamento «Bruselas I bis».

que no concurra una sola de las circunstancias que determinan la aplicación del artículo 23 RB/CL II,[269] del 17 CB o del 5.2 del Tratado España-República de El Salvador para que el acuerdo atributivo de jurisdicción se rija por el artículo 22.2 de la LOPJ.

157. Para que el acuerdo de *sumisión expresa* sea válido, en la materia que nos ocupa, es necesario, fundamentalmente, que se designen claramente los tribunales a los que se someten las partes. El 22.2 de la LOPJ permite que la designación de los tribunales españoles como competentes sea genérica o concreta. El acuerdo de sumisión expresa puede realizarse en cualquier momento, antes o después de la conclusión de un contrato o negocio internacional. Además, podrá realizarse en cualquier forma, rigiendo el principio de libertad de forma propio de nuestro sistema. Se debe probar, no obstante, el auténtico consentimiento de las partes, ya que el acuerdo ha de producirse de forma clara, explícita y bilateral, estableciéndose la renuncia al fuero propio y la designando aquél al que se someten las partes.

158. El citado artículo 22.2 de la LOPJ contempla como foro de competencia la *sumisión tácita*. Como ya hemos señalado, se entiende que las partes se someten tácitamente a los tribunales españoles cuando el demandante acude a tales tribunales interponiendo la demanda o formulando petición o solicitud que haya de presentarse ante el tribunal competente para conocer de la demanda, y cuando el demandado realiza, después de personado en el juicio tras la interposición de la demanda, cualquier gestión que no sea la de proponer en forma la declinatoria.

[269] Art. 25 en el Reglamento «Bruselas I bis».

Por otro lado, según prevé el propio artículo 22.2 de la LOPJ, son competentes los tribunales españoles cuando *el demandado tiene su domicilio en España*.

No obstante, en la práctica, el juego del artículo 22.2 —sumisión expresa o tácita y domicilio del demandado— es escaso, ya que opera con carácter general el RB (en particular, los arts. 24, 23 y 2).[270]

B. Foro especial en responsabilidad civil extracontractual: el artículo 22.3 de la LOPJ

159. En defecto de cláusula de elección de foro, cuando el demandado está domiciliado en un tercer Estado los tribunales españoles se pueden declarar competentes de acuerdo con el apartado 3 del artículo 22 de la LOPJ. La posición jerárquicamente superior que ocupa el RB en los ordenamientos jurídicos de los Estados miembros de la UE respecto de las normas de producción interna implica la desactivación de ciertos foros de competencia previstos en ciertas disposiciones de la LOPJ. Esto ocurrirá cuando los elementos necesarios para su aplicación sean los mismos que los establecidos en los foros previstos en el RB/CL 11/CB.[271]

Indica el artículo 22.3 de la LOPJ que, en materia de obligaciones extracontractuales, serán competentes los tribunales españoles «cuando el hecho del que deriven haya ocurrido en territorio español o el autor del daño y la víctima tengan su residencia habitual común en España».[272]

---

[270] Art. 26, 25 y 4 en el Reglamento «Bruselas I bis».

[271] Y en el Reglamento «Bruselas I bis».

[272] El concepto de «obligaciones extracontractuales» que emplea el artículo 22.3 de la LOPJ debe extraerse del Derecho material español. Cubre las «obligaciones ex-

160. Si el demandado dispone de domicilio en España, será aplicable el RB y el artículo 5.3 [273] del mismo y nunca el artículo 22.3 de la LOPJ. Este último (art. 22.3 de la LOPJ) incluye dos foros de competencia judicial internacional en materia no contractual para la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita:

a) Primer foro de competencia judicial internacional: cuando es España el lugar del hecho del que deriven las obligaciones extracontractuales. La precisión de este lugar del hecho del que deriven las obligaciones extracontractuales debe realizarse con arreglo a las mismas pautas hermenéuticas ya empleadas para precisar la misma noción en el artículo 5.3 del RB,[274] ya que dicho precepto fue el modelo que sirvió de directa inspiración al legislador español que elaboró el artículo 22.3 de la LOPJ.

b) Segundo foro de competencia judicial internacional: «residencia habitual común de las partes en España». Este foro es totalmente inaplicable en la actualidad, pues si ambos sujetos disponen de residencia habitual en España, la competencia judicial internacional se regirá, exclusivamente, por el artículo 2 del RB[275] y nunca por la LOPJ, ya que en Derecho español, la *residencia habitual* equivale a *domicilio* y si el demandado está domiciliado en España la compe-

---

tracontractuales» en el sentido recogido en el artículo 1089 del CC y también las derivadas de un enriquecimiento injusto (AAP Barcelona 2 mayo 1994), cobro de lo indebido (STS 29 noviembre 1991) y gestión de negocios.

[273] Art. 7.3 en el Reglamento «Bruselas I bis».

[274] Art. 7.3 en el Reglamento «Bruselas I bis».

[275] Art. 4 en el Reglamento «Bruselas I bis».

tencia judicial internacional de los tribunales españoles se regula enteramente por el RB y la LOPJ resulta inaplicable.[276]

161. La competencia territorial en estos casos vendrá determinada según lo previsto en el artículo 52.6 de la LEC para las reclamaciones del afectado (será competente el tribunal del domicilio del demandante, y cuando no lo tuviere en territorio español, el tribunal del lugar donde se hubiera producido el hecho que vulnere el derecho fundamental de que se trate).

7. Balance final

162. Resulta razonable llevar a cabo una interpretación de los foros de competencia judicial internacional con el fin de que: por un lado, se garantice un correcto equilibrio entre los distintos intereses en presencia y el sistema responda, por un lado, al principio de proximidad; y, por otro, prevea una protección eficaz del titular del derecho a la protección de datos de carácter personal, derivada de una transferencia internacional ilícita.

163. Ahora bien, aun forzando al máximo las posibilidades hermenéuticas del sistema —en el sentido más favorable de la víctima que se quiera *(forum damni)*— los criterios de competencia judicial internacional vigentes no son adecuados para procurar una protección adecuada, equilibrada y eficaz del perjudicado por una transferencia internacional ilícita de información personal sensible.

---

[276] *Vid.* Diana SANCHO VILLA, Negocios Internacionales..., op. cit., p. 238.

164. La tutela que precisaría un supuesto de tratamiento ilícito internacional de datos, para reequilibrar las posiciones de las partes, requeriría interpretar el *forum delicti commissi* en un sentido favorable a la víctima. Esto es, identificándolo con el lugar de residencia habitual del perjudicado. Propuesta que es consciente de las habituales y compartibles críticas generales al denominado *forum actoris*, pero perfectamente defendible en este caso por su adecuación a las necesidades tuitivas del supuesto tipo y, además, acorde con la jurisprudencia más reciente del TJUE (Sentencia de 25 de octubre de 2011, *eDate Advertising* (C-509/09) y *Martínez y Martínez* (C-161/10)). Habrá, por tanto, que remitirse al *lugar de residencia habitual de la víctima*, aunque no como lugar del hecho dañoso, sino como *lugar de realización global de la acción generadora de dicha responsabilidad extracontractual*.

165. De esta forma, la atribución de competencia judicial internacional a los tribunales del Estado donde resida la víctima del daño proporcionaría a ésta la tutela adecuada, equilibrada y efectiva precisa para paliar los efectos negativos de su inicial situación de inferioridad jurídica.

166. Así las cosas, hemos visto como el recurso a la resolución judicial de controversias se presenta, *a priori*, como la solución más factible para procurar una protección adecuada, equilibrada y eficaz del perjudicado por una transferencia internacional ilícita de información personal sensible. A continuación, en el **capítulo IV** incidiré en la idea de que el Derecho internacional privado se presenta como el sistema normativo más sencilla y manifiestamente mejorable para obtener una tutela adecuada, equilibrada y efectiva; ya sea reinterpretando a favor del perjudicado las normas vigentes de derecho aplicable; ya sea reformando en sentido tuitivo dicha normativa.

Capítulo IV.

Mecanismos de resolución de controversias para la protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita: determinación de la ley aplicable

167. En un orden lógico de cosas, una vez definido, deslindado y perfilado el objeto de estudio en el **capítulo** I, estudiadas, en el **capítulo** II, las normas que se proyectan sobre el supuesto tipo; y en el **capítulo** III analizados los diferentes mecanismos de resolución de controversias a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, para obtener una tutela adecuada, equilibrada y efectiva, es el momento de ocuparnos, en este **capítulo** IV, de los problemas de determinación de la ley aplicable en los litigios por vulneración del derecho a la protección de datos derivado de una transferencia internacional de datos de carácter personal ilícita.

La idea que subyace en este **capítulo** IV es clara: determinar la respuesta del ordenamiento jurídico español para la resolución material de un litigio por el tratamiento ilícito internacional de datos de carácter personal. Para ello, en particular, tras dar una panorámica del régimen jurídico de protección para la determinación de la ley aplicable a las transferencias internacionales de datos de carácter personal previsto en la Directiva 95/46/CE y en la LOPD (I), analizaré las normas de conflicto materialmente orientadas a la protección del titular del derecho a la protección de datos ante el tratamiento ilícito inter-

nacional de sus datos de carácter personal: el Reglamento «Roma II» actual (II) y el artículo 10.9 del código civil (III), el ámbito de aplicación de la ley designada para regir la responsabilidad civil extracontractual derivada de una transferencia internacional de datos de carácter personal ilícita (IV); para, finalmente, tratar de dar respuesta a una pregunta: si para la protección en la UE del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita ¿debemos apostar por la configuración de una norma de conflicto materialmente orientada a la protección de datos de carácter personal? (V).

1. RÉGIMEN DE PROTECCIÓN, TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL Y DETERMINACIÓN DE LA LEY APLICABLE SEGÚN LA DIRECTIVA 95/46/CE Y LA LOPD

168. La determinación de la ley aplicable en materia de responsabilidad civil extracontractual derivada de un tratamiento ilícito internacional de datos de carácter personal ilícita implica alinearse en alguno de estos dos bandos: el de la liberalización de la circulación de datos de carácter personal, o el de la salvaguarda del derecho fundamental a la protección de datos; ya que queda, como veremos, básicamente, en manos de dos preceptos:[277] *a)* el artículo 4.1 de la Directiva 95/46/CE, que señala como ley aplicable la ley del lugar donde esté ubicado el responsable del fichero de datos de carácter personal (**1**); o, *b)* el ar-

[277] *Vid.* Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001, pp. 154-155.

tículo 2.1 de la LOPD, que, por el contrario, establece como ley aplicable la ley del lugar donde se haya efectuado el tratamiento de los datos de carácter personal[278] (2). Así las cosas, sólo será de aplicación la LOPD, esto es la ley española, cuando el tratamiento de los datos de carácter personal sea efectuado en territorio español, en el marco de las actividades de un establecimiento del responsable del tratamiento; mientras que, cuando no sea así, será de aplicación la ley del Estado de residencia del responsable del fichero, en virtud de la Directiva 95/46/CE.[279]

1. Transferencia internacional de datos de carácter personal y determinación de la ley aplicable según la Directiva 95/46/CE

169. El artículo 4.1 de la Directiva 95/46/CE reparte la competencia legislativa entre los Estados miembros. Permite la determinación de la ley aplicable del Estado miembro donde el tratamiento sea efectuado en el marco de las actividades del responsable del tratamiento en el territorio de ese Estado miembro.[280]

---

278 Nos encontramos ante dos preceptos que, por su contradicción, inducen a la confusión, que cubren tanto las relaciones administrativas como las relaciones entre particulares en asuntos internacionales, y que aparecen preocupadas por fijar el ámbito de aplicación de la normativa del Estado cuyos tribunales conocen del asunto. *Vid.*, *ibídem,* p. 156-157.

279 *Vid.* Pedro DE MIGUEL ASENSIO, *Derecho privado de Internet*, 4.ª ed., Civitas, Cizur Menor (Navarra), 2011, pp. 332-335.

280 *Vid.* Diana SANCHO VILLA, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003, p. 95.

Por «establecimiento» debe entenderse (Considerando 19.º de la Directiva 95/46/CE)[281] el lugar donde se lleva a cabo el «ejercicio efectivo y real de una actividad mediante una instalación estable», cualquiera que sea su forma jurídica: sucursal, filial, con o sin personalidad jurídica, etc.

170. La Directiva 95/46/CE apuesta por el país de residencia del responsable del fichero como punto de conexión. El criterio elegido para establecer la ley aplicable es el *país de situación del establecimiento del responsable del fichero que trata los datos de carácter personal*. No interesa ni el lugar de tratamiento de los datos de carácter personal ni la nacionalidad ni la residencia de la víctima del tratamiento de los datos de carácter personal.[282]

La solución apuntada por la Directiva 95/46/CE, en mi opinión, beneficia a las empresas que se encargan del tratamiento y/o transferencia de datos de carácter personal en detrimento de las personas físicas titulares de los datos de carácter personal objeto de tratamiento y/o transferencia por varias razones:

a) No se aplica la ley del país donde se produce el tratamiento ilícito de los datos personales del afectado *(lex loci delicti commissi)* sino la *ley del país del establecimiento del responsable del tratamiento de los datos*: «sean cuales sean los países en los que la empresa

---

[281] El Considerando 19.º matiza que «el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable», siendo irrelevante al respecto la forma jurídica del establecimiento: simple sucursal o filial con personalidad jurídica.

[282] *Vid.* Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes...*, *op. cit.*, p. 157.

desarrolle sus actividades, la ley aplicable al tratamiento de datos será siempre la misma ley, la ley del fichero».[283]

b) Se apuesta por una ley conocida por las empresas que se encargan del tratamiento y/o transferencia de datos de carácter personal: «la empresa que trata datos personales en la UE no debe informarse sobre el contenido de las leyes de los países comunitarios donde opera, pues tales leyes no son aplicables nunca a sus actividades. Le basta con conocer su propia ley y acomodarse a ella».[284]

c) Se le evita a las empresas que se encargan del tratamiento y/o transferencia de datos de carácter personal una multiplicidad de leyes: «la empresa que trata los datos queda sometida a un mismo Derecho nacional tanto por lo que respecta a sus relaciones administrativas con las Autoridades públicas, como por lo que se refiere a las relaciones con los particulares afectados por el tratamiento de datos».[285]

Bien, pues, en virtud de la Directiva 95/46/CE, son tres los supuestos que debemos diferenciar a la hora de determinar la ley aplicable: ***A)*** Cuando el responsable del tratamiento de los datos cuenta con un establecimiento en un Estado miembro; ***B)*** Cuando el responsable del tratamiento de los datos cuenta con establecimiento en un lugar en el que se aplica la legislación de un Estado miembro en virtud del Derecho internacional público; y ***C)*** Cuando el responsable del tratamiento

---

283 Alfonso-Luis Calvo Caravaca y Javier Carrascosa González, *Conflictos de leyes...*, *op. cit.*, p. 159.

284 Alfonso-Luis Calvo Caravaca y Javier Carrascosa González, *Conflictos de leyes...*, *op. cit.*, pp. 159-160.

285 Alfonso-Luis Calvo Caravaca y Javier Carrascosa González, *Conflictos de leyes...*, *op. cit.*, p. 160.

de los datos no cuenta con un establecimiento en la UE pero el tratamiento de datos personales realiza a través de medios situados en el territorio de un Estado miembro.

A. Ley del Estado miembro en el que se halla el establecimiento del responsable del tratamiento de los datos

171. La ley que el receptor de los datos va a aplicar a su tratamiento será, en principio, la ley del Estado donde esté domiciliado (art. 4.1.a y c de la Directiva 95/46/CE). El tratamiento de los datos efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento se rige por la ley del Estado miembro en el que se halla dicho establecimiento. No es relevante ni el *lugar de tratamiento de los datos*, ni la *nacionalidad*, ni el *domicilio* o *residencia habitual* del sujeto cuyos datos se tratan, y menos la *nacionalidad*, *domicilio* o *residencia habitual* del sujeto responsable del tratamiento. Lo único que importa es el lugar de su *establecimiento*.

172. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros, las actividades que desarrolla cada establecimiento quedarán sujetas al Derecho del Estado miembro donde radique dicho *establecimiento* (art. 4.1.a *in fine* de la Directiva 95/46/CE). Si el responsable del tratamiento se encuentra establecido sólo en un país de la UE, aunque se lleven a cabo tratamientos en otros Estados miembros de la UE, se regirán por la ley del Estado de su establecimiento (art. 4.1.2 de la Directiva 95/46/CE).

B. Ley aplicable y responsable del tratamiento de los datos con establecimiento en un lugar en el que se aplica la legislación de un Estado miembro en virtud del Derecho internacional público

173. Cuando el responsable del tratamiento de los datos tiene su establecimiento en un lugar en el que se aplica la legislación de un Estado miembro en virtud del Derecho internacional público, el tratamiento de los datos se regirá por la ley de dicho Estado miembro. Este supuesto está diseñado para establecimientos situados en territorios que, aunque no forman parte del territorio de un Estado Miembro de la UE, *reciben* la legislación de ese Estado (p. ej., territorios de ultramar o antiguas colonias). El supuesto de las Embajadas y Consulados es más complejo. El tratamiento de los datos efectuado en dichos lugares debe sujetarse al criterio general: se aplicará la ley del Estado donde radique el establecimiento del responsable del tratamiento, con independencia del Estado de situación de la Embajada o Consulado.[286]

Cuando el responsable del tratamiento de los datos tenga su establecimiento en la misma Embajada o Consulado, deben diferenciarse dos casos: *1.º)* si la sede diplomática o consular se halla en un Estado miembro de la UE: entonces, rige el criterio general: se aplica la ley del Estado donde se halla la Embajada o Consulado (art. 4.1.b *a contrario* de la Directiva 95/46/CE); y, *2.º)* si la Embajada o Consulado se halla sita en un Estado no miembro de la UE: entonces, puede ser aplicable el artículo 4.1.b de la Directiva 95/46/CE: se puede conside-

[286] *Vid.* Alfonso-Luis Calvo Caravaca y Javier Carrascosa González, *Conflictos de leyes...*, *op. cit.*, p. 162.

rar que en la sede diplomática o consular sita fuera de la UE se aplica la legislación de un Estado miembro de la UE.[287]

174. No obstante, este criterio del artículo 4.1.b de la Directiva 95/46/CE sólo puede entenderse si se refiere al caso de los tratamientos que tengan lugar en localidades sujetas a las reglas de extraterritorialidad, en dependencias de Embajadas, Consulados, etc. En este caso, se aplicará la «ley nacional del Estado miembro del responsable del tratamiento de los datos»; y, el apartado *c* del artículo 4.1 de la Directiva 95/46/CE aspira a evitar que el responsable del tratamiento de los datos evada las disposiciones nacionales de protección de datos, valiéndose del recurso de establecerse en un Estado no miembro, aun cuando los medios con que se lleva a cabo el tratamiento de datos radiquen en el ámbito de la soberanía de un Estado miembro (Considerando 20.º de la Directiva 95/46/CE).

C. Ley aplicable y responsable del tratamiento de los datos sin establecimiento en la UE y tratamiento de datos personales a través de medios situados en el territorio de un Estado miembro

175. Cuando el responsable del tratamiento de datos no dispone de un establecimiento en la UE pero recurre, para el tratamiento de datos personales, a *medios*, automatizados o no, situados en el territorio de dicho Estado miembro, el tratamiento de datos personales se regirá por la ley del Estado miembro en cuyo territorio el responsable del tratamiento utiliza tales «medios» para el procesamiento de datos.

---

[287] *Vid.* Alfonso-Luis Calvo Caravaca y Javier Carrascosa González, *Conflictos de leyes...*, *op. cit.*, pp. 162-163.

176. El concepto de *medios* comprende los ordenadores personales, terminales, servidores informáticos, cámaras de televisión, el *software* espía, etc. que recogen automáticamente datos de carácter personal del usuario, y los servidores que se utilizan para el tratamiento de dichos datos (p. ej., la colocación de *cookies* en el ordenador del usuario que se conecta a la página *web* de un empresario establecido en un tercer Estado o la descarga de *javascript* por parte del usuario para acceder a los contenidos de esa página *web*, mediante los cuales el empresario recabe datos de carácter personal para su tratamiento). Es decir: tales instrumentos y mecanismos deben ser utilizados para procesar datos; así, p. ej., para captar datos o almacenarlos con el objetivo de su tratamiento futuro.[288]

La Directiva 95/46/CE nada dispone sobre la ley aplicable al tratamiento de datos realizado en el territorio de terceros Estados sin intervención de medios técnicos ubicados en la UE. Ello explica que la Directiva 95/46/CE someta a un régimen muy estricto la circulación de datos personales desde la UE con destino a terceros Estados.

Sin duda alguna, los supuestos en los que el responsable del tratamiento se encuentra establecido en un tercer Estado es uno de los aspectos más controvertidos de la legislación europea sobre protección de datos personales. Para garantizar que el estándar de protección de la UE no deja de aplicarse cuando el responsable del tratamiento tiene su establecimiento en un tercer Estado, se prevé que la aplicación de la ley del Estado miembro en cuyo territorio se encuentren situados los medios, ya sean automatizados o no, a los que recurra el respon-

[288] La utilización de estos mecanismos para un *mero tránsito* de datos con destino a otro país no provoca la aplicación de la ley del Estado miembro donde se emplean dichos *medios* (art. 2.1.c de la LOPD –y el art. 3.1.c del RLOPD– y art. 4.1.c de la Directiva 95/46/CE).

sable para el tratamiento de datos personales, salvo que los utilice con fines de mero tránsito (art. 4.1.c Directiva 95/46/CE).

177. Fundamental en la interpretación del significado del artículo 4.1.c ha sido la labor del Grupo de Trabajo del artículo 29 en la medida en que propone la revisión de la situación actual para superar las carencias que derivan de la redacción actual del mencionado artículo 4.1.c y de sus consecuencias conforme a los criterios previamente establecidos hasta la fecha.[289]

Aunque es cierto que el Grupo de Trabajo del artículo 29 había señalado ya previamente que el concepto *recurrir* utilizado en el artículo 4.1.c Directiva 95/46/CE presupone un determinado tipo de actividad emprendida por el responsable y su intención de tratar datos personales, de modo que no todo *recurso* a *medios* dentro de la UE llevaría a la aplicación de la Directiva, lo cierto es que su criterio, confirmado en reiteradas ocasiones, es que el artículo 4.1.c Directiva 95/46/CE impone la aplicación del régimen de protección de datos de la UE en los diversos supuestos en los que, p. ej., los titulares de sitios web o los prestadores de servicios a través de Internet, que no estén establecidos en la UE, emplean dispositivos para la recogida activa de datos procedentes de los ordenadores u otros dispositivos de los usuarios situados en Estados miembros, así como cuando el sitio *web* envía con el propósito de recoger y tratar información personal herramientas como los *javascript* al ordenador del usuario que permiten a servidores remotos ejecutar aplicaciones en el ordenador del usuario.

[289] Dictamen 8/2010 sobre la ley aplicable, de 16 de diciembre de 2010 del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE.

Se trata de un planteamiento que lleva a exigir el cumplimiento de la legislación europea en situaciones en las que la conexión con la UE es escasa y su aplicación excesiva, entre otros motivos porque abarca supuestos en los que el tratamiento de datos puede ser meramente accidental.

Lo que representa una notable evolución en este Dictamen del Grupo de Trabajo del artículo 29 es que concluye que el criterio basado en el uso de medios en la UE ha demostrado conducir a consecuencias no deseables, y de que, en consecuencia, que este criterio no resulta apropiado que ese criterio opere tal como está previsto en la actualidad. En nuestra opinión, una sustancial mejora de la situación vendría representada por la inclusión de un requisito que subordinara la aplicación de la legislación europea a que el responsable del tratamiento dirija su actividad a personas situadas en la UE.[290]

178. Sin duda alguna, pensamos que el criterio apuntado por el artículo 4.1 de la Directiva 95/46/CE no nos parece el más adecuado pues favorece la indefensión del titular del derecho a la protección de datos de carácter personal ante la territorialidad de la competencia de cada autoridad nacional de protección de datos.

Si una persona física considera que se ha vulnerado su derecho a la protección de datos de carácter personal si bien podrá reclamar la correspondiente indemnización por daños y perjuicios ante los tribunales del lugar donde él resida (art. 5.3 del RB/CL II/CB[291] o 4.3 del Tratado España-República de El Salvador), lo deberá hacer en base a un Derecho extranjero. Deberá probar la existencia, vigencia, conteni-

---

290 *Vid.*, Pedro De Miguel Asensio, *Derecho privado..., op. cit.*, pp. 335-338.

291 Ap. 3 del art. 7 en el Reglamento «Bruselas I bis».

do y aplicación al caso litigioso del Derecho del país donde se halla establecido el responsable del fichero de datos. Esta *carga* puede, en la práctica, disuadir al afectado de la presentación de la demanda ante los tribunales. En definitiva, «menos demandas en contra, menos gastos, mayor eficiencia» para las empresas que se encargan del tratamiento y/o transferencia de datos de carácter personal.[292]

Podríamos pensar que esa *carga*, en la práctica, no será tal, pues los diferentes Derechos extranjeros, al menos en el ámbito de la UE, presentan un contenido similar y un nivel de protección del afectado equivalente ya que derivan de una norma común: la Directiva 95/46/CE;[293] pero, en la práctica, como veremos, la realidad es otra. La protección del afectado dependerá del Estado miembro en cuestión, consecuencia de la transposición, interpretación y aplicación práctica que haya realizado de la propia Directiva 95/46/CE.[294]

179. La Directiva 95/46/CE, aunque no lo hizo entonces (su *ratio* era favorecer al responsable del fichero y no al afectado), hoy día, debería corregir, reinterpretarse y apostar por otra solución en aras a la protección del titular del derecho a la protección de datos ante un tratamiento ilícito internacional de sus datos de carácter personal. La pro-

---

[292] *Vid.* Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes...*, *op. cit.*, pp. 161-162.

[293] *Vid.*, en ese sentido, Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes...*, *op. cit.*, p. 162.

[294] *Vid.* Mónica ARENAS RAMIRO, «La protección de datos personales en los países de la Unión Europea», en *Revista Jurídica de Castilla y León*, núm. 16, Septiembre 2008, pp. 113-168.

ximidad debe guiar al legislador comunitario a la hora de interpretar y aplicar esta norma de conflicto. El resultado material debe ser otro.[295]

Como soluciones alternativas a la *ley del país del establecimiento del responsable del tratamiento de los datos* se pueden enumerar las siguientes: *a)* la *ley del Estado del domicilio o residencia del titular de datos, que han sido tratados ilícitamente*; *b)* la *ley del Estado en el que las operaciones de tratamiento de datos tengan lugar*; o, *c)* una combinación de las opciones *a* y *b* y de la *ley del Estado del establecimiento del responsable del tratamiento de datos*. Es evidente que todas estas opciones pueden ofrecen algunos *aspectos vulnerables*: que un mismo titular del derecho a la protección de sus datos pueda tener residencia en más de un Estado o dar lugar a una pluralidad de leyes aplicables, resultado de aplicar la ley del Estado de residencia del titular de datos y la ley del Estado de establecimiento. Ahora bien, vulnerabilidad a un lado, el objetivo último es que la ley aplicable garantice un nivel de protección adecuado y favorezca al afectado en la defensa de su derecho a la protección de datos de carácter personal en el marco de un tratamiento ilícito internacional de datos de carácter personal; y, sin duda alguna, aplicando la *ley del país del establecimiento del responsable del tratamiento de los datos* la desprotección de aquél está servida.

[295] *Vid.*, en sentido contrario, Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes...*, *op. cit.*, pp. 158-161.

2. Transferencia internacional de datos de carácter personal y determinación de la ley aplicable según la LOPD

180. El tratamiento de datos de carácter personal queda sujeto a la ley española (LOPD) en los tres casos siguientes: Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento (A), cuando al responsable del tratamiento no establecido en territorio español, pero le sea de aplicación la legislación española en aplicación de normas de Derecho internacional público (B), y Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos, *medios* situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito (C).

A. Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento

181. Se utiliza el criterio *lugar de tratamiento de los datos* (art. 2.1.a de la LOPD y 3.1.a del RLOPD)[296] y no el del *lugar de establecimiento del responsable del fichero*, que es lo que indica la Directiva 95/46/CE. Ante tal contradicción normativa, debe dejarse claro que el artículo 2 de la LOPD (y su corolario el artículo 3 del RLOPD) nunca debe ni puede aplicarse cuando comporte vulneración de la Directiva

[296] *Vid.* Diana Sancho Villa, «Protección de datos personales y transferencia internacional: cuestiones de ley aplicable», en *Revista Jurídica de Castilla y León*, núm. 16, Septiembre 2008, pp. 409-411.

95/46/CE. Por tanto, si el lugar del tratamiento de los datos es España, pero el responsable de dicho tratamiento tiene su establecimiento en Bélgica, la ley belga sería aplicable. Y no la ley española. No obstante, el artículo 3.1 del RLOPD[297] introduce cierta incertidumbre: según tal precepto se regirá por dicho Reglamento todo tratamiento de datos de carácter personal «cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español».

Lo esencial es, en definitiva, que el tratamiento que realiza el responsable se produzca en su establecimiento en España para que sea de aplicación la LOPD.

[297] El artículo 3 del RLOPD, al regular su ámbito de aplicación territorial, introduce aparentemente ciertas diferencias con el régimen general previsto en el artículo 2.1 de la LOPD, al delimitar los supuestos de ley aplicable al responsable y al encargado del tratamiento. Si el encargado del tratamiento ubicado en España cuando actúen en relación con un tratamiento realizado en el marco de la actividad del establecimiento de un responsable del tratamiento situado en otro Estado no se encontrarán sometidos ni a la LOPD ni al RLOPD. Ahora bien, esta regla tiene dos excepciones: *1.ª)* Si el encargado del tratamiento lo es de un responsable cuyo establecimiento se encuentra ubicado fuera de la UE se aplicará la ley española (art. 3.c del RLOPD); y, *2.ª)* Cuando el establecimiento del responsable se encuentre ubicado en otro Estado miembro de la UE será de aplicación al encargado del tratamiento las normas del RLOPD en materia de seguridad de los ficheros y tratamiento de datos (art. 3.a del RLOPD).

B. CUANDO AL RESPONSABLE DEL TRATAMIENTO NO ESTABLECIDO EN TERRITORIO ESPAÑOL, PERO LE SEA DE APLICACIÓN LA LEGISLACIÓN ESPAÑOLA EN APLICACIÓN DE NORMAS DE DERECHO INTERNACIONAL PÚBLICO

182. Este criterio (art. 2.1.c de la LOPD y 3.1.c del RLOPD),[298] que es idéntico al recogido en el artículo 4.1.b de la Directiva 95/46/CE, está pensando en la aplicación de la normativa española de protección de datos por parte de las autoridades consulares y diplomáticas en el ejercicio de sus funciones.[299]

A tenor del artículo 2.1.b de la LOPD será de aplicación la ley española cuando las normas de Derecho internacional público así lo prevean, de forma que los tratamientos de datos realizados por una oficina consular o misión diplomática quedarán sujetos a la ley estatal que acredite dicha oficina consular o misión diplomática.

C. CUANDO EL RESPONSABLE DEL TRATAMIENTO NO ESTÉ ESTABLECIDO EN TERRITORIO DE LA UNIÓN EUROPEA Y UTILICE EN EL TRATAMIENTO DE DATOS, «MEDIOS» SITUADOS EN TERRITORIO ESPAÑOL, SALVO QUE TALES MEDIOS SE UTILICEN ÚNICAMENTE CON FINES DE TRÁNSITO

183. Este criterio (art. 2.1.b de la LOPD y 3.1.b del RLOPD),[300] idéntico al recogido en el artículo 4.1.c de la Directiva 95/46/CE, cubre

---

298 *Vid.*, *ibídem,* p. 415-416

299 El art. 5.f del Convenio de Viena sobre relaciones consulares enumera las funciones de los agentes consulares entre las que se encuentran su actuación en calidad de notario, funcionario de registro civil y en funciones similares y de carácter administrativo, siempre que el Estado receptor no se oponga.

300 *Vid.*, *ibídem,* p. 412-415.

aquellas situaciones en las que el interesado se vería privado de la protección europea que normalmente le correspondería, como consecuencia de una maniobra fraudulenta del responsable del tratamiento de datos: supuestos en los que el responsable se establece artificialmente en un Estado no miembro de la UE con el fin de evitar la legislación europea: la Directiva 95/46/CE.

184. El concepto *utilización de medios* es algo genérico (localización del ordenador del usuario, utilización de las líneas de los operadores de telecomunicaciones o la instalación del proveedor del servicio en España); no obstante, dos elementos deben darse: *a)* por una parte, deben tratarse de instrumentos que posibiliten un tratamiento de datos; y, *b)* por otra, dichos medios deben ser permanentes y no de mero tránsito (p. ej., como ya se ha indicado, la colocación de *cookies* en el ordenador del usuario o la utilización de *javasript* por parte del usuario). La aplicación de este precepto a empresarios establecidos fuera de la UE reviste cierta complejidad en el contexto de Internet. Operaciones como el acceso a páginas *web* extranjeras o la descarga de *software* de estas páginas obligan a preguntarse si la legislación sobre protección de datos del país donde se localiza el equipo del usuario (medio) es de aplicación o no al tratamiento que resultase de los datos así recabados. Pensamos que no, pues si la respuesta fuese afirmativa, habríamos optado por una aplicación casi global de la normativa europea de protección de datos en Internet a través de la ley de transposición del Estado miembro donde se localiza el equipo del usuario, lo que, sin duda, contravendría el espíritu de la propia Directiva 95/46/CE: asegurar la libre circulación de datos de carácter personal.

La LOPD no define qué debe entenderse por la «utilización de un medio en España que no sea de mero tránsito». Si bien un *medio* puede ser un ordenador personal, una terminal, o un servidor informático,

lo relevante no es la existencia del medio sino su «utilización a los fines del tratamiento en España por parte del responsable», esto es, la intención del responsable de procesar los datos recabados; pues no toda utilización de un medio en España supone la aplicación de la ley española al responsable extranjero: quedan excluidos, tanto los supuestos en los que se utilizan elementos en España *accesorios* (p. ej., la utilización del servidor español para almacenar los datos, o la utilización de las líneas en España de los operadores de telecomunicaciones) como los datos que un usuario residente en España envía desde su ordenador conectado a un responsable establecido en un Estado no miembro de la UE (p. ej., le envía un email).[301]

[301] Una interpretación que podemos hacer para modular el alcance de la aplicación de la normativa europea de protección de datos a páginas *web* de responsables establecidos en terceros Estados es la que sugiere la aplicación del concepto de *actividad dirigida*: extender la aplicación de las normas imperativas europeas de protección del consumidor (afectado) del país de residencia al contrato que celebre con un profesional (responsable) establecido en un tercer Estado a través de la página *web* de este último, sin que conste la utilización de medios en España, cuando el profesional (responsable) dirige su actividad al país de la residencia del consumidor (afectado).

II. EL REGLAMENTO «ROMA II» ACTUAL Y SU EXCLUSIÓN RESPECTO A LAS OBLIGACIONES DERIVADAS DE LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS EN EL MARCO DE UNA TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL ILÍCITA

185. No podemos analizar la determinación de la ley aplicable a los supuestos de responsabilidad civil extracontractual[302] por vulneración del derecho fundamental a la protección de datos, derivada de una transferencia internacional de datos ilícita, sin acudir a una norma comunitaria de relativo reciente cuño: el Reglamento «Roma II»;[303]

---

[302] La vulneración del derecho a la protección de datos, como derecho de la personalidad que es, se califica como un supuesto de «responsabilidad civil *ex delicto*», pues lo relevante es la *reacción jurídica* frente a un comportamiento ajeno lesivo del derecho, y no lo que el sujeto está facultado a hacer en *ejercicio positivo* de su derecho. Con arreglo a esta calificación, la ley aplicable será la ley del país donde se ha producido la vulneración del derecho a la protección de datos. *Vid.* Javier CARRASCOSA GONZÁLEZ, «Circulación internacional de datos personales informatizados y la Directiva 95/46/CE», en *Actualidad Civil*, núm. 23, 1997, p. 517.

[303] Reglamento (CE) núm. 864/2007 del Parlamento Europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»). *DOUE* L 199/40, de 31 de julio de 2007. *Vid.*, en relación con el *iter* del Reglamento «Roma II», Katia FACH GÓMEZ, «Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la ley aplicable a las Obligaciones Contractuales ('Roma II')», en Alfonso-Luis CALVO CARAVACA y Santiago AREAL LUDEÑA, *Cuestiones actuales del Derecho mercantil internacional*, Colex, Madrid, 2005, pp. 519-534; y Francisco J. GARCIMARTÍN ALFÉREZ, «La unificación del derecho conflictual en Europa: el reglamento sobre ley aplicable a las obligaciones

norma que determina la legislación aplicable sobre la base del lugar en el que se produzca el daño, independientemente del país o países en los que pudiera haber consecuencias indirectas.

1. Estructura y resultado actual

186. El Reglamento «Roma II» actual establece una regla general, la conexión con el Estado donde se produzca el daño directo *(lex loci damni)*, pero también reglas específicas y, en algunas disposiciones, una *cláusula de escape* que permite apartarse de estas reglas cuando se desprenda claramente de todas las circunstancias del caso que el hecho dañoso esta manifiestamente más vinculado con otro país.

Se trata de una norma de *carácter universal*, justificada en la preocupación por garantizar el correcto funcionamiento del mercado interior; en la incidencia sobre los intereses comunitarios que tiene la gran mayoría de situaciones en las que la UE se puede establecer como sede de análisis; en el carácter potencialmente intracomunitario de todas las relaciones internacionales; y, en la necesidad de facilitar la labor de los jueces nacionales estableciendo una solución única, que no tenga en cuenta el origen de las normas materiales a aplicar.[304] Gracias a este carácter universal resulta asegurada la determinación uniforme de la ley aplicable a las obligaciones extracontractuales con independencia de los tribunales nacionales ante los que se plantee el litigio. Esto significa un incremento en la previsibilidad jurídica de las partes —les permite conocer de antemano y con una certeza razona-

extracontractuales ('Roma II')», en *Diario La Ley*, Año XXVIII, núm. 6811, Miércoles, 31 de octubre de 2007.

304 *Vid.* Exposición de motivos, p. 10.

ble, la norma aplicable a su relación jurídica—[305] y, una mejora en el funcionamiento del mercado interior y del espacio de libertad, seguridad y justicia.[306]

187. Sin embargo, el tratamiento ilícito internacional de datos personales fue excluido expresamente del ámbito de aplicación del Reglamento «Roma II». Así, su artículo 1.2.g, establece que «Se excluirán del ámbito de aplicación del presente Reglamento: [...] *g)* las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación».[307] En consecuencia, la solución pasará, como hasta el momento, por el recurso al artículo 10.9 de nuestro CC, que toma como punto de conexión también el *locus delicti*, esto es, la aplicación de *la ley del lugar donde hubiere ocurrido el hecho de que deriven*.[308,309]

---

305 *Vid.* Exposición de motivos, p. 5.

306 Considerando 4.º: «El buen funcionamiento del mercado interior exige, con el fin de favorecer la previsibilidad en el resultado de los litigios, la seguridad jurídica y la libre circulación de resoluciones judiciales que las normas de conflicto de leyes vigentes en los Estados miembros designen la misma ley nacional con independencia del tribunal ante el que se haya planteado el litigio».

307 *Vid.* Diana SANCHO VILLA, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010, pp. 94-99.

308 A diferencia de otros sistemas de Derecho internacional privado que optan por el *locus actus* (p. ej., la Ley de Derecho internacional privado austríaca), por el *locus damni* (p. ej., la jurisprudencia francesa), por el *locus damni* salvo que el perjudicado pida la aplicación de la *lex loci actus* (p. ej., en el caso de la normativa italiana); o, por el *locus actus* salvo que el lesionado requiera la intervención de la *lex loci damni* (p. ej., en la normativa alemana). *Vid.*, en sentido amplio, y en relación con la contaminación transfronteriza, Katia FACH GÓMEZ, *La contaminación transfronteriza en Derecho Internacional Privado. Estudio de derecho aplicable*, Editorial Bosch, Barcelona, 2002, pp. 91-249.

Ante la imposibilidad de llegar a un acuerdo sobre cuál debería ser la solución conflictual más apropiada, los negociadores concluyeron que lo más prudente era excluir la materia en términos generales. No obstante, el artículo 30 del Reglamento «Roma II» prevé la posibilidad de que la Comisión europea presente nuevas propuestas en este ámbito.

2. Propuesta de futuro

188. La comentada STJUE *eDate Advertising*[310] ha motivado la formulación en el seno del Parlamento Europeo de una iniciativa tendente a revisar el Reglamento «Roma II», con el objeto de incluir una regla específica en materia de violación de la intimidad o de los derechos relacionados con la personalidad (derecho a la protección de datos de carácter personal). Esta iniciativa debe ser bienvenida en la medida en que supone un nuevo intento por colmar un vacío del Reglamento «Roma II» difícilmente justificable. Ciertamente, la unificación en la UE de las normas sobre ley aplicable en esa materia reviste especial importancia, habida cuenta del enorme incremento de las actividades con repercusión en una pluralidad de Estados como consecuencia de la difusión de información y datos a múltiples países a través de Internet, lo que dota de especial relevancia a los aspectos relativos a la determinación de la ley aplicable. No obstante, el contenido de la

---

309 *Vid.*, Pedro DE MIGUEL ASENSIO, *Derecho privado de Internet*, 4.ª ed., Civitas, Cizur Menor (Navarra), 2011, pp. 339-340, Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZALEZ, *Las obligaciones extracontractuales en Derecho internacional privado. El Reglamento «Roma II»*, Comares, Granada, 2008, pp. 217-218 y 222-226; y Diana SANCHO VILLA, *Negocios Internacionales..., op. cit.,* pp. 99-107.

310 STJUE (Gran Sala) de 25 de octubre de 2011.

propuesta recogida en la iniciativa parece generar ciertas dudas, en particular, en relación con su aplicación a las actividades desarrolladas a través de Internet.[311]

189. La iniciativa incluye una propuesta concreta de reforma legislativa: ***Working Document on the amendment of Regulation (EC) núm. 864/2007 on the law applicable to non-contractual obligations (Rome II)***.[312] El documento, que se centra en la actual falta de protección frente a la violación de la intimidad y de los derechos de la personalidad y la necesidad de cubrir este vacío, incluye un *artículo 5.*a *en el Reglamento «Roma II»*.[313]

---

311 *Vid.*, en general, Elisa Torralba Mendiola, «La difamación en la era de las comunicaciones: ¿Nuevas? perspectivas de Derecho Internacional Privado Europeo», en *Revista inDret*, núm. 1/2012, disponible en http://www.indret.com.

312 Documento de Trabajo del Comité de Asuntos Legales del Parlamento Europeo. DT\836983EN.doc, de 23/05/2011.

313 «[...] *Article 5a Rome II- Privacy and rights relating to personality*
»(1) *Without prejudice to Article 4(2) and (3), the law applicable to a non-contractual obligation arising out of violations of privacy and rights relating to personality, including defamation, shall be the law of the country in which the rights of the person seeking compensation for damage are, or are likely to be, directly and substantially affected.*
»*However, the law applicable shall be the law of the country in which the person claimed to be liable is habitually resident if he or she could not reasonably have foreseen substantial consequences of his or her act occurring in the country designated by the first sentence.*
»(2) *When the rights of the person seeking compensation for damage are, or are likely to be, affected in more than one country, and that person sues in the court of the domicile of the defendant, the claimant may instead choose to base his or her claim on the law of the court seised.*
»(3) *The law applicable to the right of reply or equivalent measures shall be the law of the country in which the broadcaster or publisher has its habitual residence.*

Son varios los elementos que llaman la atención en la propuesta. En primer lugar, puede destacarse la previsión de una cláusula de «escape» para los posibles responsables en estos litigios. Con ella se permite aplicar a sus potenciales responsabilidades el ordenamiento jurídico de su residencia habitual. Como segundo elemento novedoso, que en principio no plantearía problemas, debe destacarse la posibilidad de que sean las propias partes en conflicto las que elijan el ordenamiento que va a regir su relación jurídica extracontractual. Con esta previsión se cumplen con los requisitos de previsibilidad para ambas partes y se garantiza el equilibrio entre ellas en el procedimiento.

Una de las cuestiones que llama más la atención es que se opta por utilizar como punto de conexión un criterio que, desde el punto de vista práctico, ya se ha demostrado que causa más de un problema de concreción: el lugar de materialización del daño.

190. No obstante, esta Propuesta, a nuestro modo de ver, plantea varios problemas: el criterio de conexión (*«the country in which the rights of the person seeking compensation for damage are, or are likely to be, directly and substantially affected»*) puede en la práctica localizarse en más de un Estado al mismo tiempo: por ejemplo, si la persona es conocida en varios Estados en los que la información alcanza cierta difusión cabria apreciar que sus derechos resultan directa y sustancialmente afectados en más de un Estado. Lo deseable sería que la ley aplicable fuera tan sólo una, en particular, cuando el conjunto del daño en diversos países es objeto de la demanda interpuesta ante los tribunales de un Estado miembro competente con ese alcan-

»(4) *The law applicable under this Article may be derogated from by an agreement pursuant to Article 14.*[...]»

ce. Para lograr este objetivo parece resultar insuficiente la posibilidad que abre su apartado 2 según el cual: «2) *When the rights of the person seeking compensation for damage are, or are likely to be, affected in more than one country, and that person sues in the court of the domicile of the defendant, the claimant may instead choose to base his or her claim on the law of the court seised).»* Se prevé una única opción posible: la aplicación de la ley del foro a elección del demandante cuando la demanda se presente en el Estado del domicilio del demandado, sin perjuicio de la aplicación del artículo 4.2 y 3. Pero, ¿qué ocurrirá cuando la persona perjudicada ejercite su acción de tutela para su derecho a la protección de datos de carácter personal –que ha sido directa y sustancialmente afectado en varios Estados miembros– reclamando por la totalidad de los daños sufridos ante los tribunales del lugar del establecimiento del exportador de los datos –cuando no coincida éste con el domicilio del demandado–? Y se estará ante el mismo problema –por esa falta de previsión– cuando también por la totalidad de los daños causados, la persona perjudicada opte por litigar ante los órganos jurisdiccionales del Estado miembro en el que se encuentra su centro de intereses –que generalmente coincide con su residencia habitual–. Esta falta de previsión resulta, al menos, sorprendente, ya que puede considerarse que esta iniciativa Parlamentaria trae causa directa de la STJUE *eDate advertising*.

191. Meses después de esta iniciativa el Parlamento Europeo propuso una nueva regla de conflicto específica en materia de violación de los derechos de la personalidad para su eventual inclusión en una reforma del Reglamento «Roma II». Se trata del texto contenido en ***la Resolución del Parlamento Europeo de 10 de mayo de 2012 que incluye recomendaciones destinadas a la Comisión sobre la modificación del Reglamento «Roma II».*** Esta Resolución incorpora como Anexo los

textos de un nuevo considerando y un nuevo artículo que recomienda incluir en dicho Reglamento, textos que difieren sustancialmente de los recogidos en la iniciativa parlamentaria de noviembre de 2011.[314]

3. Interpretación creativa

192. Con la inclusión de la violación de la intimidad o de los derechos relacionados con la personalidad en el ámbito de aplicación material del Reglamento «Roma II», el futuro artículo 5 bis del citado Regla-

[314] El nuevo contenido propuesto es el siguiente:
«Artículo 5 bis: Privacidad y derechos relacionados con la personalidad
»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.
»3. Cuando la violación tenga su origen en una publicación impresa o en una emisión de radio o televisión, el país en el que se produzcan o sea más probable que se produzcan el elemento o elementos más significativos de los daños y perjuicios será considerado el país al que va principalmente dirigida la publicación o emisión, o, si esto no fuese evidente, el país en el que se efectúe el control editorial, siendo la legislación de ese país la ley aplicable. En particular, se determinará el país al que se dirija la publicación o emisión por el idioma de la publicación o emisión, o por las ventas o el tamaño de la audiencia de un determinado país como proporción del total de ventas o del tamaño de la audiencia, o por una combinación de esos factores.
»4. La ley aplicable al derecho de réplica o medidas equivalentes, y a toda medida cautelar o interdicto prohibitorio contra un editor u organismo de radiodifusión o teledifusión respecto al contenido de una publicación o emisión y respecto a las violaciones de la privacidad o de los derechos relacionados con la personalidad derivadas del tratamiento de datos personales será la del país en que el emisor o editor tenga su residencia habitual.»

mento debe ponerse en relación sistemática con la aplicación preferente del vigente artículo 14, que ofrece al perjudicado y al causante del daño la posibilidad de poder elegir la ley aplicable, en virtud del principio de la autonomía conflictual. Ahora bien, dicha elección, expresa o tácita, resulta poco probable que se dé en la práctica. Como sólo es posible con posterioridad al nacimiento del litigio, es difícil que causante del daño y perjudicado se pongan de acuerdo de cara a elegir una ley que corrija la situación de desprotección en la que se encuentra este último y le ofrezca una tutela adecuada, equilibrada y efectiva. Estos resultados eventualmente no deseados del artículo 14 del reglamento «Roma II» podrían ser corregidos en un sentido materializador, estableciendo que el pacto de elección de ley, aun siendo posterior al nacimiento del litigio, no sea tenido en cuenta si la protección que la ley elegida otorga a la víctima está por debajo de los estándares en materia de defensa del derecho a la protección de datos de carácter personal que le otorga el ordenamiento de su lugar de residencia.

En todo caso, hoy día la falta de una reglamentación normativa efectiva de la UE y convencional nos obliga, como ya se ha apuntado, a acudir a las soluciones normativas autónomas clásicas: en particular, al mencionado artículo 10.9 de nuestro CC (norma de conflicto relativa a la responsabilidad *ex delicto*, *modus operandi* que procede ante la carencia de soluciones normativa autónomas específicas).

III. EL ARTÍCULO 10.9 DEL CÓDIGO CIVIL: LEY DEL LUGAR DONDE SE PRODUCE EL PERJUICIO PARA EL TITULAR DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL MARCO DE UNA TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL ILÍCITA

193. Los tribunales españoles, una vez que se hayan declarado competentes para conocer de una pretensión reparatoria de la vulneración del derecho fundamental a la protección de datos derivada de una transferencia internacional de datos ilícita, ante la imposibilidad (por el momento) de acudir al Reglamento «Roma II» y la ausencia de norma convencional aplicable al respecto deberán recurrir a la aplicación de la norma de conflicto bilateral de Derecho internacional privado autónomo, norma prevista en materia de obligaciones no contractuales en el artículo 10.9 del CC.[315]

[315] *Vid.* Manuela ESLAVA RODRÍGUEZ, «El Locus Delicti Commssi en los ilícitos contra la vida privada cometidos a través de Internet», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, núm. 34, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 2002, pp. 25-35; y, con respecto a la justificación funcional de la *lex loci delicti commissi* ante intromisiones ilícitas internacionales en la vida privada, Manuela ESLAVA RODRÍGUEZ, *La protección civil del derecho a la vida privada en el tráfico privado internacional: derecho aplicable*, Universidad de Extremadura, Servicio de Publicaciones, Cáceres, 1996, pp. 117-135.

1. Estructura y resultado

194. La vulneración del derecho fundamental a la protección de datos queda, en principio, sujeta a la regla general contenida en el artículo 10.9 del CC nos permite articular dos posibilidades: ***1.ª)*** la aplicación de la ***lex loci actus*** **(Ley del Estado en el que se produce el hecho del que deriva la responsabilidad)** o ***2.ª)*** la aplicación de la ***lex loci damni*** **(aplicación de la ley del lugar donde se materializa el daño para las víctimas).**

a) **1.ª** POSIBILIDAD: ***lex loci actus (Ley del Estado en el que se produce el hecho del que deriva la responsabilidad).***[316] Para determinar «dicho Estado» (*locus delicti commissi*), habrá de tener presente que la vulneración del derecho a la protección de datos, como derecho de la personalidad que es, se produce mediante una *cadena de ilícitos*: cada *acto de agresión* contra el derecho a la protección de datos debe considerarse verificado en el Estado donde realmente tiene lugar, que es donde despliega su *resultado lesivo*, esto es, el tratamiento automatizado de datos personales se rige por la ley del Estado en cuyo territorio tiene lugar dicho tratamiento de datos que ha provocado el daño. Es en este Estado donde se produce el ilícito, el *locus delicti* (lugar del evento causal). Si el tratamiento de datos se desarrolla, como es frecuente, en distintas fases (recogida de datos, clasificación de los mismos, cesión a terceros de los datos, transferencia internacional, etc.), cada

316 *Vid.* Diana SANCHO VILLA, Negocios Internacionales..., op. cit., pp. 99-102.

una de esas *fases* se regirá por la ley del Estado en cuyo territorio haya tenido lugar.[317]

Un dato a tener en cuenta a efectos de utilización de este criterio es el de la ubicación de los ficheros de datos. Es frecuente que estos se encuentren alojados en un Estado distinto al del establecimiento del responsable. Otro elemento que debe ser considerado es el relativo a la actividad de un tercero en otro Estado que provoca el daño. En principio, la participación de este tercero como encargado no debería ser suficiente para identificar el origen del daño en el Estado de su establecimiento.

La finalidad de esta regla no es otra sino que «restaurar el equilibrio roto por el acto dañoso, imponiendo la obligación de reparar el daño causado. Así la obligación está ligada al hecho que la ha causado, el cual se localiza en el lugar donde se ha producido».[318] La persona que se encuentra en un lugar determinado cuenta con la protección ofrecida por el Derecho local. Así, p. ej., por aplicación del artículo 10.9 de nuestro Código Civil la ley aplicable sería la española cuando *a)* el responsable del fichero tuviera su domicilio fuera de la UE y, *b)* el tratamiento de datos se hubiera realizado en España. Si la transferencia internacional de datos de carácter personal se hace a un Estado con un nivel de protección adecuado, en aplicación del artículo 10.9 del CC el tratamiento de

---

317 *Vid.* Javier CARRASCOSA GONZÁLEZ, «Circulación internacional de datos personales informatizados y la Directiva 95/46/CE», en *Actualidad Civil*, núm. 23, 1997, p. 525.

318 Silvia FELIU ÁLVAREZ DE SOTOMAYOR, «Competencia judicial internacional y ley aplicable a los supuestos de responsabilidad extracontractual de los intermediarios básicos de Internet», en Santiago CAVANILLAS MÚGICA (Coord.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Comares, Granada, 2005, p. 226.

datos se debe regir por la Ley del país donde se lleve a cabo dicho tratamiento.[319] Por el contrario, si se realiza la transferencia internacional de datos a un Estado que no garantiza un nivel de protección adecuado, en virtud del artículo 4 de la Directiva 95/46/CE la ley aplicable será la del Estado donde radica el establecimiento del responsable de la transferencia de datos[320] (y, si el establecimiento del responsable de la transferencia de datos se encuentra en España, en virtud del artículo 2.1 de la LOPD, se aplicará la ley española). Finalmente, recordemos que si el tratamiento de datos se realiza en la UE, pero en el marco de actividades de un fichero de datos ubicado fuera de la UE, será de aplicación, sobre la base del mencionado artículo 4.1.c de la Directiva 95/46/CE, la ley del Estado miembro donde se ha realizado el tratamiento de datos.[321]

b) 2.ª POSIBILIDAD: ***lex loci damni (aplicación de la ley del lugar donde se materializa el daño para las víctimas).***[322] El recurso a la ley del Estado donde se ha producido el daño directo para la víctima es un criterio de conexión especial y adecuado para localizar la lesión del derecho a la protección de datos derivado de una transferencia internacional. Frecuentemente ese lugar donde se manifiesta la consecuencia directa para la víctima se corresponde con el lugar de su residencia habitual; sin embargo, esto no tiene por qué se así en todos los supuestos.

---

319 *Vid.*, en el mismo sentido, Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes...*, *op. cit.*, pp. 163-164.

320 *Vid.*, en el mismo sentido, Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes...*, *op. cit.*, pp. 164-165.

321 *Vid.*, en el mismo sentido, Alfonso-Luis CALVO CARAVACA y Javier CARRASCOSA GONZÁLEZ, *Conflictos de leyes...*, *op. cit.*, p. 166.

322 *Vid.* Diana SANCHO VILLA, Negocios Internacionales..., op. cit., pp. 102-107.

Por regla general, la residencia habitual de la víctima es el centro de las relaciones sociales, personales y económicas susceptibles de verse afectadas por un atentado contra la intimidad u otros derechos de la personalidad. Es una conexión previsible tanto para la persona perjudicada (confía en la protección que le ofrece el Estado de su residencia habitual) como para el responsable del daño, ya que suele conocer las circunstancias personales de la persona perjudicada, incluido el lugar de su residencia habitual. Permite además aplicar una ley única en aquellos supuestos frecuentes en la práctica en los que el daño se manifiesta en una pluralidad de Estados. La aplicación de esta ley permite que responsable de un daño transfronterizo sólo este obligado a respetar los límites a la libertad de expresión previstos en la ley de la residencia habitual del perjudicado. Así, por ejemplo, si se publica un dato incorrecto sobre la solvencia de un consumidor que reside en España y que solicita un préstamo en un tercer Estado, el *locus damni* no se localiza en España sino en ese tercer Estado.

Puede interpretarse que, en el contexto del artículo 10.9 del CC, la ley donde se produce el resultado dañoso directo para la víctima es la *ley de la residencia habitual del afectado*, salvo que las circunstancias del supuesto indiquen que otra ley es la que refleja el lugar donde se manifiesta el daño. Si el daño se manifestara en varios lugares, sería de aplicación cada una de las leyes implicadas respecto al alcance del daño padecido en ese lugar.

2. Interpretación creativa

195. La aplicación del artículo 10.9 del Código Civil nos conduce a resultados claramente insatisfactorios. Se trata de una norma de conflicto de corte clásico, es decir, con un supuesto de hecho muy genérico, un punto de conexión meramente localizador y una consecuencia

jurídica aparentemente neutra. Dichas características parecen evidentemente inadecuadas para regular un caso tan específico como es el tratamiento ilícito de datos personales, dada la situación de inferioridad jurídica del perjudicado.

La generalidad del supuesto de hecho del artículo 10.9 del Código Civil, que tiene sus consabidas ventajas —como el facilitar el proceso de calificación, etc.— es absolutamente irrelevante en el supuesto tipo, cuyo encaje en la categoría *responsabilidad civil extracontractual* no reviste especiales dificultades. Al contrario, la generalidad del precepto priva de visibilidad al problema de la desprotección del titular del derecho a la protección de datos ante un tratamiento ilícito internacional. La prueba de la pertinencia de la introducción de una norma específica para estos supuestos es la inminente reforma del Reglamento «Roma II», que especializa las soluciones generales tradicionales *(lex loci delicti commissi)*, introduciendo un futuro artículo 5 bis (violación de la intimidad o de los derechos relacionados con la personalidad).

En segundo lugar, el artículo 10.9 de nuestro Código Civil adolece de no pocas dosis de rigidez, puesto que sólo ofrece al juzgador una opción meramente localizadora entre la aplicación de la ley del lugar donde se ha producido el hecho causal (país de origen), o la ley del lugar donde se manifiesta la acción (país o países de resultado). Esta opción tan reducida no permite asegurar la tantas veces reclamada *actividad judicial creativa*, en aras a proporcionar al perjudicado una protección adecuada, equilibrada y efectiva de sus legítimos intereses.

En tercer lugar, la mayor crítica que se puede realizar al artículo 10.9 del Código Civil es su tradicional *ceguera material* o neutralidad. Cuando se parte de una situación en la que una de las partes está en manifiesta inferioridad, la neutralidad, lejos de ser una virtud, se convierte en una potencial fuente de injusticia.

IV. ÁMBITO DE APLICACIÓN DE LA LEY DESIGNADA PARA REGIR LA RESPONSABILIDAD CIVIL EXTRACONTRACTUAL DERIVADA DE UNA TRANSFERENCIA INTERNACIONAL ILÍCITA

196. La ley designada para regir la responsabilidad civil extracontractual derivada de una transferencia internacional de datos de carácter personal ilícita determinará las condiciones de dicha responsabilidad: imputabilidad, tipo de responsabilidad, daños indemnizables y acciones ejercitables. La ley rectora de la responsabilidad es la que debe resolver estas cuestiones.[323]

Una cuestión importante es la imputabilidad de la conducta del causante del daño en sentido amplio, cuestión que se vincula al reparto de responsabilidades y al alcance de la misma (si es solidaria o no), cuando intervengan varios sujetos.

La ley rectora de la responsabilidad se ocupará también del tipo de responsabilidad: objetiva o subjetiva, las causas de exoneración (fuerza mayor, caso fortuito) y de aquellas cuestiones relativas a la participación del afectado en la producción del daño.[324]

La ley rectora de la responsabilidad indicará también los daños indemnizables (patrimoniales y no patrimoniales) y su alcance. Habrá que determinar si la finalidad de la indemnización es meramente compensatoria o también punitiva (*punitive damages*).

---

[323] *Vid.*, en general, Manuela ESLAVA RODRÍGUEZ, *La protección civil..., op. cit.*

[324] Cuando la ley rectora de la responsabilidad sea la ley española, el artículo 19 de la LOPD (derecho a indemnización) deberá ser puesto en relación con el artículo 1902 de nuestro Código Civil (cláusula general de responsabilidad basada en la culpa).

Finalmente, la ley aplicable a la responsabilidad se ocupará de las acciones ejercitables (de resarcimiento y/o de cesación), de las personas físicas con derecho a indemnización. También se ocupará de la carga de la prueba en la medida en que disponga de reglas propias de responsabilidad civil extracontractual.[325]

V. BALANCE FINAL Y PROPUESTA DE *LEGE FERENDA*: CONFIGURACIÓN DE UNA NORMA DE CONFLICTO MATERIALMENTE ORIENTADA A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL MARCO DE UNA TRANSFERENCIA INTERNACIONAL DE DATOS DE CARÁCTER PERSONAL ILÍCITA

197. En los supuestos de tratamiento transfronterizo ilícito de datos de carácter personal, es preciso realizar una posible lectura materializadora del artículo 10.9 de nuestro Código Civil, en el sentido de que a la hora de determinar la *lex loci delicti commissi*, que puede ser la elección entre la ley del lugar donde se capturaron los datos personales o a la del Estado donde se trató dicha información personal, debe estar presidida por el *favor laesi*.

Aun así, esta interpretación del artículo 10.9 del Código Civil sigue siendo insatisfactoria. Al dejar en manos del órgano jurisdiccional la interpretación, caso por caso, de la *lex loci delicti commissi,* introduce

[325] Así, p. ej., el artículo 12.3 del RLOPD carga al responsable con la prueba del consentimiento del afectado para el tratamiento de sus datos de carácter personal.

notables dosis de inseguridad jurídica; sin garantías respecto de otorgar al perjudicado una protección adecuada, equilibrada y efectiva.

198. A mi modo de ver, esta nueva Propuesta sigue siendo fuente de inseguridad jurídica, debido a su escasa claridad, pues el criterio básico de conexión establecido en el apartado 1 se refiere a 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 perjuicio» y conforme a su apartado segundo la conexión recogida en dicho apartado 1 no opera cuando el demandado (responsable del daño) no pudiera «haber previsto razonablemente consecuencias importantes de su acto en el país designado en el apartado 1»: en estos casos la ley aplicable será la del país de residencia habitual del demandado (responsable del daño).

Con vistas a valorar (y limitar) el potencial impacto de un apartado 2 como el propuesto, que favorece la aplicación de la ley de la residencia habitual del presunto responsable, puede ser relevante traer a colación el apartado 50 de la mencionada sentencia del TJUE *eDate*, en el que el propio TJUE señaló: «La competencia del órgano jurisdiccional del lugar en el que la presunta víctima tiene su centro de intereses es conforme con el objetivo de la previsibilidad de las normas de competencia [...] también con respecto al demandado, dado que el emisor de un contenido lesivo puede, en el momento de la publicación en Internet de ese contenido, conocer los centros de intereses de las personas que son objeto de éste [...]». Si este planteamiento se traslada a la interpretación de una norma como la propuesta puede limitar en la práctica de manera significativa la operatividad del apartado 2 como correctivo del apartado 1.

Aunque en caso de que la iniciativa siguiera adelante en los términos actuales sería el TJUE el que tendría que establecer cómo debiera

interpretarse estas lagunas, podrían aventurarse las posibles soluciones interpretativas. Para los supuestos en los que se materializaran una pluralidad de daños en distintos Estados y la demanda no se hubiera presentado en el foro del domicilio del demandado, al no poder aplicarse la regla especial del apartado 2 del artículo 5 de la Propuesta, habría que acudir a la regla general contenida en su apartado 1 (aplicación de la *ley del lugar del daño*). Esto supondría que en caso de que se litigara por la totalidad de los daños el tribunal del foro debería aplicar tantos Derechos como Estados en los que se manifestó el daño. Esto es, de manera fraccionada, específicamente para resolver sobre los daños ocasionados en cada una de las jurisdicciones en presencia. Más sencillo sería, a nuestro juicio, el supuesto en el que la persona perjudicada optara por litigar en cualquiera de los lugares del daño (p. ej., en los lugares de emisión, de recepción, o de tratamiento de sus datos de carácter personal). En estos casos la solución general de ley aplicable prevista no presentaría ningún problema, es más, facilitaría con mucho la tramitación del procedimiento, pues se traduciría en que el tribunal del foro aplicaría su propia ley.

199. Si bien la persona perjudicada, como ya hemos visto, puede elegir entre los tribunales de distintos Estados para reclamar por los daños sufridos (domicilio del demandado *vs. forum delicti commissi)*, esta misma posibilidad de elección no se permite en el sector de la ley aplicable. Podría entenderse que la persona perjudicada sí puede elegir entre la *lex loci damni* o la *lex loci delicti commissi*, pero esta última sólo cuando coincida con el domicilio del demandado, y los daños se hayan materializado en diversos Estados al mismo tiempo. La redacción propuesta parece que motiva a la persona perjudicada a que se decida por demandar en el lugar del daño, para simplificar el procedimiento, lo que sería bastante adecuado si se trata de supuestos donde

el daño se manifiesta en un único Estado. Además, en principio, en este tipo de litigios suele coincidir el lugar del daño principal y directo con el de residencia habitual de la víctima, pues es allí donde se la conoce, donde tiene su reputación y desarrolla su vida y, en consecuencia donde pueden ser lesionados sus derechos.

200. Con todo ello, en aras a lograr esa tutela adecuada, equilibrada y efectiva al perjudicado debemos apostar por la configuración de una norma de conflicto materialmente orientada a lograr dicha tutela en el marco de una transferencia internacional ilícita de sus datos de carácter personal.

El artículo 5.1.bis es manifiestamente mejorable desde una perspectiva materializadora con un mínimo retoque de *lege ferenda*, que se justificaría en la propia situación jurídica de indefensión, inferioridad y de irreparabilidad del daño en la que se encuentra el perjudicado frente al causante del mismo. Para equilibrar dicha situación de desigualdad entre las partes sería deseable introducir una cláusula de escape materializadora, de forma que, *si del conjunto de circunstancias se desprende claramente que el caso presenta vínculos manifiestamente más estrechos con otro país distinto, se aplicará la ley de este otro país* y *se presumirá que los vínculos más estrechos se producen con la ley del país que otorgue una protección más adecuada, equilibrada y efectiva al perjudicado*.

Conclusiones

PRIMERA: El estudio de los mecanismos y reglas de protección vigentes en los distintos niveles de producción normativa –superestructura jurídica internacional, sistemas de integración regional, realizaciones del denominado *derecho transnacional* o Derecho internacional privado– arroja un balance claro: el marco normativo existente es a todas luces insuficiente para garantizar el derecho a la protección de datos, ya que se encuentra fragmentado en unidades nacionales de regulación, custodiadas por autoridades de protección independientes*. El titular del derecho a la protección de datos ante una transferencia internacional ilícita de sus datos se encuentra en una evidente situación de inferioridad jurídica, que le sitúa al borde de la desprotección frente al superior conocimiento técnico y poder económico de los infractores.*

SEGUNDA: *Las normas emanadas de las instancias internacionales* (ONU, OMC, OCDE) o bien no son directamente invocables por los particulares o bien carecen de una traducción adecuada al plano práctico. Por supuesto que sería deseable lograr un gran acuerdo internacional, cuyo objetivo principal fuese la protección del titular del dere-

cho a la protección de datos de carácter personal, sin que ello supusiese una carga excesiva al libre flujo de datos que afectase negativamente a las relaciones comerciales internacionales. La apuesta debería ser, al tiempo, ambiciosa y equilibrada. Ambiciosa, porque partimos de la inexistencia de experiencias concretas en este campo; lo que implicaría buscar el foro más adecuado para su discusión y adopción, así como el mecanismo jurídico con la proyección más universal posible. Equilibrada, porque hay que conjugar intereses legítimos de muy variada naturaleza y contrapuestos: por un lado, el derecho fundamental a la protección de datos de carácter personal y, por otro, las necesidades del comercio electrónico y los pactos internacionales de liberalización de los intercambios comerciales transfronterizos.

En cualquier caso, el contenido mínimo de ese instrumento legislativo universal y vinculante debería ser: *a)* establecer y llevar a la práctica los principios comunes existentes en materia de protección de datos y los límites a la libre circulación de información de carácter personal; *b)* reforzar la cooperación internacional entre las autoridades de protección de datos; y *c)* contemplar mecanismos de resolución de controversias adecuados y coercitivos. De momento, la agenda de las distintas organizaciones internacionales y la experiencia jurídica comparada no parecen contemplar nada parecido a tal emprendimiento.

TERCERA: ***Los intentos normativos de las organizaciones de integración regional*** (Consejo de Europa, APEC, UE) se enfrentan a una doble dificultad. Por una parte, la capacidad para llegar a soluciones *ad intra* —armonizando (Directiva) o uniformizando (Reglamento) legislaciones, o procurando la coordinación de autoridades (Convenios internacionales)— no puede prescindir, dada la naturaleza propiamente internacional del problema, del diálogo con otros sistemas jurídicos. Por otra, las soluciones tradicionales de Derecho internacional privado

no sólo no son del todo adecuadas para funcionar en una perspectiva *ad extra* —normas de competencia judicial internacional que discriminan entre demandados domiciliados dentro o fuera del sistema regional, particularismos, problemas de alegación y prueba del derecho extranjero, etc.— sino que tampoco resultan satisfactorias para proteger a la parte débil. Ello resulta manifiesto si se tiene en cuenta el establecimiento del domicilio del demandado como foro general (*verbi gratia*, foro del infractor) o la difícil precisión de los fueros especiales aplicables en la materia (*forum delicti commissi*), especialmente cuando el daño se produce a escala mundial. Todo ello conduce a que el titular afectado por un tratamiento transfronterizo ilícito de sus datos personales se sienta evidentemente desincentivado para reclamar en sede extracontractual.

CUARTA: Tampoco las posibles ***soluciones que provengan del denominado «derecho transnacional»*** ofrecen un balance esperanzador para el perjudicado. Sus realizaciones más notables consisten en códigos de conducta, recomendaciones, instrumentos de *soft law*, etc., que tienen como destinatarios a las empresas de la industria de tratamiento internacional de datos, o en sistemas alternativos de resolución de controversias, pensados desde y para la defensa de esas mismas empresas, prescindiendo del necesario contrapeso de intereses.

QUINTA: Para obtener esa compensación ante la violación de un derecho fundamental el ***Derecho internacional privado se presenta como el sistema normativo más sencilla y manifiestamente mejorable***; ya sea reinterpretando a favor del perjudicado las normas vigentes de competencia judicial internacional y derecho aplicable; ya sea reformando en sentido tuitivo dicha normativa. En el sector del reconocimiento y ejecución de decisiones no se presentan peculiaridades

dignas de estudio particular en este ámbito, por lo cual no han sido objeto de análisis.

SEXTA: Las vigentes normas de competencia judicial internacional, elaboradas en los distintos niveles normativos (institucional, convencional y autónomo), no sólo son claramente inadecuadas para proteger a la víctima de un tratamiento ilícito internacional de sus datos sino que pueden incluso conducir a resultados contraproducentes. En primer lugar, el recurso a la autonomía de la voluntad resulta peligroso ante una situación de desequilibrio entre las partes; tal y como se pone de manifiesto en la existencia de foros de protección (contratos individuales de trabajo, contratos de seguro y contratos celebrados por consumidores) en los diferentes sistemas de Derecho internacional privado comparado. La posibilidad de que se produzca un supuesto de sumisión tácita (regulada en el artículo 24 del RB/CL ll, 18 del CB, 5.1 del Tratado España-República de El Salvador o 22.2 de la LOPJ) es difícilmente verificable en la práctica: primero, porque el damnificado tendrá una tendencia lógica a demandar ante los tribunales del lugar de su residencia; segundo, porque parece evidente que el causante del daño, más que someterse a dichos tribunales, lo que haría sería impugnar su competencia, para no resultar enjuiciado por los tribunales de la contraparte.

En cualquier caso, si se produce la sumisión tácita es de suponer que el demandante (perjudicado) habrá realizado un cálculo previo de las posibilidades de éxito de su reclamación. Suposición que, dadas las características de los afectados y del conocimiento especializado que requiere el tratamiento de las situaciones privadas internacionales, dista mucho de coincidir con el estudio de campo realizado respecto de estas infracciones. La prorrogación expresa de fuero será, cuando menos, igual de difícilmente verificable que el supuesto de la sumisión

tácita y, además, ciertamente peligroso para el perjudicado, dada la situación de desigual *bargaining power* en el que se encuentran las partes enfrentadas.

SÉPTIMA: En defecto de elección de tribunales competentes, la opción entre fuero general y fueros especiales tampoco ofrece al damnificado una alternativa favorable a sus intereses. El fuero general del domicilio del demandado resulta evidentemente perjudicial para la víctima: *a)* porque, generalmente, tendrá que correr con el coste de internacionalización del proceso; y, *b)* porque la sitúa tan lejos de su ámbito de desarrollo social y personal como cerca del centro de intereses del causante del daño.

OCTAVA: El fuero especial en materia de responsabilidad civil extracontractual, *forum delicti commissi*, merece un análisis más detenido, como solución potencial y manifiestamente mejorable. Es la solución tradicional más extendida en el campo comparado y presente en nuestro derecho positivo (arts. 5.3 del RB/CL 11/CB, 4.3 del Tratado España-República de El Salvador o 22.3 de la LOPJ).

Su aplicación al supuesto tipo plantea no sólo los problemas habituales de precisión del *locus delicti commissi* ante supuestos de dispersión mundial del daño, sino también resultados particularmente nocivos en materia de tratamientos ilícitos internacionales de datos. La interpretación habitual del *locus delicti commissi* conduce bien a los tribunales del lugar donde se capturaron los datos personales, bien a la competencia de la jurisdicción del Estado donde se trató dicha información personal. En uno y otro caso, el estudio de campo revela que estamos lejos de darle una protección adecuada, equilibrada y efectiva al perjudicado, obligándole a litigar lejos de su centro de desarrollo social y personal.

La tutela que precisaría un supuesto de tratamiento ilícito internacional de datos, para reequilibrar las posiciones de las partes, requeriría ***interpretar el* forum delicti commissi *en un sentido favorable a la víctima.*** Esto es, identificándolo con el lugar de residencia habitual del perjudicado. Propuesta que es consciente de las habituales y compartibles críticas generales al denominado *forum actoris*, pero perfectamente defendible en este caso por su adecuación a las necesidades tuitivas del supuesto tipo y, además, acorde con la jurisprudencia más reciente del TJUE (Sentencia de 25 de octubre de 2011, *eDate Advertising* (C-509/09) y *Martínez y Martínez* (C-161/10)). Habrá, por tanto, que remitirse al *lugar de residencia habitual de la víctima*, aunque no como lugar del hecho dañoso, sino como *lugar de realización global de la acción generadora de dicha responsabilidad extracontractual*.

NOVENA: En el terreno del Derecho aplicable, en tanto en cuanto el artículo 1.2.g del vigente Reglamento «Roma II» establece que «Se excluirán del ámbito de aplicación del presente Reglamento: [...] *g)* las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación», la solución pasa por el recurso al artículo 10.9 de nuestro Código Civil, que toma como punto de conexión el *locus delicti commissi;* esto es, la aplicación de «la ley del lugar donde hubiere ocurrido el hecho de que deriven» *(lex loci delicti commissi)*.

La aplicación del artículo 10.9 del Código Civil nos conduce a resultados claramente insatisfactorios. Se trata de una norma de conflicto de corte clásico, es decir, con un supuesto de hecho muy genérico, un punto de conexión meramente localizador y una consecuencia jurídica aparentemente neutra. Dichas características parecen evidentemente inadecuadas para regular un caso tan específico como

es el tratamiento ilícito de datos personales, dada la situación de inferioridad jurídica del perjudicado.

DÉCIMA: La generalidad del supuesto de hecho del artículo 10.9 del Código Civil, que tiene sus consabidas ventajas —como el facilitar el proceso de calificación, etc.— es absolutamente irrelevante en el supuesto tipo, cuyo encaje en la categoría *responsabilidad civil extracontractual* no reviste especiales dificultades. Al contrario, la generalidad del precepto priva de visibilidad al problema de la desprotección del titular del derecho a la protección de datos ante un tratamiento ilícito internacional. La prueba de la pertinencia de la introducción de una norma específica para estos supuestos es la inminente reforma del Reglamento «Roma II», que especializa las soluciones generales tradicionales *(lex loci delicti commissi)*, introduciendo un futuro artículo 5 bis (violación de la intimidad o de los derechos relacionados con la personalidad).

En segundo lugar, el artículo 10.9 de nuestro Código Civil adolece de no pocas dosis de rigidez, puesto que sólo ofrece al juzgador una opción meramente localizadora entre la aplicación de la ley del lugar donde se ha producido el hecho causal (país de origen), o la ley del lugar donde se manifiesta la acción (país o países de resultado). Esta opción tan reducida no permite asegurar la tantas veces reclamada *actividad judicial creativa*, en aras a proporcionar al perjudicado una protección adecuada, equilibrada y efectiva de sus legítimos intereses.

En tercer lugar, la mayor crítica que se puede realizar al artículo 10.9 del Código Civil es su tradicional *ceguera material* o neutralidad. Cuando se parte de una situación en la que una de las partes está en manifiesta inferioridad, la neutralidad, lejos de ser una virtud, se convierte en una potencial fuente de injusticia.

Por tanto, en los supuestos de tratamiento transfronterizo ilícito de datos de carácter personal, es preciso realizar una posible lectura

materializadora del artículo 10.9 de nuestro Código Civil, en el sentido de que a la hora de determinar la *lex loci delicti commissi*, que puede ser la elección entre la ley del lugar donde se capturaron los datos personales o a la del Estado donde se trató dicha información personal, debe estar presidida por el *favor laesi*.

Aun así, esta interpretación del artículo 10.9 del Código Civil sigue siendo insatisfactoria. Al dejar en manos del órgano jurisdiccional la interpretación de la *lex loci delicti commissi,* introduce notables dosis de inseguridad jurídica; sin garantías respecto de otorgar al perjudicado esa protección adecuada, equilibrada y efectiva que se viene demandando en el presente proyecto de investigación.

DECIMOPRIMERA: Hay que tener en cuenta, *de lege data* inminente, que el Parlamento Europeo ha propuesto una nueva norma de conflicto específica en materia de violación de la intimidad o de los derechos relacionados con la personalidad (derecho a la protección de datos de carácter personal), para su eventual inclusión en la ***proyectada reforma del Reglamento «Roma II».*** **El futuro artículo 5 bis del Reglamento «Roma II»** establece como ley aplicable *1)* «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»; o, en su defecto, si el demandado no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país, *2)* «la ley del país de residencia habitual del demandado».

Con la inclusión de la violación de la intimidad o de los derechos relacionados con la personalidad en el ámbito de aplicación material del Reglamento «Roma II», el futuro artículo 5 bis del citado Reglamento debe ponerse en relación sistemática con la aplicación preferente del vigente artículo 14, que ofrece al perjudicado y al causante del daño la posibilidad de poder elegir la ley aplicable, en virtud del

principio de la autonomía conflictual. Ahora bien, dicha elección, expresa o tácita, resulta poco probable que se dé en la práctica. Como sólo es posible con posterioridad al nacimiento del litigio, es difícil que causante del daño y perjudicado se pongan de acuerdo de cara a elegir una ley que corrija la situación de desprotección en la que se encuentra este último y le ofrezca una tutela adecuada, equilibrada y efectiva. Estos resultados eventualmente no deseados del artículo 14 del reglamento «Roma II» podrían ser corregidos en un sentido materializador, estableciendo que el pacto de elección de ley, aun siendo posterior al nacimiento del litigio, no sea tenido en cuenta si la protección que la ley elegida otorga a la víctima está por debajo de los estándares en materia de defensa del derecho a la protección de datos de carácter personal que le otorga el ordenamiento de su lugar de residencia.

DECIMOSEGUNDA: Si, como es más que probable, el art. 14 del Reglamento «Roma II» no resulta de aplicación, entrará en juego la propuesta del futuro artículo 5 bis. Precepto que, en principio, debe ser saludado favorablemente —pues especializa y colma un vacío del Reglamento «Roma II» difícilmente justificable— pero sigue ofreciendo una solución conflictual no satisfactoria desde el punto de vista de la protección que precisa el titular del derecho fundamental a la protección de datos ante una transferencia internacional ilícita de los mismos. ***El artículo 5 bis no sólo no protege al perjudicado sino que, paradójicamente, puede favorecer al causante del daño.***

Del párrafo primero del nuevo artículo 5 bis cabría entender que la persona lesionada por una transferencia internacional ilícita de sus datos personales podría fundamentar su demanda en 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 en la *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 perjuicio). Esta posible alternativa sigue siendo una opción meramente localizadora, cuyas mejores virtudes son especializar y flexibilizar la solución tradicional; pero no persigue un resultado material tuitivo, en la medida en que puede conducir a resultados que no otorguen una protección adecuada, equilibrada y efectiva al perjudicado.

Más discutible aún es la solución que ofrece el párrafo segundo del propio artículo 5 bis del citado Reglamento «Roma II» para los tratamientos transfronterizos ilícitos de datos de carácter personal, ya que establece la aplicación de la ley de la residencia habitual del presunto responsable del daño, si se dan las siguientes condiciones: *a)* que resulte imposible determinar el elemento o los elementos más significativos del daño o perjuicio (condición normativa objetiva); y *b)* que el causante del daño no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país (condición normativa subjetiva).

En principio, dado el juego combinado del foro general del domicilio del demandado (foro del causante) y el párrafo segundo del artículo 5 bis (ley del causante del daño) el demandante (perjudicado) queda en una situación muy delicada, muy apartado de su centro de desenvolvimiento social y personal de sus intereses.

El artículo 5 bis es manifiestamente mejorable desde una perspectiva materializadora con un mínimo retoque de **lege ferenda*****, que se justificaría en la propia situación jurídica de indefensión, inferioridad y de irreparabilidad del daño en la que se encuentra el perjudicado frente al causante del mismo.*** Para equilibrar dicha situación de desigualdad entre las partes sería deseable introducir una cláusula de escape materializadora, de forma que, *si del conjunto de circunstancias se desprende claramente que el caso presenta vínculos*

manifiestamente más estrechos con otro país distinto, se aplicará la ley de este otro país y *se presumirá que los vínculos más estrechos se producen con la ley del país que otorgue una protección más adecuada, equilibrada y efectiva al perjudicado.*

Referencias

1. Bibliografía consultada

A. Derecho internacional privado

1. Obras generales.

Calvo Caravaca, Alfonso-Luis y Javier Carrascosa González, *Derecho internacional privado. Vol. I.,* 14.ª ed., Comares, Granada, 2013

— *Derecho internacional privado. Vol. II*, 14.ª ed., Comares, Granada, 2013

Díaz-Ambrona Barjadí, M.ª Dolores (Dir.), *Derecho Civil de la Unión Europea*, 4.ª ed., Colex, Madrid, 2010

Esplugues Mota, C. y J. L. Iglesias Buhigues, *Derecho internacional privado*, 7.ª ed., Tirant lo blanch, Valencia, 2013

Fernández Rozas, José Carlos y Sixto Sánchez Lorenzo, *Derecho Internacional Privado*, Civitas, 7.ª ed., Madrid, 2013

Garcimartín Alférez, Francisco J., *Derecho internacional privado*, Civitas, Madrid, 2012

Virgos Soriano, Miguel y Francisco J. GARCIMARTÍN ALFÉREZ, *Derecho procesal civil internacional. Litigación internacional*, Civitas, Madrid, 2000

2. MONOGRAFÍAS

ALONSO-CUEVILLAS SAYROL, Jaume, *La competencia jurisdiccional internacional de los Tribunales españoles del orden civil*, Tirant lo Blanch, Valencia, 2006

ARENAS GARCÍA, Rafael, *El control de oficio de la competencia judicial internacional*, EUROLEX, Madrid, 1996

CALVO CARAVACA, Alfonso-Luis y Javier CARRASCOSA GONZALEZ, *Las obligaciones extracontractuales en Derecho internacional privado. El Reglamento «Roma II»*, Comares, Granada, 2008

– *Conflictos de leyes y conflictos de jurisdicción en Internet*, Colex, Madrid, 2001

CALVO CARAVACA, Alfonso-Luis, *Comentario al convenio de Bruselas relativo a la Competencia Judicial y a la Ejecución de resoluciones judiciales en materia civil y mercantil*, Universidad Carlos III de Madrid. Boletín Oficial del Estado, Madrid, 1994

CARRASCOSA GONZÁLEZ, Javier, *Desarrollo judicial y Derecho Internacional Privado,* Comares, Granada, 2004

DE MIGUEL ASENSIO, Pedro, *Derecho privado de Internet*, 4.ª ed., Civitas, Cizur Menor (Navarra), 2011

FELIU ÁLVAREZ DE SOTOMAYOR, Silvia, *La contratación internacional por vía electrónica con participación de consumidores: la elección entre la vía judicial y la vía extrajudicial para la resolución de conflictos*, Comares, Granada, 2006

GARAU SOBRINO, Federico F., *Los acuerdos internacionales de elección de foro*, Colex, Madrid, 2008

PALAO MORENO, Guillermo, *Aspectos internacionales de la responsabilidad civil por servicios*, Comares, Granada, 1995

3. Estudios en obras colectivas

Fach Gómez, Katia, «Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la ley aplicable a las Obligaciones Contractuales ('Roma II')», en Alfonso-Luis Calvo Caravaca y Santiago Areal Ludeña, Santiago, *Cuestiones actuales del Derecho mercantil internacional*, Colex, Madrid, 2005, pp. 519-534

Feliu Álvarez De Sotomayor, Silvia, «Competencia judicial internacional y ley aplicable a los supuestos de responsabilidad extracontractual de los intermediarios básicos de Internet», en Santiago Cavanillas Múgica (Coord.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Comares, Granada, 2005, pp. 203-226

Palao Moreno, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», en Javier Plaza Penadés, *Cuestiones actuales de derecho y Tecnologías de la Información y Comunicación (TICs)*, Editorial Aranzadi, Cizur Menor (Navarra), 2006, pp. 275-297

Xalabarder Plantada, Raquel, «Cuestiones de derecho internacional privado: jurisdicción competente y ley aplicable», en *Derecho y nuevas tecnologías*, Editorial UOC, Barcelona, 2005, pp. 471-590

4. Artículos

Bing, J., *Data protection, jurisdiction and the choice of law*, en *Privacy Law & Policy. Reporter*, volume 6, 199, pp. 92-98

De Miguel Asensio, Pedro A., «El nuevo Reglamento sobre competencia judicial y reconocimiento y ejecución de resoluciones», en *Diario La Ley*, núm. 8013, Sección Tribuna, 31 de enero de 2013, Año XXXIII, editorial La Ley, pp. 1-15

DE MIGUEL ASENSIO, Pedro A., «Competencia judicial y protección de los derechos de la personalidad en Internet», en *Diario La Ley*, núm. 7787, Sección Tribuna, 31 de enero de 2012, Año XXXIII, editorial La Ley, pp. 1-7

DESANTES REAL, Manuel, y José Luis IGLESIAS BUHIGUES, «Hacia un Sistema de derecho Internacional privado de la Unión Europea», en *Anuario de Derecho internacional Privado (2009)*, Tomo IX, Iprolex, Madrid, 2010, pp. 115-128

ESLAVA RODRÍGUEZ, Manuela, «El *Locus Delicti Commssi* en los ilícitos contra la vida privada cometidos a través de Internet», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, núm. 34, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 2002, pp. 14-38

GARCIMARTÍN ALFÉREZ, Francisco J., «La unificación del derecho conflictual en Europa: el reglamento sobre ley aplicable a las obligaciones extracontractuales ('Roma II')», en *Diario La Ley*, Año XXVIII, núm. 6811, Miércoles, 31 de octubre de 2007

GOÑI URRIZA, Natividad, «La concreción del lugar donde se ha producido el hecho dañoso en el art. 5.3 del Reglamento 44/2001: nota a la STJCE de 16 de julio de 2009», en *Cuadernos de Derecho Transnacional* (Marzo 2011), Vol. 3, núm. 1, pp. 290-295

LORENTE MARTÍNEZ, Isabel, «Lugar del hecho dañoso y obligaciones extracontractuales. La Sentencia del TJUE de 25 octubre 2011 y el coste de la litigación internacional en Internet», en *Cuadernos de Derecho Transnacional* (Marzo 2012), Vol. 4, núm. 1, pp. 277-301

SUQUET CAPDEVILA, Josep, «Internet, marcas y competencia judicial internacional: ¿O la superación de la regla *forum loci delicti commissi*? A propósito de la sentencia de la Cour de Cassation de 9 de diciembre de 2003», en *La Ley Unión Europea*, núm. 6073, Madrid, 2004, pp. 1- 7

B. Protección de datos de carácter personal

1. Obras generales y Monografías

Agencia de protección de datos de la Comunidad de Madrid, *Repertorio de Legislación y Jurisprudencia sobre Protección de Datos*, Thomson-Civitas, Madrid, 2004

Almuzara Almaida, Cristina (Coord.) y otros, *Estudio práctico sobre la protección de datos de carácter personal*, 2.ª ed., Lex Nova, Valladolid, 2007

Álvarez-Cienfuegos Suárez, José María, *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Elcano (Navarra), 1999

Álvarez Civantos, Oscar José, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, 3.ª ed., Comares, Granada, 2008

Álvarez Rubio, Juan José (Dir.), *Difamación y protección de los derechos de la personalidad: ley aplicable en Europa*, Aranzadi Thomson Reuters, Cizur Menor (Navarra), 2009

Amadeo Gadea, Santiago Luis, *Informática y Nuevas Tecnologías*, La Ley-Actualidad, Madrid, 2001

Aparicio Salom, Javier, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Elcano (Navarra), 2002

— *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, 2.ª ed., Aranzadi, Elcano (Navarra), 2002

Arenas Ramiro, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006

Ballesteros Moffa, Luis Ángel, *La privacidad electrónica. Internet en el centro de protección*, Tirant lo Blanch, Valencia, 2005

BARCELÓ, Rosa, *Protección de datos en Internet: régimen general*, UOC, Barcelona, 2005

BARRAL VIÑALS, Inmaculada (Coord.), *La regul@ción del comercio electrónico*, Dykinson, Madrid, 2003

BERTRAND, André y Thierry PIETTE-COUDOL, *Internet et le droit*, Presses Universitaires de France, Paris, 1999

BYGRAME, Lee A., *Data protection law: approaching its rationale logic and limits*, Kluwer Law International, USA, 2002

CAMPUZANO, Herminia, *Vida privada y datos personales,* Tecnos, Madrid, 2000

CASTAÑEDA GONZÁLEZ, Alberto (Coord.), *Derecho tecnológico. Respuestas legales a nuevos retos*, Ediciones Experiencia, Barcelona, 2004

CASTAÑEDA GONZÁLEZ, Alberto, Rodrigo BONADEO FIOONI y Jesús SÁNCHEZ ECHEVARRÍA, *Guía práctica de Protección de Datos de Carácter Personal*, Ediciones Experiencia, Barcelona, 2002

CONDE ORTIZ, Concepción, *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson, Madrid, 2005

DAVARA FERNÁNDEZ DE MARCOS, Isabel, *Hacia la estandarización de la protección de datos personales*, La Ley, Madrid, 2011

DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de Derecho Informático*, 2.ª ed., Aranzadi, Elcano (Navarra), 1997

– *La protección de datos en Europa: principios, derechos y procedimiento*, Universidad Pontificia de Comillas, Madrid, 1998

– *Nueva guía práctica de protección de datos desde la óptica del titular del fichero*, Dykinson, Madrid, 2001

– *Guía práctica de protección de datos para las pymes. Lo que debe saber el gestor de una PYME sobre Protección de Datos*, CIRSA, Madrid, 2002

DAVARA RODRÍGUEZ, Miguel Ángel, (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2002*, Fundación VODAFONE, Madrid, 2002

– *Guía práctica de comercio electrónico para las pymes. ¿Qué debe saber un gestor de una PYME sobre comercio electrónico?*, CIRSA, Madrid, 2003

– (Coord.), *XVII Encuentros sobre Informática y Derecho 2002-2003*, Universidad Pontificia de Comillas, Madrid, 2003

– *La transposición de la Directiva sobre la privacidad y las comunicaciones electrónicas,* DAVARA & DAVARA, Madrid, 2004

– *Guía práctica de protección de datos para abogados*, DaFeMa, Madrid, 2004

– (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2002*, Fundación VODAFONE, Madrid, 2002

– (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2003*, Fundación VODAFONE, Madrid, 2003

– (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2004*, Fundación VODAFONE, Madrid, 2004

– (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2005*, Fundación VODAFONE, Madrid, 2005

– (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC) 2006*, Fundación VODAFONE, Madrid, 2006

– *Manual de Protección de Datos para Abogados*, Aranzadi, Elcano (Navarra), 2006

DECKER, Micheline, *Aspects internes et internacionaux de la protection de la vie privée en droits français, allemand et anglais*, Presses Universitaries d´Aix, Marseille, 2001

DEL PESO NAVARRO, Emilio, *Ley de Protección de Datos. La nueva LORTAD*, Ediciones Díaz de Santos, Madrid, 2000

– *Servicios de la Sociedad de la Información (Comercio electrónico y protección de datos)*, Díaz de Santos, Madrid, 2003

– y Miguel Ángel RAMOS GONZÁLEZ, *LORTAD. Análisis de la Ley*, 2.ª ed., Díaz de Santos, Madrid, 1998

– – *LORTAD. Reglamento de seguridad*, Díaz de Santos, Madrid, 1999

– – *La seguridad de los datos de carácter personal*, 2.ª ed., Díaz de Santos, Madrid, 2002

DEL VALLE FERNÁNDEZ, Julián, *Auditoría informática. Glosario de términos*, Fundación DINTEL, Madrid, 2002

DRAETTA, Ugo, *Internet e commercio elettronico: nel diritto internazionale dei privati*, Giuffrè, Milán, 2001

DRUMMOND, Víctor (Traducción de Isabel Espín Alba), *Internet, Privacidad y Datos Personales*, Reus, Madrid, 2004

FENOLL-TROUSSEAU, Marie-Pierre et Gérard HAAS, *Internet et protection des données personalles*, Litec, París, 2000

FERNÁNDEZ ESTEBAN, María Luisa, *Nuevas tecnologías, internet y derechos fundamentales*, McGraw-Hill, Madrid, 1998

FERNÁNDEZ RODRÍGUEZ, José Julio, *Secreto e intervención en las comunicaciones en Internet*, Civitas, Madrid, 2004

FERNÁNDEZ SALMERÓN, Manuel, *La protección de los datos personales en la Administraciones Públicas*, Civitas, Madrid, 2003

FREIXAS GUTIÉRREZ, Gabriel, *La protección de los datos de carácter personal en el Derecho español. Aspectos teóricos y prácticos*, Bosch, Barcelona, 2001

GALINDO, Fernando, *Derecho e informática*, La Ley-Actualidad, Madrid, 1998

GARCÍA-BERRIO HERNÁNDEZ, María Teresa, *Informática y libertades: la protección de datos personales y su regulación en Francia y España*, Servicio de Publicaciones de la Universidad de Murcia, Murcia, 2003

GARCÍA MEXÍA, Pablo (Dir.), *Principios de Derecho de Internet*, 2.ª ed., Tirant lo Blanch, Valencia, 2005

GARRIGA DOMÍNGUEZ, Ana, *La protección de los datos personales en el Derecho español*, Dykinson, Madrid, 1999

– *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004

GÓMEZ GAMBOA, David, *El tratamiento automatizado de datos frente a los derechos fundamentales al honor, intimidad y protección de datos de carácter personal*, 2.ª ed., Dykinson, Madrid, 2003

GÓMEZ MARTÍNEZ, Carlos (Dir.), *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2004

GONZÁLEZ GAITANO, Norberto, *El deber de respeto a la intimidad*, EUNSA, Pamplona, 1990

GÓMEZ SEGADE, José Antonio (Dir.) y otros, *Comercio electrónico en Internet*, Marcial Pons, Madrid, 2001

GONZÁLEZ SORIA, Julio (Coord.) y otros, *Comentarios a la Nueva Ley de Arbitraje 60/2003, de 23 de diciembre*, Thomson-Aranzadi, Cizur Menor (Navarra), 2004

GRIMALT SERVERA, Pedro, *La responsabilidad civil en el tratamiento automatizado de datos de personales*, Comares, Granada, 1999

GRIMALT SERVERA, Pedro, *La protección civil de los derechos al honor, a la intimidad y a la propia imagen*, Iustel, Madrid, 2007

GUERRERO PICÓ, M.ª Carmen, *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006

HEREDERO HIGUERAS, Manuel, *La directiva comunitaria de protección de los datos de carácter personal: Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos*, Aranzadi, Pamplona, 1997

HERRÁN ORTIZ, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999.

— *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dykinson, Madrid, 2002

— *El derecho a la protección de datos personales en la sociedad de la información*, Cuadernos Deusto de derechos Humanos, Universidad de Deusto, Bilbao, 2003

KUNER, Christopher, *European Data Privacy Law and online business*, Oxford University Press, New York, 2003

LESMES SERRNO, Carlos (Coord.) y otros, *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*, Lex Nova, Valladolid, 2007

LÓPEZ-VIDRIERO TEJEDOR, Iciar y Efrén SANTOS PASCUAL, *Protección de datos personales. Manual práctico para empresas*, Fundación CONFEMETAL, Madrid, 2005

MARTINEZ MARTINEZ, Ricard, *Una aproximación crítica a la autodeterminación informativa*, Civitas, Madrid, 2004

MARTINEZ MARTINEZ, Ricard y Santiago BERMELL GIRONA, Santiago, *El Graduado Social y la Ley de Protección de datos*, Thomson Aranzadi, Cizur Menor (Navarra), 2006

MARZO PORTERA, Ana, Fernando RAMOS SUÁREZ y otros, *La protección de datos en la gestión de empresas*, Aranzadi, Cizur Menor (Navarra), 2004

MARZO PORTERA, Ana y Alejandro MACHO-QUEVEDO PÉREZ-VICTORIA, Alejandro, *La Auditoría de Seguridad en la Protección de Datos de Carácter Personal*, Ediciones Experiencia, Barcelona, 2004

MESSÍA DE LA CERDA BALLESTEROS, Jesús Alberto, *La cesión o comunicación de datos de carácter personal*, Civitas, Madrid, 2003

– *La protección de datos de carácter personal en las telecomunicaciones,* Universidad Rey Juan Carlos, Madrid, 2004

MOLES, Ramón J., *Derecho y control en Internet. La regulabilidad de Internet*, Ariel, Barcelona, 2004

MURILLO DE LA CUEVA, Pablo Lucas, *Informática y protección de datos personales. (Estudio sobre la ley orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993

ORTÍ VALLEJO, Antonio, *Derecho a la intimidad e informática: tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada*, Comares, Granada, 1994.

PALLARO, Paolo, *Libertà della persona e trattamento dei dati personali nell´unione europea*, Giuffrè Editore, Milano, 2002

PIATTINI VELTHUIS, Mario Gerardo y Fernando HERVADA VIDAL (Coords.) y otros, *Gobierno de las Tecnologías y los Sistemas de Información*, RA-MA Editorial, Paracuellos de Jarama (Madrid), 2007

PIÑAR MAÑAS, José Luis y Álvaro CANALES GIL, *Legislación de protección de datos*, Iustel, Madrid, 2008

RIBAS ALEJANDRO, Javier, *Aspectos Jurídicos del Comercio Electrónico en Internet*, 2.ª ed., Thomson-Aranzadi, Cizur Menor (Navarra), 2003

REBOLLO DELGADO, Lucrecio, *Derechos fundamentales y protección de datos*, Dykinson, Madrid, 2004

– *El derecho fundamental a la intimidad*, 2.ª ed., Dykinson, Madrid, 2005

– *Vida privada y protección de datos en la Unión Europea*, Dykinson, Madrid, 2008

– y M.ª Mercedes SERRANO PÉREZ, *Introducción a la protección de datos*, Dykinson, Madrid, 2006

RIPOLL CARULLA, Santiago (Ed.), Jordi BACARIA MARTRUS (Coord.) y otros, *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Agencia Catalana de Protección de Datos, Marcial Pons, Madrid, 2006

RUBIO NAVARRO, Antonio María, *Aspectos prácticos de la protección de datos de las personas físicas*, Bosch, Barcelona, 2004

RUIZ CARRILLO, Antonio, *Los datos de carácter personal: concepto, requisitos de circulación, procedimientos, normativa y formularios*, Bosch, Barcelona, 1999

– *Manual práctico de protección de datos*, Bosch, Barcelona, 2005

– *La protección de los datos de carácter personal*, Bosch, Barcelona, 2001

SÁNCHEZ ALMEIDA, Carlos y Javier A. MAESTRE RODRÍGUEZ, *La Ley de Internet. Régimen jurídico de los Servicios de la Sociedad de la Información y Comercio Electrónico*, SERVIDOC, Barcelona, 2002

SANTANIELLO, Giuseppe, *La Protezione dei dati personali*, CEDAM, Padova, 2005

SANTOS GARCÍA, Daniel, *Nociones generales de la ley orgánica de protección de datos*, Tecnos, Madrid, 2006

SERRANO PÉREZ, María Mercedes, *El derecho fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, 2003

SERRERA COBOS, Pedro, *Buenas prácticas en protección de datos*, Fundación DINTEL, Madrid, 2007

TÉLLEZ AGUILERA, Abel, *Nuevas tecnologías, intimidad y protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Dykinson, Madrid, 2001

— *La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002

VELÁZQUEZ BAUTISTA, Rafael, *Protección jurídica de datos personales automatizados*, Colex, Madrid, 1993

— *Derecho de tecnologías de la información y las comunicaciones (T.I.C.)*, 1.ª ed., Colex, Madrid, 2001

— *100 interrogantes fundamentales en Derecho de Tecnologías de la Información y las Comunicaciones (T.I.C.)*, Colex, Madrid, 2004

VIZCAÍNO CALDERÓN, Miguel, *Problemática jurídica en torno al fenómeno de Internet*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2000

— *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001

— *XIV Encuentros sobre Informática y Derecho: 2000-2001, Facultad de Derecho, Instituto de Informática Jurídica de la Universidad Pontificia Comillas de Madrid*, Aranzadi, Elcano (Navarra), 2001

— *Comercio electrónico y protección de los consumidores*, La Ley-Actualidad, Madrid, 2001

— *Protección de datos personales: el manual práctico para cumplir la LOPD y el Reglamento de Medidas de Seguridad: factbook*, Aranzadi, Elcano (Navarra), 2003

— *Factbook Comercio Electrónico*, 3.ª ed., Aranzadi, Elcano (Navarra), 2004

VIZCAÍNO CALDERÓN, Miguel, *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2005

– *Derecho y nuevas tecnologías*, Editorial UOC, Barcelona, 2005

– *Proceedings of the First European Congress on Data Protection, Madrid, 29-31 March 2006*, Fundación BBVA, Bilbao, 2008

– *Internet, Derecho y Política*, Editorial UOC, Barcelona, 2009

ZABÍA DE LA MATA, Juan (Coord.), *Protección de datos. Comentarios al Reglamento*, 1.ª ed., Lex Nova, Valladolid, 2008

2. Estudios en obras colectivas

AMUTIO GÓMEZ, Miguel, «Panorámica general sobre normas de seguridad de tecnologías de la información», en Mario Gerardo PIATTINI VELTHUIS y Fernando HERVADA VIDAL (Coords.) y otros, *Gobierno de las Tecnologías y los Sistemas de Información*, RA-MA Editorial, Paracuellos de Jarama (Madrid), 2007, pp. 215-243

ARENAS RAMIRO, Mónica, «El derecho a la protección de datos personales en la jurisprudencia del TJCE», en Javier PLAZA PENADÉS, (Coord.), *Cuestiones actuales de Derecho y Tecnologías de la información y la Comunicación (TICs)*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 95-119

Jordi BACARIA MARTRUS, «La Agencia Catalana de Protección de Datos (algunos aspectos comparativos con la Agencia de Protección de Datos de la Comunidad de Madrid). La cuestión de las competencias autonómicas sobre ficheros de titularidad privada en la ley catalana», en Miguel Ángel DAVARA RODRÍGUEZ (Coord.), *XVII Encuentros sobre Informática y Derecho 2002-2003*, Universidad Pontificia de Comillas, Madrid, 2003, pp. 47-56

BAYO DELGADO, Joaquín, «Derecho comunitario sobre protección de datos», en Carlos GÓMEZ MARTÍNEZ, (Dir.), *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2004, pp. 45-76

BENEDITO AGRAMUNT, José, «Anteproyecto de Ley de creación de la Agencia Valenciana de Protección de Datos», en Antonio TRONCOSO REIGADA (Dir.), *Estudios sobre Administraciones públicas y protección de datos personales. 1 Encuentro entre Agencias Autonómicas de Protección de Datos Personales: celebrado el día 2 de noviembre de 2004 en la Sede de la Universidad Carlos III de Madrid; organizado por la Agencia de Protección de Datos de la Comunidad de Madrid*, Agencia de Protección de Datos de la Comunidad de Madrid, Madrid, 2006, pp. 247-257

FRAYSSINET, Jean, «La protection des données personnelles est-elle assurée sur l'Internet?, en Georges CHATILLON, Le *droit international de l'internet: actes du colloque organisé à Paris les 19 et 20 novembre 2001 par le Ministère de la Justice, l'Université Paris 1 Panthéon Sorbonne et l'Association Arpeje*, Bruylant, Bruselas, 2003, pp. 435-443

GARCÍA ONTOSO, Rosa, «Funciones de la Agencia de Protección de Datos y de las Agencias autonómicas», en VV. AA., *Jornadas sobre Protección de Datos personales*, Escuela Riojana de Administración Pública, Logroño, 2003, pp. 27-35

GÓMEZ MARTÍNEZ, Carlos, «El ejercicio de acciones civiles de protección de la intimidad del usuario de Internet. Aspectos procesales», en Carlos GÓMEZ MARTÍNEZ, (Dir.), *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2004, pp. 143-186

GRIMALT SERVERA, Pedro, «Deberes y responsabilidades en materia de protección de datos», en Santiago CAVANILLAS MÚGICA (Coord.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Comares, Granada, 2005, pp. 165-226

HERRÁN ORTIZ, Ana Isabel, «Los derechos de las personas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal», en Miguel Ángel DAVARA RODRÍGUEZ (Coord.), *XVII Encuentros sobre Informática y Derecho 2002-2003*, Universidad Pontificia de Comillas, Madrid, 2003, pp. 57-70

KUNER, Christopher, «The point of view on BCRs from a Large International Business Organization», en VV.AA., *Proceedings of the First European Congress on Data Protection, Madrid, 29-31 March 2006*, Fundación BBVA, Bilbao, 2008, pp. 185-188

LLÁCER MATACÁS, M.ª Rosa, «La Protección de los Datos Personales en Internet», en Inmaculada BARRAL VIÑALS, (Coord.), *La regul@ción del comercio electrónico*, Dykinson, Madrid, 2003, pp. 158-190

— «Las comunicaciones comerciales por vía electrónica», en Inmaculada BARRAL VIÑALS (Coord.), *La regul@ción del comercio electrónico*, Dykinson, Madrid, 2003, pp. 191-207

MARTÍN Y PÉREZ DE NANCLARES, José, «Comentario al artículo 8. Protección de Datos de Carácter Personal», en *Carta de los Derechos Fundamentales de la Unión Europea*, Fundación BBVA, Madrid, 2008, pp. 223-243

MUNAR BERNAT, Pedro A., «Protección de datos en el comercio electrónico», en Gema Alejandra BOTANA GARCÍA, (Coord.), *Comercio electrónico y protección de los consumidores*, La Ley, Madrid, 2001, pp. 275-306

OLIVER LALANA, A. Daniel, «Autorregulación, normas jurídicas y tecnologías de privacidad. El lado virtual del derecho a la protección de datos», en Miguel Ángel DAVARA RODRÍGUEZ (Coord.), *XVII Encuentros sobre Informática y Derecho 2002-2003*, Universidad Pontificia de Comillas, Madrid, 2003, pp. 85-102

PALLARO, Paolo, «La tutela della vita privata in relazione ai trattamenti dati personali in Internet: l´approccio della Comunità Europea», en *Diritto comunitario e degli scambi internazionali*, vol. 39, núm. 1, Editoriale Scientifica, Milano, 2000, pp. 7-35

PAYERAS CAPELLA, M.ª Magdalena y Josep Lluís FERRER GOMILA, «Explicación técnica de las amenazas de las TIC a la intimidad», en Carlos GÓMEZ MARTÍNEZ (Dir.), *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2004, pp. 77-106

PIÑAR MAÑAS, José Luis, «El derecho fundamental a la protección de datos personales. Contenido esencial y retos actuales. En torno al nuevo Reglamento de Protección de Datos», en José Luis PIÑAR MAÑAS y Álvaro CANALES GIL, *Legislación de protección de datos*, Iustel, Madrid, 2008, pp. 17-94

— «Nuevo Reglamento de Protección de Datos. Efectos en la Abogacía», en *Revista Abogados*, Consejo General de la Abogacía Española, Madrid, abril 2008, pp. 36-39

SUÑÉ LLINÁS, Emilio, «Marco jurídico del tratamiento de datos personales en la Unión Europea y en España», en VV.AA., *La armonización legislativa de la Unión Europea*, Dykinson, Madrid, 1999, pp. 245-274

— «La protección de la intimidad en el sector de las telecomunicaciones», en VV.AA., *La armonización legislativa de la Unión Europea (II)*, Dykinson, Madrid, 2000, pp. 367-380

TRONCOSO REIGADA, Antonio, «La contribución de las Agencias Autonómicas al derecho fundamental a la protección de datos», en Miguel Ángel DAVARA RODRÍGUEZ (Coord.), *XVII Encuentros sobre Informática y Derecho 2002-2003*, Universidad Pontificia de Comillas, Madrid, 2003, pp. 23-45

2. ARTÍCULOS

ÁLVAREZ-CIENFUEGOS SUÁREZ, José M.ª, «Notas a la nueva regulación de la protección de datos de carácter personal», en *La Ley*, núm. 5036, 17 de abril de 2000, pp. 1709-1716

ARENAS RAMIRO, Mónica, «La protección de datos personales en los países de la Unión Europea», en *Revista Jurídica de Castilla y León*, núm. 16, Septiembre 2008, pp. 113-168

ARIAS POU, María, «El futuro reglamento de la LOPD», en *La Ley*, núm. 6455, 4 de abril de 2006, pp. 1-5

BLOSS, Kevin, «Raising or razing the e-curtain?: the EU Directive on the Protection of Personal Data», en *Minnesota Journal of Global Trade*, vol. 9, 2000, pp. 645-661

CAMPUZANO LAGUILLO, Ana Belén, «Algunas consideraciones sobre la libertad informática y el derecho a la protección de datos de carácter personal en la jurisprudencia constitucional», en *Revista de Derecho y Nuevas Tecnologías*, Aranzadi, Cizur Menor (Navarra), 2003, pp. 99-103

CASTILLO JIMÉNEZ, Cinta, «Protección de la Intimidad en Internet», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, núm. 28, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 1998, pp. 461-468

DE MIGUEL ASENSIO, Pedro, Nota a la «Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal», en *Anuario de Derecho internacional Privado (2001)*, Tomo I, Iprolex, Madrid, 2001, pp. 621-627

— «Algunas tendencias jurídicas de la globalización», en *Los nuevos escenarios internacionales y europeos del Derecho y la Seguridad*, Colección Escuela Diplomática, núm. 7, Madrid, BOE-AEPDIRI, 2003, pp. 47-84

— «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», en http://www.uaipit.com, 2003, pp. 1-12

— «Avances en la interpretación de la normativa comunitaria sobre protección de datos personales», en *La Ley Unión Europea*, núm. 5964, Madrid, 2003, pp. 1-4

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

DEL PESO NAVARRO, Emilio, «La Protección de Datos y la Privacidad en Internet», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, núm. 33, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 2000, pp. 61-85

DIONNE BALAZ, Suzan and Oliver HANCE, «Privacy and the Internet: Intrusion, Surveillance and Personal Data», en *International Review of Law Computers & Technology*, vol. 10, núm. 2, 1996, pp. 219-234

DRESNER, Stewart H. (Traductor: Santiago RIPOLL CARULLA), «Panorama de la Legislación Europea sobre Protección de Datos Personales», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, números 6-7, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 1994, pp. 385-395

ESTADELLA YUSTE, Olga, «The draft Directive of the European Community regarding the protection of personal data», en *International and Comparative Law Quarterly*, vol. 41, January 1992, pp. 170-179

— «Spain is on the Road to Implementing EU Directive 95/46», en *International Review of Law Computers & Technology*, vol. 11, núm. 1, 1997, pp. 33-46

EWING, Mike, «The perfect storm: the safe harbour and the Directive on Data protection», en *Houston Journal of International Law*, vol. 24, núm. 2, pp. 315-344

FERNÁNDEZ CHATEIGNIER, Vanessa, «La protección jurídica del secreto de las comunicaciones en Internet», en La Ley, núm. 5732, Madrid, 2003, pp. 1-3

FERNÁNDEZ LÓPEZ, Juan Manuel, «Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD», en *Revista Española de Protección de Datos*, núm. 3, Julio-Diciembre 2007, Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, 2007, pp. 35-64

FLEISCHMANN, Amy, «Personal data security: divergent standards in the European Union and the United States», en *Fordham International Law Journal*, vol. 19, núm. 1, 1995, pp. 143-180

GARCÍA ONTOSO, Rosa M.ª, «Comentarios a la nueva Ley de Datos de Carácter Personal de 13 de diciembre», en *Actualidad Informática Aranzadi*, Aranzadi, Elcano (Navarra), 2000

GUERRERO PICÓ, M.ª del Carmen, «El derecho fundamental a la protección de los datos de carácter personal en la constitución Europea», en *RDCE*, núm. 4, Julio-Diciembre 2005, pp. 293-332

HIERRO, Antonio, «Automatic handling of personal data: treatment under Spanish law», en *Computer Law & Practice*, vol. 11, núm. 1, 1995, pp. 12-15

LLÁCER MATACÁS, M.ª Rosa, «La Protección de los Datos Personales en Internet», en Inmaculada BARRAL VIÑALS (Coord.), *La regul@ción del comercio electrónico*, Dykinson, Madrid, 2003, pp. 158-190

— «Las comunicaciones comerciales por vía electrónica», en BARRAL VIÑALS, Inmaculada (Coord.), *La regul@ción del comercio electrónico*, Dykinson, Madrid, 2003, pp. 191-207

MANRESA FARRERAS, Blanca, «Los datos personales en la legislación en materia de protección de datos: ¿Qué debe entenderse por dato de carácter personal?», en *REDI: Revista Electrónica de Derecho Informático*, núm. 45, 16 de marzo de 2002, pp. 1-5

MARTINEZ MARTINEZ, Ricard, «El Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Consideraciones Generales», en *Revista Española de Protección de Datos*, núm. 2, Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, 2007, pp. 63-94

MARZO, Ana, «Novedades de la Ley de Protección de Datos», en *Revista IURIS*, Madrid, 2002, pp. 42-47

OXMAN, Stephen A., «Exemptions to the European Union personal data privacy Directive: will they shallow the Directive?», en *Boston College International and Comparative Law Review*, vol. 24, núm. 1, 2000, pp. 191-203

PEARSON, Hillary E., «The Draft European Directives on the Protection of Personal Data», en *Computer Law & Practice*, vol. 7, núm. 4, pp. 182-187

PUENTE ESCOBAR, Agustín. «Reflexiones sobre el desarrollo reglamentario de la Ley Orgánica de Protección de Datos de carácter Personal» en *Protección de Datos*, *Otrosí*, *Boletín del Ilustre Colegio de Abogados de Madrid*, 2007

QUILEZ ÁGREDA, Ernesto, «Interpretación de la Ley Orgánica de Protección de Datos Personales conforme a la Constitución», en *Actualidad Jurídica Aranzadi*, año XIV, núm. 618, 1 de abril de 2004, Aranzadi, Cizur Menor (Navarra), pp. 9-11

REST, Alfred, «Transfrontier Environmental Damages: judicial competence and the *forum delicti commissi*», en *Environmental Policy and Law*, vol. 1, 1975, pp. 127-131

RETZER, Karin, Cynthia RICH y Miriam WUGMEISTER, «Corporate codes of conduct under scrutiny», en *Computer Law Review International*, núm. 5, 2003, pp. 129-132

ROCA JUNYENT, Miguel y Elisa TORRALBA MENDIOLA, «Ley de Protección de datos», en *La Ley*, núm. 5014, 16 de marzo de 2000, pp. 1733-1736

RODRÍGUEZ LAINZ, José Luis, «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», en *Diario La Ley*, núm. 8308, Sección Doctrina, 12 de Mayo de 2014

SALBU, Steven R., «The European Union Data Privacy Directive and International Relations», en *Vanderbilt Journal of Transnational Law*, vol. 35, núm. 2, 2002, pp. 655-695

SALEEM, Omar, «The establishment of a U. S. federal data protection agency to define and regulate internet privacy and its impact on U.S.-China relations: Marco polo where are you?, en *The John Marshall Journal of Computer & Information Law*, vol. 19, núm. 1, 2000, pp. 169-196

SERRERA COBOS, Pedro, «Breves notas sobre el RDLOPD», en *Revista Auditoría y Seguridad*, Fundación Dintel, núm. 20, 2008, pp. 138-139

SOLAR CALVO, Puerto, «La doble vía europea en protección de datos», en *Diario La Ley*, núm. 7832, Sección Doctrina, 4 de abril de 2012, Año XXXIII, Editorial LA LEY

STEELE, Jonathan, «Data protection: an opening door? The Relationship between Accessibility and Privacy in Sweden in an EU Perspective», en *The Liverpool Law Review*, vol. 24, núm. 1, pp. 19-39

TAN, Domingo R., «Personal privacy in the information age: comparison of Internet Data Protection Regulations in the United States and The European Union», en *Loyola of Los Angeles International and Comparative Law Journal*, vol. 21, núm. 4, 1999, pp. 661-684

TORRALBA MENDIOLA, Elisa, «La difamación en la era de las comunicaciones: ¿Nuevas? perspectivas de Derecho Internacional Privado Europeo», en *Revista inDret*, núm. 1/2012, disponible en http://www.indret.com

VIGURI PEREA, Agustín, «Intimidad versus informática. La protección de datos personales: perspectiva desde el Derecho comparado», en *La Ley*, núm. 2, 1999, pp. 1-10

VITALE, Angela, «The EU Privacy Directive and the Resulting Safe Harbour: The Negative Effects on U.S. legislation Concerning Privacy on the Internet», en *Vanderbilt Journal of Transnational Law*, vol. 35, núm. 1, pp. 321-358

XALABARDER PLANTADA, Raquel, «La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios», en *Revista IDP de los Estudios de Derecho y Ciencia Política de la UOC*, 2 (2006), pp. 01-15

WINER, Jonathan M., «Regulating the free flow of information: a privacy czar as the ultimate big brother», en *The John Marshall Journal of Computer & Information Law*, vol. 19, núm. 1, 2000, pp. 37-70

ZINSER, Alexander, «International data transfer out of the European Union: the adequate level of data protection according to article 25 of the European Data Protection Directive», en *The John Marshall Journal of Computer & Information Law*, vol. 21, núm. 4, 2003, pp. 547-565

C. Transferencia internacional de datos de carácter personal

1. MONOGRAFÍAS

ESLAVA RODRÍGUEZ, Manuela, *La protección civil del derecho a la vida privada en el tráfico privado internacional: derecho aplicable*, Universidad de Extremadura, Servicio de Publicaciones, Cáceres, 1996

ESTADELLA YUSTE, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995

GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, 2014

SANCHO VILLA, Diana, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003

— *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010

2. Estudios en obras colectivas

Aced Félez, Emilio, «Transferencias internacionales de datos», en Piñar Mañas, José Luis (Dir.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua-Guatemala, 2-6 de junio de 2003)*, Tirant lo Blanch, Valencia, 2005, pp. 105-127

Barceló, Rosa y M.ª Verónica Pérez Asinari, «Transferencia internacional de datos personales», en Ricard Martínez Martínez, (Coord.), *Protección de datos. Comentarios de desarrollo de la LOPD,* Tirant lo Blanch, Valencia, 2009, pp. 141-166

Bellamy, Bojana, «Case Study of Binding Corporate Rules», en VV.AA., *Proceedings of the First European Congress on Data Protection, Madrid, 29-31 March 2006*, Fundación BBVA, Bilbao, 2008, pp. 169-177

Calvo Caravaca, Alfonso-Luis y Javier Carrascosa González, «International Data Protection, Privacy, and Directive 95/46/EEC», en *Anfbruch Nach Europa*, Mohr Sieberck, TÜBINGEN, 2001, pp. 167-182

— — «La sumisión tácita como foro de competencia judicial internacional y el artículo 24 del Reglamento 44/2001, de 22 de diciembre 2000», en Alfonso-Luis Calvo Caravaca, y Santiago Areal Ludeña, *Cuestiones actuales del Derecho mercantil internacional*, Colex, Madrid, 2005, pp. 203-215

Heredero Higueras, Manuel, «La transmisión internacional de los datos de la salud», en Santiago Ripoll Carulla (Ed.), Jordi Bacaria Martrus (Coord.) y otros, *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Agencia Catalana de Protección de Datos, Marcial Pons, Madrid, 2006, pp. 187-211 y 329-331

HERRÁN ORTIZ, Ana Isabel, «Problemas jurídicos del flujo internacional de datos personales en la legislación española», en Miguel Ángel DAVARA RODRÍGUEZ, (Coord.), *XIII Encuentros sobre Informática y Derecho 1999-2000*, Aranzadi, Elcano (Navarra), 2000, pp. 81-93

Joan PIÑOL I RULL, y Olga ESTADELLA YUSTE, «La regulación de la transmisión internacional de datos en la L.O. 5/1992 de 29 de octubre», en Santiago RIPOLL I CARULLA (Coord.), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Universitat Pompeu Fabra, Barcelona, 1993, pp. 75-91

PUENTE ESCOBAR, Agustín, «International Data Transfers Based on the So-called 'Binding Corporate rules'», en VV.AA., *Proceedings of the First European Congress on Data Protection, Madrid, 29-31 March 2006*, Fundación BBVA, Bilbao, 2008, pp. 149-168

RUBÍ NAVARRETE, Jesús, «Transferencia internacional de datos», en Miguel Ángel DAVARA RODRÍGUEZ (Coord.), *XVII Encuentros sobre Informática y Derecho 2002-2003*, Universidad Pontificia de Comillas, Madrid, 2003, pp. 15-22

KOHSTAMM, Jacob, «What is the *Raison d´etre* of the Binding Corporate Rules?», en VV.AA., *Proceedings of the First European Congress on Data Protection, Madrid, 29-31 March 2006*, Fundación BBVA, Bilbao, 2008, pp. 139-147

USTARÁN, Eduardo, «Adoption of Binding Corporate Rules: Action Plan», en VV.AA., *Proceedings of the First European Congress on Data Protection, Madrid, 29-31 March 2006*, Fundación BBVA, Bilbao, 2008, pp. 179-183

VASALLO, John, «Practical Experience on Binding Corporate Rules», en VV.AA., *Proceedings of the First European Congress on Data Protection, Madrid, 29-31 March 2006*, Fundación BBVA, Bilbao, 2008, pp. 189-196

3. ARTÍCULOS

ANCOS FRANCO, Helena, «La regulación de las transferencias internacionales de datos de carácter personal como barrera al comercio internacional: de la Directiva 95/6 a los Acuerdos UE-Terceros Estados», en *RDCE*, núm. 6, Julio-Diciembre 1999, pp. 497-516

— «La progresiva configuración de las transferencias de datos como objeto del tráfico comercial internacional», en *Boletín ICE*, núm. 788, noviembre 2000, pp. 147-160

— «Las Transferencias Internacionales de datos de carácter personal como barrera al comercio internacional. El caso de los EE.UU.», en Miguel Ángel DAVARA RODRÍGUEZ (Coord.), *III Jornadas sobre Informática y Sociedad 2000*, Universidad Pontificia de Comillas, Madrid, 2001, pp. 23-42

ARRIBAS LUQUE, José María, «Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: el sistema de principios de puerto seguro», en *La Ley*, núm. 5497, 7 de marzo de 2002, pp. 1-10

BLAS, Frédéric, «Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales», en *Revista Derecho del Estado núm. 23, diciembre de 2009*, pp. 37-66

CARRASCOSA GONZÁLEZ, Javier, «Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado», en *Revista Española de Derecho Internacional,* vol. XLIV, núm. 2, 1992, pp. 417-441

— «Circulación internacional de datos personales informatizados y la Directiva 95/46/CE», en *Actualidad Civil*, núm. 23, 1997, pp. 509-539

CORDERO ÁLVAREZ, Clara Isabel, «Asuntos acumulado eDate Advertising y Martínez y Martínez (STJUE de 25 de octubre)», en *Foro, Nueva época*, núm. 14/2011, 267-268

DAVARA RODRÍGUEZ, Miguel Ángel, «La Transferencia Internacional de Datos», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid- CIVITAS, Madrid, 2007, pp. 17-60

DE MIGUEL ASENSIO, Pedro, recensión a Diana SANCHO VILLA, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003, 294 pp., en *REDI*, vol. LVI (2004), 1, pp. 636-639

ESTADELLA YUSTE, Olga, «Transborder Data Flows and the Sources of Public International Law», en *North Carolina Journal of International Law and Commercial Regulation*, vol. 16, 1990-1991, pp. 379-433

— «The draft Directive of the European Community regarding the protection of personal data», en *International and Comparative Law Quarterly*, vol. 41, January 1992, pp. 170-179

FERNÁNDEZ LÓPEZ, Juan Manuel, «Movimiento internacional de datos y buen gobierno corporativo», en *Boletín del Ilustre Colegio de Abogados de Madrid*, núm. 35, 3.ª ép., Febrero 2007, pp. 173-203

FLINT, David, «Internet: data transmission (EU)», en *Business Law Review*, vol. 19, núm. 7, 1998, pp. 180-181

GARCÍA DEL POYO, Rafael y GARI, Francisco, «Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales», en *Revista Española de Protección de Datos*, núm. 2, Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, 2007, pp. 239-266

GONZÁLEZ VAQUÉ, Luis, «El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EE.UU. para la transmisión de los datos sobre los pasajeros por las compañías aéreas», en *Civitas. Revista española de derecho europeo*, núm. 20, 2006, pp. 557-576

GUERRERO PICÓ, M.ª del Carmen, «Operadores privados y seguridad pública: la retención de los datos de tráfico a la luz de la sentencia PNR», en *Revista Española de Protección de Datos*, núm. 2, Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, 2007, pp. 185-215

MELL, Patricia, «A hichhiker's guide to trans-border data exchanges between EU member states and the United States under the European Union Directive on the protection of personal information», en *Pace International Law Review*, vol. 9, núm. 1, 1997, pp. 147-183

POULLET, Yves, «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid-CIVITAS, Madrid, 2007, pp. 93-113

PULIDO QUECEDO, Manuel, «La catequista y los riesgos de Internet», en *Actualidad Jurídica Aranzadi*, año XIII, núm. 602, 4 de diciembre de 2003, Aranzadi, Cizur Menor (Navarra), pp. 14-15

PUTNAM LOWRY, Houston, «Transborder data flow: public and private international law aspects», en *Houston Journal of International Law*, vol. 6, núm. 2, 1984, pp. 159-174

RIPOLL CARULLA, Santiago, «El Movimiento Internacional de Datos en la Ley Española de Protección de Datos», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, números 6-7, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 1994, pp. 313-322

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

SANCHO VILLA, Diana, «Normas corporativas vinculantes (*binding corporate rules*): aspectos sustantivos y de cooperación internacional de autoridades», en *Revista Española de Protección de Datos*, núm. 4. Enero-Junio 2008, pp. 35-60

II. Jurisprudencia de Interés

A. Unión Europea

Disponible en http://curia.europa.eu

– STJUE (Gran Sala) de 13 de mayo de 2014. Asunto C-131/12, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la Audiencia Nacional, mediante auto de 27 de febrero de 2012, recibido en el Tribunal de Justicia el 9 de marzo de 2012, en el procedimiento entre Google Spain, SL, Google Inc. y Agencia Española de Protección de Datos (AEPD), Mario Costeja González. «Datos personales – Protección de las personas físicas en lo que respecta al tratamiento de dichos datos – Directiva 95/46/CE – Artículos 2, 4, 12 y 14 – Ámbito de aplicación material y territorial – Motores de búsqueda en Internet – Tratamiento de datos contenidos en sitios de Internet – Búsqueda, indexación y almacenamiento de estos datos – Responsabilidad del gestor del motor de búsqueda – Establecimiento en territorio de un Estado miembro – Alcance de las obligaciones de dicho gestor y de los derechos del interesado – Carta de los Derechos Fundamentales de la Unión Europea – Artículos 7 y 8»

– STJUE (Sala Tercera) de 8 de abril de 2014. Asunto C-473/12. Asuntos C-293/12 y C-594/12. Electronic Communications – Directive 2006/24/EC – Publicly available electronic communications services or public communications networks services – Retention of data generated or processed in connection with the provision of such services – Validity – Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union.
– STJUE (Sala Tercera) de 7 de noviembre de 2013. Asunto C-473/12. Tratamiento de datos personales – Directiva 95/46/CE – Artículos 10 y 11 – Obligación de información – Artículo 13, apartado 1, letras d y g – Excepciones – Alcance de las excepciones – Detectives privados que actúan para el organismo de control de una profesión regulada – Directiva 2002/58/CE – Artículo 15, apartado 1.
– STJUE (Sala Tercera) de 18 de octubre de 2012, «Football Dataco II». Asunto C-173/11.
– STJUE (Sala Tercera) de 24 de noviembre de 2011. Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado. Peticiones de decisión prejudicial: Tribunal Supremo - España. Tratamiento de datos personales - Directiva 95/46/CE - Artículo 7, letra f - Efecto directo. Asuntos acumulados C-468/10 y C-469/10.
– STJUE (Gran Sala) de 25 de octubre de 2011. En los asuntos acumulados C-509/09 y C-161/10, que tienen por objeto dos peticiones de decisión prejudicial presentadas, con arreglo al artículo 267 TFUE, por el *Bundesgerichtshof* (Alemania) (asunto C-509/09) y por el *Tribunal de grande instance* de Paris (Francia) (asunto C-161/10), mediante sendas resoluciones de 10 de noviembre de 2009 y 29 de marzo de 2010, recibidas en el Tribunal de Justicia, respectivamente, el 9 de diciembre de 2009 y el 6 de abril de 2010.

– STJUE (Sala Tercera) de 5 de mayo de 2011 (petición de decisión prejudicial planteada por el *Bundesverwaltungsgericht*, Alemania) - Deutsche Telekom AG / *Bundesrepublik Deutschland* (Asunto C-543/09). Sobre «Comunicaciones electrónicas - Directiva 2002/22/CE - Artículo 25, apartado 2 - Directiva 2002/58/CE - Artículo 12 - Prestación de servicios de información sobre números de abonados y guías - Obligación, impuesta a una empresa que asigna números de teléfono, de transmitir a otras empresas los datos que posea relativos a los abonados de terceras empresas».
– STJUE de 9 de noviembre de 2010, C-92/09 y C-93/09. «Protección de las personas físicas en lo que respecta al tratamiento de datos personales – Publicación de información sobre los beneficiarios de ayudas agrícolas – Validez de las disposiciones del Derecho de la Unión que establecen dicha publicación y determinan sus modalidades – Carta de los Derechos Fundamentales de la Unión Europea – Artículos 7 y 8 – Directiva 95/46/CE – Interpretación de los artículos 18 y 20».
– STJUE de 16 de julio de 2009, C-189/08, *Zuid-Chemie BV*, FD 27 y 28.
– STJUE de 16 de diciembre de 2008, C-73/07, *Tietosuojavaltuutettu*.
– STJUE de 27 de octubre de 1998, C-51/97.
– STJUE de 30 de mayo de 2006, C-317/04 y 317/05, *Parlamento/Consejo*.
– STJUE de 10 de junio de 2004, C-168/2002.
– STJUE de 6 de noviembre de 2003, C-101/01, *Lindqvist*.
– STJUE de 20 de mayo de 2003, C-138/01, C-139/01 y C-465/00, *Österreichischer Rundfunk* y otros.
– STJUE asunto *Alblasgracht VOO2*, de 27 de octubre de 1998 (C-51/1997).
– STJUE de 19 de septiembre de 1995, *Marinarai*.
– STJUE en el asunto *Fiona Shevill*, de 7 de marzo de 1995.

– STJUE de 26 de marzo de 1992, *Reichert y Kockler*, C-261/90.
– STJUE de 11 de enero de 1990, *Dumez*.
– STJUE, asunto *Kalfelis c. Banco Schöder, Münchmeyer, Hengst & Co. y otros*, de 27 de septiembre de 1988, (asunto C-189/1987).
– STJUE de 24 de junio de 1980, *Elefanten Schuh*.
– STJUE de 9 de noviembre de 1978, *Meeth*.
– STJUE de 14 de diciembre de 1976, asunto 24/76, *Colzani c. RÜWA*.
– STJUE de 30 de noviembre de 1976, *Bier vs. Mines de Potase d´Alsace*.
– STJUE de 12 de noviembre de 1969, *Stauder*.

B. España

1. Tribunal Constitucional

– STC 292/2000, de 30 de noviembre de 2000 (RTC 2000\292).
– STC 290/2000, de 30 de noviembre de 2000 (RTC 2000\290).
– STC 202/1999, de 8 de noviembre de 1999 (RTC 1999\202).
– STC 44/1999, de 22 de marzo de 1999 (RTC 1999\44).
– STC 30/1999, de 8 de marzo de 1999 (RTC 1999\30).
– STC 158/1998, de 13 de julio de 1998 (RTC 1998\158).
– STC 126/1998, de 15 de junio de 1998 (RTC 1998\126).
– STC 125/1998, de 15 de junio de 1998 (RTC 1998\125).
– STC 124/1998, de 15 de junio de 1998 (RTC 1998\124).
– STC 123/1998, de 15 de junio de 1998 (RTC 1998\123).
– STC 104/1998, de 18 de mayo de 1998 (RTC 1998\104).
– STC 106/1998, de 18 de mayo de 1998 (RTC 1998\106).
– STC 105/1998, de 18 de mayo de 1998 (RTC 1998\105).
– STC 94/1998, de 4 de mayo de 1998 (RTC 1998\94).
– STC 60/1998, de 16 de marzo de 1998 (RTC 1998\60).
– STC 11/1998, de 13 de enero de 1998 (RTC 1998\11).

– STC 143/1994, de 9 de mayo de 1994 (RTC 1994\143).
– STC 254/1993, de 20 de julio de 1993 (RTC 1993\254).

2. TRIBUNAL SUPREMO

– STS, Sala de lo Contencioso-Administrativo, de 15 de julio de 2010 (Recursos núm. 23/2008, 25/2008 y 26/2008).
– STS núm. 7551, de 18 de septiembre de 2003 (RJ 2003\6075).
– STS núm. 8672, de 23 de septiembre de 2002 (RJ 2002\8672).
– STS núm. 8643, de 29 de julio de 2002 (RJ 2002\6357).
– STS núm. 5435, de 26 de abril de 2002 (RJ 2002\5565).
– STS núm. 3608, de 18 de abril de 2002 (RJ 2002\3608).
– STS núm. 4689, de 15 de abril de 2002 (RJ 2002\6315).
– STS núm. 9380, de 13 de abril de 2002 (RJ 2002\4251).
– STS núm. 9380, de 28 de octubre de 2000 (RJ 2000\9380).

3. AUDIENCIA NACIONAL

– SAN, Sala de lo Contencioso-Administrativo, de 11 de febrero de 2004 (RJCA 2004\421).
– SAN, Sala de lo Contencioso-Administrativo, de 15 de marzo de 2002 (RJCA 2002\784).
– SAN, Sala de lo Contencioso-Administrativo, de 21 de septiembre de 2001 (JUR 2001\294008).
– SAN, Sala de lo Contencioso-Administrativo, de 6 de julio de 2001 (JUR 2001\293812).

III. ENLACES *WEB* DE INTERÉS

A. Foros internacionales

1. INSTITUCIONES INTERGUBERNAMENTALES

Conferencia Interamericana especializada en Derecho internacional privado (CIDIP):
http://www.oas.org

Conferencia de La Haya de Derecho internacional privado:
http://www.hcch.net

Instituto Internacional para la Unificación del Derecho Privado (Unidroit):
http://www.unidroit.org

Organización de las Naciones Unidas (ONU):
http://www.un.org

Organización Mundial del Comercio (OMC):
http://www.wto.org

Organización Mundial de la Propiedad Intelectual (OMPI):
http://www.ompi.org

Organización para la Cooperación y el Desarrollo Económicos (OCDE):
http://www.oecd.org
UNCITRAL:
http://www.uncitral.org

2. INSTITUCIONES DE LA UE

Autoridad Común de Control de Europol:
https://www. europol.europa.eu
Autoridad Común de Control de Schengen:
www.schengen-jsa.dataprotection.org
Comisión Europea:
http://ec.europa.eu
Consejo de Europa:
www.coe.int
Consejo UE:
http://www.european-council.europa.eu
Grupo del artículo 29:
http://europa.eu/justice/data-protection
Parlamento Europeo:
www.europarl.europa.eu
Supervisor Europeo de Protección de Datos:
http://www.edps.eu.int
Tribunal de Justicia UE:
http://curia.europa.eu/es

3. INSTITUCIONES PRIVADAS

Cámara de Comercio Internacional (CCI):
http://www.iccwbo.org

Institut de Droit International:
http://www.idi-iil.org

4 Autoridades de Protección de Datos en Europa

Alemania:
www.bfdi.bund.de
Andorra:
https://www.apda.ad
Austria:
www.dsk.gv.at
Bélgica:
www.privacycommission.be
Bulgaria:
www.cpdp.bg
Chipre:
www.dataprotection.gov.cy
Dinamarca:
www.datatilsynet.dk
Eslovaquia:
www.dataprotection.gov.sk
Eslovenia:
www.varuh-rs.si
Estonia:
www.dp.gov.ee
Finlandia:
www.tietosuoja.fi
Francia:
www.cnil.fr

Grecia
www.dpa.gr
Guernsey:
www.dataprotection.gov.gg
Hungría:
www.naih.hu
Irlanda:
www.dataprivacy.ie
Islandia:
www.personuvernd.is
Italia:
www.garanteprivacy.it
Jersey:
www.dataprotection.gov.je
Letonia:
www.dvi.gov.lv
Liechtenstein:
www.sds.llv.li
Lituania:
www.ada.lt
Luxemburgo:
www.cnpd.lu
Malta:
www.dataprotection.gov.mt
Noruega:
www.datatilsynet.no
Países Bajos:
www.cbpweb.nl
Polonia:
www.giodo.gov.pl

Portugal:
www.cnpd.pt
Reino Unido:
www.ico.gov.uk
República Checa:
www.uoou.cz
Rumanía:
www.avp.ro
Suecia:
www.datainspektionen.se
Suiza:
www.edsb.ch

5. Autoridades de Protección de Datos en Iberoamérica

Argentina:
http://www.jus.gov.ar/dnpdp
Chile – Servicio de Registro Civil e Identificación:
http://www.registrocivil.cl
http://www.modernizacion.cl
Colombia:
http://www.defensoria.org.co
México:
http://www.ifai.org.mx
Nicaragua:
http://www.conicyt.gob.ni

6. Otras instituciones de Protección de Datos en otros países

Australia:
www.privacy.gov.au
Canadá:
www.privcom.gc.ca
EE.UU. (Federal Trade Commission, FTC, web en español):
www.ftc.gov/ftc/spanishinfo/consumer.htm
EE.UU. (Departamento de Seguridad Interior):
www.dhs.gov
Hong Kong:
www.pco.org.hk
Nueva Zelanda:
www.privacy.org.nz

B. Foros nacionales

Agencia Española de Protección de Datos (AEPD):
http://www.agpd.es
Autoridad Catalana de Protecció de Dades:
http://www.apdcat.net
Agencia Vasca de Protección de Datos:
http://www.avpd.euskadi.net/s04-4319/es/
Congreso de los Diputados:
www.congreso.es
Ministerio de Justicia:
www.mju.es
Poder Judicial:
www.poderjudicial.es

Portal del Ciudadano:
www.administracion.es
Senado:
www.senado.es
Tribunal Constitucional:
www.tribunalconstitucional.es

C. Otros foros

Asociación Profesional Española de Privacidad (APEP):
http://www.apep.es
Blog Conflictus Legum:
http://conflictuslegum.blogspot.com
Blog de Pedro de Miguel Asensio:
http://pedrodemiguelasensio.blogspot.com
Blog del Departamento Derecho internacional público y Derecho internacional privado UCM:
http://blogs.uab.cat/adipr
Blog Lvcentinvs:
http://lucentinus.blogspot.com
IPR-Helpdesk:
http://www.ipr-helpdesk.org
Asociación Española para el Fomento de la Seguridad de la Información (ISMS FORUM Spain):
https://www.ismsforum.es
Portal de la Universidad de Alicante sobre Propiedad Industrial e Intelectual y Sociedad de la Información –UAIPIT:
http://www.uaipit.com

Calvo Caravaca & Carrascosa González. Grupo universitario español de investigación, docencia y práctica del Derecho internacional privado: http://www.accursio.com