ALGUNAS CUESTIONES RELEVANTES DE DERECHO INTERNACIONAL PRIVADO DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

SOME RELEVANT ISSUES ABOUT INTERNATIONAL PRIVATE LAW OF IN GENERAL DATA PROTECTION REGULATION

Rev. Boliv. de Derecho Nº 26, julio 2018, ISSN: 2070-8157, pp. 404-437

Juan José
GONZALO
DOMÉNECH

ARTÍCULO RECIBIDO: 2 de febrero de 2018
ARTÍCULO APROBADO: 10 de abril de 2018

RESUMEN: El presente trabajo tiene como objetivo analizar el régimen de Derecho internacional privado del nuevo Reglamento General de Protección de Datos, tales como los supuestos de aplicación, la competencia judicial internacional, y la determinación de la ley aplicable a las controversias judiciales. El RGPD muestra un avance parcial en esta materia, puesto que presenta problemas con la compatibilidad con el Reglamento Bruselas I bis, y no existen avances en la determinación de la ley aplicable.

PALABRAS CLAVE: RGPD; Derecho internacional privado; Competencia judicial internacional; ley aplicable; protección de datos.

ABSTRACT: This paper aims to analyse the international private law regime of the new General Data Protection Regulation, such as the application of European law, international jurisdiction, and the determination of the applicable law to lawsuits. The GDPR shows a partial progress in this area, since it presents problems with the compatibility in the Brussels I bis Regulation, and there is no progress in determining the applicable law.

KEY WORDS: GDPR; Private international law; International jurisdiction; applicable law; data protection.

I. INTRODUCCIÓN.

La sociedad de la información ha evolucionado. La rigidez de las actuales normas ha provocado una "obsolescencia programada" de la regulación sobre protección de datos por el nacimiento de nuevas tecnologías tales como el *Big Data*, *Internet of Things*, o *Cloud Computing*. El nuevo Reglamento 679/2016, General de Protección de Datos[1] tiene como objetivo principal actualizar el marco regulatorio europeo sobre protección de datos para adaptarlo a la nueva realidad tecnológica y los nuevos ataques contra la privacidad que se derivan del uso de dichas tecnologías. Por ello la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales[2]. Es por ello que la sociedad de la información se ha transformado en la sociedad del dato.

1 DOUE L 119/1, de 4 de mayo de 2016.

2 Considerando 6 del RGPD.

• Juan José Gonzalo Doménech
Graduado en Derecho (UMH), y estudiante del Máster en Derecho de las Telecomunicaciones y protección de datos (UC3M). Colaborador del área de Derecho internacional privado de la UMH. Ganador del IX premio Jurídico Internacional del ISDE.

El RGPD ha transformado el sistema de Derecho internacional privado para adaptarlo a las disputas globales y multi-jurisdicionales que genera la protección de datos[3]. En el presente artículo, se tratará la reclamación de los afectados debido al uso ilícito de los datos personales tratados desde la perspectiva del Derecho internacional privado, explicando el nuevo derecho a la indemnización que establece el RGPD, y abordando las cuestiones sobre la determinación de la competencia judicial internacional por el nuevo régimen de compatibilidad entre el Reglamento Bruselas I bis y el RGPD, y de la ley aplicable a la controversia, cuyas novedades son nulas en esta última, y nos vuelven a obligar a aplicar las leyes autónomas.

II. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS.

Debido a la globalización, la deslocalización, la variedad de opciones para el tratamiento de datos, y la posibilidad de que un tratamiento realizado fuera del territorio de la Unión quede sujeto a la legislación europea[4] por la permeabilidad de las fronteras en materia de protección de datos[5], conviene analizar el artículo 3 del RGPD para explicar los supuestos en los que el tratamiento de datos está sujeto al Derecho de la Unión, cuyo alcance es mucho mayor por su extraterritorialidad (o *long-arm jurisdiction* en la doctrina anglo-sajona)[6] que la actual Directiva[7], con el objetivo de evitar los problemas acaecidos por el intercambio de datos con EE.UU[8].

En comparación con la rúbrica estipulada en la Directiva 95/46/CE, la cual rezaba en su equivalente actual al complejo artículo 4 "Derecho nacional aplicable"[9], el artículo 3 del RGPD adopta como rúbrica "Ámbito territorial", esto se debe a que el Reglamento tiene por objeto unificar la normativa en Europa, y reforzar el derecho fundamental a la protección de datos, más que concretar la ley del

3 Kuner, C.: *"The Internet and the Global Reach of EU Law", Legal studies research. Paper series*, 2017, núm. 24, p. 20.

4 Kuner, C.: *"The European Union and the Search for an International Data Protection Framework", Groningen Journal of International Law*, 2015, vol. 2, ed. 1, p. 61.

5 Carrascosa González, J., y Calvo Caravaca, A-L.: *Derecho internacional privado*, Vol. II Comares, Granada, 16ª ed, 2016, p. 1378.

6 Moerel, L.: "*The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", International Data Privacy Law*, 2011, núm 1°, vol. 1, pp. 28-46.

7 Taylor, M.: *"Permissions and prohibitions in data protection jurisdiction", Brussels Privacy* Hub *working paper*, 2016, núm. 6, vol. 2, p. 13.

8 Schiedermair, S.: *"The new General Data Protection Regulation of the European Union-Will it widen the gap between Europe and the U.S?"*, en AA.VV. (coord. por Dörr, D., y Weaver, R.), *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries*, De Gruyter, Berlín, 2015, p. 76.

9 El artículo 4 de la Directiva, mas que verse como una cláusula de "mercado interno", concepción que tenía el legislador europeo, se consideraba más una norma de Derecho internacional privado, en cuanto se le atribuía la función de determinar la ley aplicable al tratamiento de datos dentro de la Unión Europea. Piroddi, P. *"profili internacional-privatistici della responsabilità delgestore di un motore di ricerca per li trattamento dei dati personali"*, en AA.VV. (dirigido por Resta, G., y Zeno-Zencovich, V.), *Il Dirito all' oblio su internet dopo la sentenza Google Spain, Roma TrE-`ress,* Roma, 2015, p. 66.

Estado miembro que se debe aplicar, salvo algún supuesto[10]. Por ello, las empresas se enfrentarán a un solo derecho paneuropeo de protección de datos, no a veintiocho; ignorando las posiciones que defienden que el nuevo RGPD puede provocar más diferencias entre los Estados miembros de las que existen a día de hoy por a remisión que prevé la norma a los Estados miembros para que legislen sobre determinados elementos dispositivos del RGPD, olvidando que, al ser un reglamento, y no una Directiva, la aplicación de esta nueva norma es directa para todos los Estados miembros[11]. Esto se manifiesta en la declaración conjunta de las Autoridades de España, Francia, Bélgica, Holanda y Hamburgo han determinado que la hipótesis de Facebook, de someterse solamente a la legislación irlandesa, es errónea, puesto que el argumento principal de Facebook es que el tratamiento de dichos datos es realizado en su filial irlandesa, obviando la doctrina sentada por el TJUE[12] cuya manifestación se ha visto en la Resolución R/01870/2017 de la AEPD contra Facebook, y que veremos a continuación que dicha problemática planteada será alterada por el nuevo régimen del RGPD.

Debemos partir de la definición de "tratamiento" realizada por el RGPD en el artículo 4. b), definido como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Esta definición debe tener una concepción finalista por el cual el tratamiento se refiere a utilización de datos personales de una base de datos o fichero, entendido este como un conjunto organizado de datos[13], con la consecuencia de que prácticamente cualquier actividad con datos personales quedará englobada en el concepto de "tratamiento"[14]. El concepto de tratamiento está directamente ligado al de dato personal; y ya que la mera recogida de datos considerados personales supone un "tratamiento", este acto supone causa suficiente para la aplicación de la normativa europea sobre protección de datos.

El artículo 3 del RGPD se compone de tres supuestos que a continuación pasaremos a explicar a la luz del "Dictamen 8/2010 sobre el Derecho aplicable",

10 Como la determinación de la edad mínima del menor para otorgar su consentimiento (artículo 8 del RGPD).

11 Albrecht, J. P.: *"How the GDPR Will Change the World", European Data Protection Law Review*, 2016, núm. 3°, vol. 2, pp. 287-289.

12 *Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium.* 16 May 2017. Disponible en: http://www.agpd.es/portalwebAGPD/noticias-inicio/common/pdf/2017/05_may_17/Common_Statement_16_May_2017.pdf

13 Erdozáin López, J. C.: "La protección de los datos de carácter personal en las telecomunicaciones", *Revista Doctrinal Aranzadi Civil-Mercantil*, 2007, núm. 1°, p. 2.

14 Erdozáin López, J. C.: "La protección", cit, p. 3.

actualizado a 2015, y la doctrina establecida por el TJUE[15]. Como rasgo general, el artículo 3 presenta un doble criterio para determinar la aplicación de la normativa[16]: 1) el principio de país de origen, que se centran en la ubicación geográfica del tratamiento y el uso de los datos, y 2) el principio de mercado, que se orienta hacia el mercado objetivo.

1. En el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea.

El artículo 3.1 estipula que se aplicará la legislación europea cuando ese tratamiento de datos se lleve a cabo en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. Así pues; cualquiera de esos actos realizados sobre los datos personales de cualquier individuo en el ámbito de la Unión se les aplicará la legislación europea.

La cuestión más discutida por el TJUE ha sido la definición de "establecimiento". Tanto la Directiva en su Considerando 19 como el RGPD en su Considerando 22 describen que "un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto".

En este sentido, la STJUE *Weltimmo* busca establecer un concepto flexible de establecimiento "que rechaza cualquier enfoque formalista según el cual una empresa estaría establecida únicamente en el lugar en que se encontrase registrada. Por lo tanto, para determinar si una sociedad, responsable de un tratamiento de datos, dispone de un establecimiento [...] procede interpretar tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades en ese otro Estado miembro tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión" (párrafo 29).

El TJUE establece un criterio de ponderación sobre la base del tipo de prestación o actividad que la empresa ejerza u oferte en otro Estado miembro, llegando a bastar un solo representante en otro Estado miembro si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación de los servicios en la Unión[17].

15 SSTJUE de 20 de junio de 2014, *Google Spain*, C-131/12; 1 de octubre de 2015, *Weltimmo*, C-230/14, y 21 de diciembre de 2016, *Amazon EU Sàrl*, C-362/14.

16 Zell, A-M.: *"Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field"*, *German Law Journal*, 2014, 2014, vol. 15, p. 482.

17 De Miguel Asensio, P.A.: "Aspectos internacionales de la protección de datos: las sentencias *Schrems* y *Weltimmo* del Tribunal de Justicia", *La Ley Unión Europea*, 2015, núm. 31°, p. 8.

En definitiva, el concepto de "establecimiento" se extiende a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable (párrafo 31). Se utiliza esta concepción flexible de establecimiento para garantizar el derecho a la protección de datos, como reza el Considerando 23 del RGPD.

A todo esto, el artículo 4. 16) del RGPD ha considerado en su definición el concepto de "establecimiento principal". La inclusión de dicha definición aclara y delimita cuestiones altamente relevantes como la concreción de un establecimiento principal del responsable o de un encargado con varios establecimientos en la Unión mediante reglas marcadas por el principio de especialidad y jerarquía.

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

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

Tal y como se acaba de decir, y como se dicta en reiteradas SSTJUE[18], tal tratamiento debe llevarse a cabo "en el contexto de las actividades del establecimiento". Para explicar tal concepto, debemos acudir al Dictamen 8/2010, el cual aporta una serie de elementos para valorar si ese tratamiento se desarrolla en tal contexto:

1º) Grado de implicación del establecimiento en las actividades en cuyo contexto se traten los datos personales. Consiste en determinar qué actividades realiza cada establecimiento, y determinar que que tales actividades están comerciales están destinados a cualquier Estado miembro de la Unión Europea[19].

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

18 *Google Spain*, C-131/12, ECLI:EU:C:2013:424 (pár. 52); *Weltimmo*, C-230/14 ECLI:EU:C:2015:639 (pár. 35), y *Amazon EU Sàrl*, C-362/14 ECLI:EU:C:2015:650 (pár. 78).

19 STJUE *Amazon EU Sàrl*, (pár. 76).

A todo esto; se le debe añadir la doctrina que estableció la STJUE en el caso *Google Spain*, exige confirmar que las actividades de un establecimiento local y las actividades de procesamiento de datos puedan estar inextricablemente vinculadas, Incluso si ese establecimiento no está asumiendo realmente ningún papel en el propio procesamiento de datos.

En resumen, si el tratamiento de los datos se lleva a cabo por establecimientos no establecidos en la Unión, y el establecimiento en la Unión no interviene en dicho tratamiento, las actividades llevadas a cabo por ese establecimiento pueden, subsidiariamente, otorgar la protección que ofrece la legislación europea, siempre que exista esa "vinculación inextricable" entre las actividades del establecimiento en la Unión y el procesamiento de datos, independientemente de que el tratamiento se lleve a cabo en la Unión.

La STJUE *Google Spain* determinó que un establecimiento cuya actividad principal son los servicios publicitarios web mediante los motores de búsqueda puede ser suficiente como para que la legislación europea sea de aplicación; pero existen varias formas para en las que una empresa puede organizarse, sin tener que ser esta una de ellas. Cada caso es distinto, y se deben atener a los hechos del caso concreto. Ni la sentencia debe interpretar de forma totalmente expansiva, ni de forma restrictiva a las empresas con modelos de negocio relacionados con los motores de búsqueda.

2. Actividades de tratamiento relacionadas con la oferta de bienes o servicios a afectados en la Unión Europea, independientemente de si a estos se les requiere su pago.

Como apunte general al criterio de la situación del afectado del apartado 3.2 del RGPD, facilita el sometimiento a la legislación europea de quienes no están establecidos en la Unión y tratan datos de individuos que se encuentran en ese territorio en circunstancias en las que se observa necesario aplicarlas[20]. Este criterio genera una mayor protección de los individuos al haber ampliado en alcance de la norma, sobre todo en lo que viene siendo la monitorización de su conducta[21].

El presente artículo ha de ponerse en relación con el artículo 27 y el Considerando 80, los cuales obligan al responsable o encargado de nombrar a un representante establecido en la Unión en relación con las obligaciones que estipula el RGPD.

20 De Miguel Asensio, P. A.: "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea", *Revista Española de Derecho Internacional*, 2015, núm. 1°, vol. 69, 2017, p. 14.

21 Hijmans, H.: *The European Union as Guardian of Internet Privacy: The Story of Artículo 16 TFEU*, Springer, Bruselas, 2016, p. 559.

Pasando a estudiar el inciso a), debemos partir de la descripción que realiza el Considerando 23, el cual determina que si el responsable o encargado ofrece bienes o servicios a afectados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a afectados en uno o varios de los Estados miembros de la Unión (*targeting-based analysis*)[22]. El Considerando no contempla que la accesibilidad web, el uso de un tercer idioma común o datos de contacto como indicios de oferta de servicios y productos en la Unión, como dicta la STJUE *Wertimmo*. Sí considera, por el contrario, el uso de la lengua, la moneda, o la mención de clientes o usuarios que residen en la Unión indicios de que el encargado o responsible dirige su oferta al territorio de la Unión.

Podemos considerar que, salvaguardando las distancias entre un caso y otro, sería de aplicación los criterios mostrados en la doctrina creada por la STJUE *Pammer y Hotel Alpenhor*[23], y consolidada en las SSTJUE *Mühlleitner*[24], y *Emrek*[25][26].

Uno de los criterios más relevantes de esa sentencia es tener en cuenta "todas las manifestaciones de voluntad de atraer a los consumidores de dicho Estado", como la oferta de tales servicios o productos en el Estado miembro, o la publicidad en distintos medios que facilitan su conocimiento por consumidores del Estado. La STJUE ofrece un listado de indicios no exhaustivos, en los que se consideran como tal 1) el carácter internacional de la actividad; 2) la indicación del prefijo internacional en los números de teléfono; 3) utilización de un nombre de dominio de primer nivel geográfico distinto al del Estado del vendedor; 4) descripción de un itinerario de envío desde un Estado miembro al lugar de la prestación del servicio; 5) la mención de una clientela internacional formada por clientes domiciliados en un Estado miembro, y 6) el empleo de lenguas o divisas que no se corresponden con las habituales en el Estado a partir del cual ejerce su actividad el empresario[27].

Pero podemos ver cumplida las condiciones del artículo 3.2 a) del RGPD cuando cualquier servicio o actividad es ofertada sin restricciones geográficas respecto de la UE, y son adquiridos por un número significativo de habitantes de la Unión[28].

22 Geist, M.: *"Is There a There There? Toward Greater Certainty for Internet Jurisdiction",* 2001, *Berkeley Technology Law Journal*, núm. 3º, vol. 16, pp. 1345-1406.

23 STJUE de 7 de diciembre de 2010, *Pammer and Hotel Alpenhof* , C-585/08, ECLI:EU:C:2010:740.

24 STJUE de 6 de septiembre de 2012, *Daniela Mühlleitner,* C-190/11.

25 STJUE 17 de octubre de 2013, *Emrek,* C□218/12, ECLI:EU:C:2013:494.

26 El caso tratado en las SSTJUE citada no versa sobre protección de datos, sino de controversias en materia mercantil.

27 La doctrina establecida por el TJUE deriva de la establecida por la *Supreme Court* estadounidense *Calder v. Jones* (465 U.S. 783 (1984)), en la que permite a los tribunales considerar si existe un mercado objetivo determinado mediante el uso de elementos como la lengua utilizada, la divisa, o la nacionalidad. Aunque algún sector entiende que a esta doctrina se le puede achacar su fuerte componente subjetivo. Jiménez-Benítez (2015) p. 30.

28 De Miguel Asensio, P.A.: "Aspectos internacionales", cit, p. 16.

Debemos reseñar la dicotomía literal entre la versión en inglés del RGPD con la versión en español. La versión inglesa exige que los afectados solo "estén" en la Unión Europea (*data subjects who are in the Union*), mientras que en la versión en español exige que los afectados "residan". Esto ha causado una disparidad de criterio entre artículos de escritura inglesa respecto a una posible interpretación amplia del artículo, haciendo que el RGPD pueda extralimitarse en su aplicación extraterritorial[29].

3. Actividades de tratamiento relacionadas con el control de su comportamiento, en la medida en que este tenga lugar en la Unión Europea.

El artículo 3.2 b) del RGPD será de aplicación cuando el tratamiento de los datos de los afectados que verse sobre la observación del comportamiento, en la medida en que este tenga lugar en la Unión y si el responsable o encargado no estuviera establecido en la Unión. Mientras la doctrina tiene asumida que este supuesto está destinado solamente al uso de archivos o programas informáticos que almacenan y permiten acceso al dispositivo de usuario (*cookies*), y excluye por lo tanto el ofrecimiento de productos o servicios[30]. Considero que este artículo puede incluirse directamente en los productos ofertados mediante el uso del *Big Data* que, al fin y al cabo, no hace más que monitorizar el comportamiento del ser humano.

Si entendemos el comportamiento como el conjunto de actos realizados por el ser humano producido por la interacción con el entorno en el que vive, algunas de las categorías de datos tratados por el *Big Data* revelan dichos actos[31].

El presente artículo hay que ponerlo en relación con el Considerando 24, que determina que se entenderá como un control de comportamiento el seguimiento del afectado en Internet; pero a continuación estipula una referencia resume a la perfección el objeto y la esencia del *Big Data*[32].

Por las razones anteriores, consideramos que el artículo 3.2 b) del RGPD es aplicable no solo a la motorización de los comportamientos mostrados en

29 Brkan, M.: *"Data protection and conflict-of-laws: a challenging relationship", European Data Protection Law Review,* 2016, núm. 3°, vol. 2, p. 337; Svantesson, D. J.: *Extraterritoriality in Data Privacy Law*, Ex tuto Publishing, Copenhague, 2013, p. 107. Los autores discuten sobre la incoherencia del artículo 3.2 a) respecto al resto del RGPD, afirmando que el artículo debe exigir la residencia.

30 Albrecht, J. P., y Jotzo, F.: *Das neue Datenschutzrecht der EU*, Nomos, Baden-Baden, 2017., p. 67; Ernst, S: *"Allgemeine Bestimmungen",* en AA.VV. (Coord. por B. Paal y D. Pauly), *Datenschutz-Grundverordnung*, Beck, Munich C.H. 2017, pp. 25-26; De Miguel Asensio, P.A.: "Competencia ", cit, p. 16.

31 P. ej., la ubicación de los individuos, los hábitos diarios relacionados con las horas de sueño o la actividad deportiva.

32 *inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.*

Internet; sino también a cualquier motorización realizada por cualquier medio destinado a ello.

III. DERECHO A INDEMNIZACIÓN DEL RGPD.

Debemos resaltar que la acción de responsabilidad contemplada en el RGPD se refiere a una responsabilidad extracontractual como explicaremos con más detenimiento posteriormente, puesto que se resuelve fuera de un hipotético marco contractual. Aunque debemos destacar la existencia de una eventual responsabilidad contractual en el caso de que una empresa se haya comprometido a custodiar los datos conforme a la legislación vigente y a los fines que se determinen en el propio contrato.

El RGPD regula por primera vez el derecho a la indemnización derivado de los daños causados por el tratamiento ilegal de los datos de carácter personal en el artículo 82; al contrario que la Directiva, la cual se dedicaba en el artículo 23 a obligar a los Estados a configurar el derecho a la indemnización en sus ordenamientos internos.

El artículo 82 establece la responsabilidad del responsable del tratamiento que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Se estables la responsabilidad del responsable cuando participe en una operación el no cumpla, tanto por acción como por omisión, las normas del RGPD dirigidas a los encargados, o cuando el encargado obvie las indicaciones del responsable.

El RGPD establece un sistema de responsabilidad directa del responsable del tratamiento por los daños causados a una persona física tanto si el tratamiento se llevase a cabo en un establecimiento del responsable como si se externalizase a un tercero encargado. La responsabilidad de este último es limitada, puesto que solo responderá cuando el daño y perjuicio deriven de un incumplimiento de las obligaciones legales del RGPD y de sus normas derivadas. Podemos entender cómo lógica esta limitación, puesto que el encargado del tratamiento actúa por mandato del responsable[33].

Cuando nos referimos al incumplimiento de lo dispuesto en el RGPD, incluimos un tratamiento que infrinja también los actos delegados y de ejecución de conformidad con el RGPD, así como las normas de desarrollo aportadas por los Estados miembros en cumplimiento del RGPD[34].

33 Recio Gayo, M.: "Acerca de la evolución de la figura del encargado del tratamiento", *Revista de Privacidad y Derecho Digital,* 2015, nº 0, p. 37.

34 Considerando 146 del RGPD.

En este punto, cabe distinguir una doble esfera de responsabilidad[35]:

1º) La que se deriva del incumplimiento de las disposiciones del RGPD y sus normas de desarrollo, que conlleva automáticamente a indemnizar el daño.

2º) Demostrar la ausencia de responsabilidad en el hecho que haya causado el daño y que va junto con la adopción de las medidas técnicas y organizativas que impone el artículo 24 del RGPD. Se debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta[36]. La anterior afirmación hace que nos situemos en el supuesto del artículo 1902 del CC[37]. pero es un mero espejismo, puesto que el mismo Considerando debe demostrar, además, la conformidad de las actividades del tratamiento con el RGPD. Esto conlleva a invertir a carga de la prueba y demostrar que no se actuó con la debida diligencia.

Podemos encontrarnos una responsabilidad subjetiva, aquella que se genera con el incumplimiento de cualesquiera obligaciones civiles legales o contractuales y asimismo de los actos u omisiones ilícitos, siempre y cuando intervenga culpa o negligencia y se produzca un daño; y una responsabilidad objetiva, aquella que se genera con la mera producción de un determinado daño concreto, sin que la causa del mismo provenga de una determinada infracción del ordenamiento jurídico, o de culpa o negligencia (ya sea directa o indirecta) del imputado.

En cuanto a la posibilidad de imputación del deber de reparar el daño causado a terceros, hay que recordar que la concepción de la responsabilidad civil ha evolucionado desde una perspectiva meramente subjetiva (responsabilidad civil subjetiva) que vinculaba la obligación de resarcimiento a la existencia de una culpa o negligencia, a otra perspectiva objetiva (responsabilidad objetiva) que contempla el resarcimiento del daño, en sí mismo considerado[38]. El sistema introducido por el RGPD es un sistema de responsabilidad subjetiva. En este sentido, el párrafo tercero del artículo 82 del RGPD exonera de responsabilidad por los daños causados en la operación de tratamiento al responsable y encargado si se demuestra que no es responsable en modo alguno del hecho que haya causado los daños y perjuicios.

Respecto al objeto que se debe indemnizar, son indemnizables los daños y perjuicios materiales o inmateriales; es decir, se cubren tanto los daños físicos como morales, interpretándose el concepto de "daños y perjuicios" que dicta el

35 López Álvarez, L. F.: *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, Madrid, 2016, p. 176.

36 Considerando 74 del RGPD.

37 "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".

38 Páez Mañá, J.:"Responsabilidades derivadas del tratamiento nominativo de datos", *Informáticos europeos expertos*, s/f. Disponible en: http://www.iee.es/pages/bases/articulos/derint026.html

TJUE[39], por lo que se viene a buscar una reparación integral del daño sufrido. En cuanto a los daños morales, destacamos desde la perspectiva española, la reciente STS 261/2017, de 26 de abril en la que estipula los criterios para evaluar el daño moral por el incumplimiento de los requisitos de la legislación sobre protección de datos. En ella, el Tribunal considera como relevantes: 1) el tiempo de permanencia de los datos; 2) el alcance de la divulgación de los datos personales a terceros, y 3) la inacción del Responsable del tratamiento.

El RGPD regula la responsabilidad solidaria del responsable y el encargado, permitiendo al afectado demandar una indemnización total y efectiva tanto al responsable como al encargado, pudiendo repetir el sujeto que abonó la indemnización contra el resto de sujetos intervinientes por la parte que les correspondería pagar.

A todo esto, hay que diferenciar esta acción civil de la reclamación por vía administrativa, y que eventualmente, puede desencadenar en un recurso contencioso-administrativo, puesto que esta última vía no está destinada a la reparación económica del daño, sino en la imposición de sanciones respecto a las infracciones estipuladas tanto en la LOPD como en el RGPD. Aunque también cabe la posibilidad de dirimir determinadas infracciones a través de un proceso civil, como por ejemplo, la imposición al responsable de una limitación o prohibición al tratamiento, tal y como expresa la STS (Sala de lo Civil) de 15 de octubre de 2015.

Actualmente, existe una divergencia entre una reclamación realizada por la vía civil y la vía administrativa, siendo posible efectuar acciones indistintamente sin que una excluya a la otra derivada de las sentencias relacionadas con el derecho de supresión en la contradicción entre las SSTS 574/2016 y 210/2016, de diferentes jurisdicciones. Ambas sentencias discuten sobre quién es el responsable del tratamiento de los datos en el contexto del ejercicio del Derecho al olvido debido a las cuestiones sin contestar de la STJUE *Google Spain*, a lo que las salas dan respuestas contradictorias[40]:

1º) La STS 574/2016 estipula que el responsable del tratamiento de esos datos es quien gestiona técnica y administrativamente los medios para la indexación de la información, como es, en este caso, el motor de búsqueda. Y es la empresa matriz quien destina los medios para gestionarlo. La empresa filial no sería responsable si entre sus actividades principales no consta ninguna orientada a la indexación o almacenamiento de datos. No existiría tampoco corresponsabilidad al no existir unidad de negocio, ya que sus actividades están diferenciadas. Aunque

39 Considerando 146 del RGPD. En cuanto a la doctrina del TJUE, STJUE de 17 de marzo de 2016, *Liffers*, C-99/15.

40 De Miguel Asensio, P.A.: "La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google", *Diario La Ley*, 2016, núm. 8773º, pp. 1-6.

sean representantes de la empresa matriz, es una sociedad con personalidad jurídica diferenciada y con objetivos diferenciados. Esta consideración se reduce en la jurisdicción C-A, cuyo objeto pueden ser las reclamaciones de los afectados por el medio indexador, así como las resoluciones de la Agencia española de Protección de Datos (AEPD) en procedimientos de tutela de derechos en materia de protección de datos. Estas incidencias no pueden dirigirse contra la entidad filial, sino contra la matriz.

2º) Por el contrario, la STS 210/2016 considera que el responsable del tratamiento es en la mayoría de casos la filial; ya que, según el TJUE, interpretando la Directiva 95/46, no se exige para la aplicación del Derecho nacional que el tratamiento de los datos sea efectuado directamente por el propio establecimiento (la matriz) sino que se halle en las actividades de este. Considera que las actividades de la matriz y de la filial están ligadas; porque la filial, aun no dedicándose directamente a la indexación de la información, realiza actividades de promoción del medio de indexación (motor de búsqueda), además de ofrecerle los recursos económicos, sin importar la forma jurídica de la filial. Por lo tanto, la filial y la matriz son corresponsables del tratamiento de datos, y está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición.

En resumen, la STS 210/2016 explica que las sentencias no son contradictorias; ya que ambos casos están regidos por normas y principios totalmente diferentes, por lo que son complementarios en el siguiente sentido: para los casos respecto a procedimientos de tutela de derechos en materia de protección de datos, el responsable será la matriz extranjera. Para el ejercicio en un proceso civil de sus derechos; lo será también la filial nacional. La postura adoptada por el TS está fundamentada en el alto coste que supondría litigar contra una persona jurídica en el extranjero; aparte, está postura tiene el objetivo de favorecer a la parte débil (consumidor) en las transacciones internacionales de flujos de datos, permitiendo al afectado litigar en su lugar de residencia y sobre la base de su derecho nacional[41].

IV. ASPECTOS JURÍDICOS RELEVANTES DESDE EL PUNTO DE VISTA DEL DERECHO INTERNACIONAL PRIVADO.

1. Competencia judicial internacional.

El artículo 82 del RGPD remite al artículo 79.2 el lugar donde debe dirigirse el afectado derivado de un supuesto de responsabilidad del artículo 82. En este sentido, el artículo 82.6 nos remite al artículo 79.2, el cual dispone que las acciones

41 Idea recogida en la STJUE de de 25 de octubre de 2011 *eDate Advertising*, C-509/09 y C-161/10, y plasmada en el artículo 79.2 del RGPD.

dirigidas contra encargados o responsables deberán dirigirse ante los tribunales competentes del Estado miembro estos tengan un establecimiento.

Alternativamente, podrán ejercitarse tales acciones en los tribunales competentes del Estado miembro donde el reclamante tenga su domicilio, en concordancia con lo estipulado en el Considerando 145.

Como hemos visto, las acciones objeto del artículo 82 tienen un carácter "civil-mercantil", que a su vez, se encuadran dentro del ámbito de aplicación del artículo 1.1 del Reglamento (UE) 1215/2012 "Bruselas I Bis"[42], y cuya materia no está en los supuestos de exclusión del artículo 1.2.

Aunque se dé por hecha la adecuación de esta acción a los supuestos de responsabilidad extracontractual cuando exista un perjuicio relacionado con un tratamiento de datos ilícito según el artículo 82.6 del RGPD; pero es posible que ese tratamiento de datos se produzca en el contexto de un contrato, y según la jurisprudencia del TJUE, una acción de responsabilidad civil de naturaleza extracontractual deberá entenderse incluida en la materia contractual a los efectos del artículo 7 del Reglamento "Bruselas I Bis" si el comportamiento recriminado comporta un incumplimiento de las obligaciones contractuales cuando se estudie caso por caso el objeto del contrato[43]. Puesto que en un contrato se puede pactar el compromiso del cuidado de los datos personales en virtud de la legislación vigente; aunque la mayoría de los supuestos que nos encontraremos en la práctica serán de naturaleza extracontractual, o el objeto de los datos sea el tratamiento de datos.

Concretando más en el fuero del establecimiento del responsable, el artículo 79.2 permite demandar en el Estado miembro en el que el responsable o el encargado tengan un establecimiento. Como hemos estudiado en el apartado III del presente trabajo, debe tenerse un concepto flexible de "establecimiento", tal y como se indica en la STJUE *Weltimmo* debe extenderse "a cualquier actividad real y efectiva, aun mínima, ejercida mediante una instalación estable"[44]. Para ello, debe valorarse también el "grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión". En la STJUE *Amazon EU Sàri* considera posible considerar la existencia de un establecimiento en un Estado miembro cuando no exista ni una filial o sucursal, siendo necesario valorar el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en

42 DOUE L 351/1, de 20 de diciembre de 2012.

43 SSTJUE de 13 de marzo de 2014, *Brogsitter*, C-548/12, ECLI:EU:C:2014:148; 14 de julio de 2016, *Granarolo*, C-196/15, ECLI:EU:C:2016:559.

44 Apartados 31 de la STJUE *Weltimmo* y 75 de la STJUE *Amazon EU Sàrl*.

ese Estado[45], siendo posible considerar como "establecimiento" un representante de la sociedad si actúa con un grado de estabilidad suficiente[46].

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

El foro alternativo que prevé el RGPD permite a los afectados demandar en los tribunales del Estado donde tengan su residencia habitual. Para su consideración, será necesario que el afectado tenga un grado de permanencia que revele una situación de estabilidad[47].

La residencia habitual no es un concepto sinónimo al de "centro de intereses de la víctima" que promulga la STJUE *eDate Advertising*[48], que aunque en principio suele coincidir con la "residencia habitual"[49], podemos encontrarlo en otro Estado cuando exista un vínculo particularmente estrecho con ese otro Estado que resulte de otros indicios, como el ejercicio de una actividad profesional. La consideración de este foro de competencia no parece ser la más adecuada para determinar el tribunal que debe conocer de la pretensión, puesto que no exige que exista una vinculación entre el centro de intereses y el lugar donde efectivamente se produce el daño[50]. Por lo que se puede dar el caso, por ejemplo, de que una persona conocida en Islandia que resida en España sin que sea conocido, sufra una difamación en España utilizando para ello la lengua islandesa. En este supuesto, el nacional islandés podrá demandar ante los tribunales españoles, aunque no se haya producido efectivamente el daño[51]. En el caso de que el centro de intereses del afectado no se encuentre en el Estado de residencia, sino en el Estado con vínculos profesionales; volviendo al ejemplo anterior, supongamos que este nacional trabaja como tertuliano en una televisión española, y sufre una difamación que atenta

45 Apartados 76 y 77.

46 Apartado 30 de la STJUE *Weltimmo*.

47 STJUE de 22 de diciembre de 2010, *Mercredi,* C-497/10, ECLI:EU:C:2010:829.

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

49 Buonaiuti, F. M.: *"La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento 'Bruxelles i-bis'"*, *Cuadernos de Derecho Transnacional*, 2017, núm. 2, vol. 7, p. 8.

50 Orejudo Prieto De Los Mozos, P.: "La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia", *La Ley Unión Europea*, 2013, núm. 4°, p. 23.

51 Sentencia del Tribunal Federal Supremo alemán (*Bundesgerichtshof*) BGH NJW 2011, 2059: El demandante y el acusado eran de Rusia y habían asistido a la escuela secundaria juntos en Moscú. Habiendo terminado la escuela, el demandante llegó a residir habitualmente en Alemania, el demandado en los Estados Unidos. Se reunieron de nuevo en septiembre de 2006 para una reunión de clases en Moscú. Después de este acontecimiento, el demandado fijó una entrada en la páginawww.womanineurope.com, que fue funcionado por una compañía alemana. En este post, el demandado describió las condiciones de vida y el aspecto del demandante en términos bastante desfavorables. El post fue escrito en lengua rusa y en letras kirílicas. El BGH denegó la jurisdicción porque la publicación carecía de una conexión suficiente con Alemania.

contra sus derechos a la personalidad; pero tal publicación está escrita en islandés, por lo que no tiene efecto "real" en España[52]. En este sentido, creemos que hubiera sido mejor el criterio del Abogado General del asunto estudiado, el cual proponía como criterio para determinar la competencia –el cual rechazó seguir el TJUE– el "centro de gravedad del conflicto"[53]. Este criterio bebe del asimilado por el TJUE, que lo consagra como el lugar donde el afectado "desarrolla esencialmente su proyecto vital" (59 de las Conclusiones), pero que tiene en cuenta dos criterios más:

1º) El contenido de la información: esto es, si la información tiene interés en el territorio, y

2º) La conexión que pueda tener con el territorio, a la luz de indicios que derivan de la propia web, tales como el nombre de dominio de primer nivel, el idioma empleado, la publicidad que esta contenga o las palabras clave que se han suministrado a motores de búsqueda para identificar la página, o incluso de indicios exteriores, tales como los registros de la página.

La compatibilidad entre los foros del artículo 79.2 y los del Reglamento Bruselas I bis deriva del artículo 67 de este último Reglamento, al estipular que no prejuzgará la aplicación de las disposiciones contenidas en instrumentos particulares, como es el caso del artículo 79.2 del RGPD. En cuanto a los argumentos presentados por el RGPD, encontramos el Considerando 147 que afirma que las normas generales de competencia judicial del Reglamento Bruselas I bis "deben entenderse sin perjuicio de la aplicación de las normas específicas del RGPD". El Considerando 145 estipula que el demandante "deberá tener la opción" de ejercitar las acciones en los tribunales de los Estados miembros.

Observando lo anterior, revela que el RGPD pone a disposición de los afectados la posibilidad puedan utilizar los foros de competencia del artículo 79.2, en contra del inciso imperativo que recoge ese mismo párrafo. Por lo tanto, cabe

52 Orejudo Prieto De Los Mozos, P.: "La vulneración", cit, p. 23.

53 El criterio del "centro de gravedad del conflicto" no es un descubrimiento reciente. Los tribunales estadounidenses, por ejemplo, aplican un análisis de intereses al determinar la ley aplicable que también se denomina enfoque de "contactos más significativos", o "centro de gravedad" (p. ej. *Tooker v Lopez*, 24 N.Y.2d 569, 301 N.Y.S.2d 519, 249 N.E.2d 394 (1969), o *Neumeier v Kuehner*, 31 N.Y.2d 121, 335 (1972)). Esto incluye, junto con consideraciones tradicionales como el lugar de contratación, lugar de ejecución o lugar del hecho dañoso, la consideración de qué jurisdicción mantiene la relación más significativa o los contactos con el objeto de la controversia. Estos principios están recogidos en la *Section 145 of the Restatement (Second), Conflict of Laws, aprobado por el American Law Institute* en 1971. El artículo 145 (1) establece que "los derechos y responsabilidades de las partes con respecto a una cuestión extracontractual son determinados por la ley del Estado que, con respecto a esa cuestión, tenga la relación más significativa con el hecho y las partes [...]". El párrafo 2 identifica entonces los contactos que deben tenerse en cuenta en un caso de responsabilidad civil para determinar la ley aplicable a una cuestión como a) el lugar donde ocurrió la lesión, b) el lugar donde ocurrió la conducta que causó la lesión; c) el domicilio, residencia, etc., de las partes en la acción, y d) El lugar donde se centra la relación, si la hay, entre las partes, estos contactos deben evaluarse en función de su importancia relativa con respecto al asunto en cuestión. Oster (2012) p. 120.

afirmar, en principio, que los foros recogidos en el RGPD son complementarios a los recogidos por el Reglamento Bruselas I bis[54]:

1º) Sumisión expresa (artículo 25 Bruselas I bis). También se conoce como una prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional[55]. El artículo 25 dicta que "si las partes, con independencia de su domicilio, han acordado que un órgano jurisdiccional o los órganos jurisdiccionales de un Estado miembro sean competentes para conocer de cualquier litigio que haya surgido o que pueda surgir con ocasión de una determinada relación jurídica, tal órgano jurisdiccional o tales órganos jurisdiccionales serán competentes". El propio artículo pone como límite material a este mismo precepto la adecuación de la cláusula al derecho material de dicho Estado miembro, siendo esta una norma de conflicto uniforme para resolver todos estos casos e independiente del resto de un hipotético contrato. En cuanto a los límites formales, el acuerdo atributivo de competencia deberá celebrarse:

a) por escrito, o verbalmente con confirmación escrita, o

b) en una forma que se ajuste a los hábitos que las partes tengan establecido entre ellas. Permitiéndose en cualquiera de las formas anteriores materializarse mediante instrumentos electrónicos que permitan un registro duradero. En este sentido, podemos plantearnos sobre la compatibilidad de dicho artículo con el RGPD debido a la imperatividad de la que goza la legislación sobre protección de datos[56]. Esta situación puede ser comparable a la recogida en el artículo 19 del Reglamento Bruselas I bis relativo a las cláusulas en contratos de consumo. Por ello, entendemos que los acuerdos jurisdiccionales pueden perdurar siempre y cuando se respeten los requisitos de ambos reglamentos: 1) el requisito de pacto escrito del artículo 25 de Bruselas I bis, y 2) no eliminar los foros que proporciona el artículo 79.2 del RGPD. En resumen, tales acuerdos deben ampliar –¿más?– los foros disponibles para el afectado.

2º) Sumisión tácita (artículo 26 Bruselas I bis). La siguiente conducta procesal de las partes significará que estamos ante una sumisión tácita: cuando el demandante presenta una demanda ante el tribunal de un Estado miembro y la comparecencia del demandado ante ese tribunal no tiene por objeto impugnar su competencia judicial[57]; es decir, entra a discutir sobre el fondo del asunto. Aunque en el caso

54 Albrecht, J. P., y Jotzo, F.: *Das neue*., cit, pp. 127-128. Aunque se ha entendido que los fueros del RGPD plantean conflictos con las competencias exclusivas del Reglamento Bruselas I bis. *Cfr*. Brkan, M.: *"Data Protection and European Private International Law", Robert Schuman Centre for Advanced Studies*, 2015, Research Paper Nº RSCAS 2015/40, p. 23.

55 Ortega Giménez, A.: "Imagen y circulación internacional de datos", *Revista boliviana de Derecho*, 2013, núm. 15º, p. 138.

56 Hoeren, T. *et al.*: *Legal Aspects of Digital Preservation*, Edward Elgar Publishing, Cheltenham, 2013, p. 86.

57 Ortega Giménez, A.: "Imagen y circulación", cit, p. 139.

de que, por razón de la materia, o por existir un acuerdo de sumisión expresa anterior al litigio, el demandado puede declinar la competencia mediante una declinatoria, dependiente del derecho procesal de cada Estado miembro. En España, la declinatoria se regula en el artículo 39 de la LEC. Peligroso precedente encontramos en la STJUE *Ceská podnikatelská* v. *Michal Bilas*[58], la cual permite declararse competente el tribunal al que se ha sometido un litigio contraviniendo las reglas de competencia relativas a los contratos de seguros. La propia STJUE es consciente de la protección de la parte débil, pero esta se debió haber prevenido de la posibilidad de litigar según los foros de protección que establece el Reglamento Bruselas I bis, es por ello que el TJUE autoriza al juez no natural a asegurarse que tiene pleno conocimiento de las consecuencias de su aceptación de comparecer, pero no impone la obligación, puesto que esa previsión debe ser introducida en el Reglamento. Pero debemos entender que este artículo es incompatible con el artículo 1.2 del RGPD, puesto que el fin último de esta norma es proteger de manera eficaz el derecho fundamental a la protección de datos[59]. La sumisión tácita en materia de protección de datos tiene como parte débil a la persona física demandante, si no, no se crearían normas específicas sobre competencia judicial internacional específicas para tales sujetos. Permitiendo la sumisión tácita del artículo 26 del Reglamento Bruselas I bis, dejaría al afectado en una situación de debilidad ante la parte fuerte del litigio (normalmente una empresa), y atentaría contra el derecho fundamental a la protección de datos.

3º) Foro del domicilio del demandado (artículo 4 Bruselas I bis). Este foro de competencia en un clásico de los instrumentos normativos de atribución de competencia en virtud del principio *actor sequitur forum rei*. A falta de pacto expreso o tácito, el criterio atributivo de competencia es el del domicilio del demandado, que hace competentes a los tribunales del domicilio del demandado. El propio Reglamento Bruselas I bis nos da una definición de domicilio en el artículo 63, el cual se entenderá que una persona jurídica está domiciliada en el Estado en el que se encuentra: a) su sede estatutaria; b) su administración central, o c) su centro de actividad principal. En cuanto a la residencia habitual de una persona física, el artículo 62 nos remite a la ley interna del propio Estado[60], puesto que el Reglamento Bruselas I bis no nos aporta una noción autónoma del concepto. Aunque debemos resaltar la nula practicidad de este foro; puesto que genera muchos más perjuicios al propio demandante que al propio demandado, como el desconocimiento del idioma, los costes, y las diferentes normas procesales aplicables.

58 STJUE de 20 de mayo de 2010, *Ceská podnikatelská* v. *Michal Bilas,* C-111/09.

59 Considerando 1, y artículo 1.2 del RGPD.

60 En el caso de España, el artículo 40 CC señala que "para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual, y en su caso, el que determine la Ley de Enjuiciamiento Civil".

4º) Foro especial en materia de obligaciones extracontractuales. El "lugar donde se hubiere producido o pudiere producirse el hecho lesivo" (artículo 7.3 del Reglamento Bruselas I bis). Consiste en un foro especial regido por el principio de ubicuidad que en el caso de efectuar una acción por daños y perjuicios, el demandante tiene derecho a elegir entre los tribunales del lugar donde se produjo el hecho lesivo (ya sea donde se haya producido el hecho generador del daño o donde se padezca el daño) constituye la solución tradicional –y no siempre muy acertada– en esta materia[61]:

a) El principal problema que plantea el *forum locus delicti commissi* es el de determinar si por país en que se produce el daño debemos entender el del lugar en el que se localiza el hecho causal (p. ej. el Estado donde se recaban los datos).

b) O el del lugar en que se verifica el resultado dañoso (p.ej. el Estado donde se acceden a los datos).

Estas situaciones dificultan la determinación del lugar donde se ha producido el hecho dañoso, que se manifiesta en dos preguntas:

1º) Cuál es el lugar donde tienen lugar el evento generador del daño? En el Estado donde se ha difundido o tratado ilícitamente los datos.

2º) Cuál es el lugar donde se concreta el resultado lesivo? Aquí no hay una respuesta concreta, sino una multitud de posibilidades:

a) El país desde donde se han introducido los datos;

b) en el marco de Internet, el lugar donde está ubicado el servidor que los alberga;

c) El país desde donde se puede tener acceso a los datos, o

d) El país donde reside el titular del derecho infringido, que es, en definitiva, donde se ha producido el hecho dañoso.

e) El país donde radique el fichero de datos.

Como hemos observado, este artículo se caracteriza por una gran "dispersión competencial" que ataca directamente a la protección del titular del derecho a la protección de datos. A esclarecer la competencia judicial relacionada con litigios derivados de ilícitos contra los derechos de la personalidad en materia de competencia judicial contribuyó la STJUE e*Date Advertising,* derivada de la

61 Ortega Giménez, A.:"Imagen y circulación", cit, p. 142.

doctrina creada por la STJCE *Fiona Shevill*[62] que interpretaba el antiguo artículo 5.3 del Reglamento Bruselas I. La STJCE *Fiona Shevill* permitía –y sigue permitiendo– a la víctima de la vulneración del derecho a la intimidad por la difamación de datos personales publicados y accesibles en varios Estados miembros ejercer una acción resarcitoria contra el promotor de la acción que causa el hecho dañoso ante los tribunales del domicilio de tal persona para reclamar una indemnización íntegra, o bien demandar ante los tribunales de cada Estado miembro el el que la publicación sea difundida, y en el que la víctima alegue haber sufrido un ataque contra su reputación. La STJUE *eDate Advertising* viene a reducir esta "dispersión competencial" permitiendo al afectado que alegue un daño o perjuicio en un Estado miembro exija una indemnización integral por todo el daño sufrido ante los tribunales del Estado promotor de la acción, y el Estado donde la víctima tenga su centro de intereses[63].

Pero la coexistencia de los artículos 7.2 de Bruselas I bis, y el 79.2 del RGPD se encuentra en entredicho. Mientras que la jurisdicción general del Reglamento Bruselas I bis es "neutral", la jurisdicción específica al menos indica que ya hay algún tipo de conexión significativa entre el foro y la cuestión jurídica a decidir[64]. Podemos observarlo en los foros especiales del artículo 79.2 del RGPD en los que se permite demandar 1) ante los tribunales del Estado en el que esté domiciliado algún establecimiento tanto del responsable como del encargado, o 2) ante los tribunales del Estado de la residencia habitual del afectado por un supuesto tratamiento ilícito de los datos personales que genera una responsabilidad extracontractual. Estos foros estipulados por el RGPD están redactados para adecuarse al supuesto concreto. En cambio, los foros del Reglamento Bruselas I bis tienen como objeto cubrir supuestos generales (p. ej. accidentes de circulación). En otras palabras, los principios que subyacen de ambos reglamentos son diferentes y excluyentes entre sí, y uno de debe imponer su justicia sobre el otro[65], por lo que el artículo 79.2 del RGPD debe prevalecer sobre el artículo 7.2 del Reglamento Bruselas I bis[66].

Vista esta disposición de foros otorgados por diferentes instrumentos normativos, hubiese sido más apropiado regular las reglas de competencia judicial internacional en el Reglamento Bruselas I bis en vez del propio RGPD para evitar

62 STJCE de 7 de marzo de 1995, C-68/03, *Ixora Trading Inc; Chequepoint SARL, Chequepoint International Ld. C Press Alliance S*, ECLI:EU:C:1995:61.

63 Véase también la STJUE de 3 de octubre de 2013, *Pickney*, C-170/12, ECLI:EU:C:2013:635 (párr. 36), que siguiendo la doctrina de la STJUE *eData*, permite también demandar en el Estado miembro donde el contenido sea accesible.

64 Von Hein, J.: *"Social Media and the Protection of Privacy", European Data Science Conference*, 2016, p. 24.

65 Revolidis, I.: *"Judicial jurisdiction over Internet privacy violations and the GDPR: a case of "privacy tourism"?", Masaryk University Journal of Law and Technology*, 2017, núm. 1, vol. 11, p. 23.

66 Carrascosa González, J., y Calvo Caravaca, A-L.: *Derecho internacional privado*, Vol. II Comares, Granada, 17ª ed., 2017, pp. 1528.

así está complicada compatibilidad de foros disponibles establecida tanto por el Reglamento Bruselas I bis como por el RGPD, y los problemas de litispendencia y conexidad del artículo 81 del RGPD para, a su vez, mantener coherencia entre ambos Reglamentos[67].

Además, debemos destacar que podemos encontrarnos que tal perjuicio se materialice en el marco de una relación contractual, por lo que debemos atenernos a los foros concretos en materia contractual del Reglamento Bruselas I bis[68], y que actúan con una doble función: 1) por un lado, establecer un foro de protección especial para la parte que ha sufrido el daño y perjuicio, que en casos en los que una parte de una relación contractual es la parte débil como en los contratos de seguro o celebrados por los consumidores; 2) y por el otro, suplir la ausencia de unos foros especiales para los responsables del tratamiento cuando estos pretendan ejercitar alguna acción contra los afectados. Y es especialmente destacable la relación contractual entre consumidores, porque para servicios como Facebook, o empresas de servicios similares, se firma un contrato de adhesión dirigido principalmente a consumidores, y que es de relevancia la recentísima STJUE *Schrems II*[69], la cual se resuelve la vertiente civil del caso original. El caso resuelve un conflicto de competencia judicial internacional entre Schrems y Facebook Ireland, por el cual el demandante instó acciones judiciales contra Facebook en Viena utilizando para ello el foro para consumidores del Reglamento (UE) 44/2001, a lo que Facebook respondió con una excepción de competencia internacional, puesto que entendía que el uso que realizaba el demandante respecto a Facebook no correspondía con el de un consumidor, sino con el de un profesional. La STJUE resuelve que en este tipo de contratos realizados con empresas dedicadas a las redes sociales, la finalidad para la cual se realiza el contrato puede variar a lo largo del tiempo; es por ellos que hay que utilizar un término de contrato "dinámico" para adaptar el contrato a la finalidad y uso que el usuario hace de él. Hay que observar la evolución del uso no profesional del servicio, a un uso "esencialmente profesional". Por lo tanto, el mero hecho de compatibilizar en una red social tanto actividades privadas como comerciales, no supone que se le deje de aplicar la protección hacia los consumidores que proporciona el Derecho europeo y, por lo tanto, se pueden ejercer los foros de protección de las normas relativas a la competencia judicial a favor de los consumidores.

67 Brkan, M.: *"Data protection and European private international law: observing a bull in a China shop"*, *International Data Privacy Law*, 2015, núm. 4°, vol. 5, p. 275.

68 1) Competencia especial en materia contractual del artículo 7.1); 2) foros especiales de protección en materia de seguros de los artículos 10-16; 3) foros especiales de protección en materia de contratos celebrados por los consumidores de los artículos 17-19, 3) y foros especiales de protección en materia de contratos individuales de trabajo de los artículos 20-23.

69 STJUE de 25 de enero de 2018, *Schrems vs. Facebook*, C-498/16, ECLI:EU:C:2018:37.

Respecto a la posibilidad de ejercer a favor de otros, acciones judiciales de consumidores residentes en otro Estado miembro, o en terceros Estados (en el presente caso, la India) no puede llevarse a cabo. Aunque sea requisito indispensable la celebración de un contrato entre el consumidor y el profesional demandado[70], el cesionario de los derechos solo puede ejercer los derechos que le son inherentes a su relación con el profesional demandante, no quedando sometidos a la competencia del tribunal los consumidores los cedentes de los derechos.

2. Determinación de la Ley aplicable a la controversia.

La primacía de la legislación de protección de datos se manifiesta en una limitada autonomía de la ley aplicable en una cláusula contractual, la cual siempre deberá atenerse a los criterios del RGPD en los casos de obligaciones contractuales, cuyas cláusulas pueden estar sujetas a las leyes de otro Estado según el Reglamento (CE) 594/2008 "Roma I"[71]. Podemos tomar como ejemplo las cláusulas de términos y condiciones de Facebook (ES), en la que su artículo 15.2 estipula que cualquier litigio deberá dirimirse aplicando las leyes del Estado de California. En principio, puede ser aplicable tal cláusula en virtud del artículo 3.1, pero deberá cumplir lo estipulado en el propio artículo 6.2 relativo a los contratos de consumo, en el que obliga a estipular en el acuerdo que las disposiciones legales que protegen al consumidor continúan siendo aplicables al ser este la parte débil de la relación contractual. A falta de esta disposición en el contrato, la cláusula se considera abusiva[72].

Puede llegar a entenderse que la imperatividad de la legislación sobre protección de datos no afecta solo a las obligaciones propias que proporciona el RGPD, sino también puede afectar a la ley aplicable a la controversia, que deberá coincidir con la que se determine por el RGPD mediante el artículo 3 de esta norma, puesto que se puede pensar que realizar un contrato entre usuario-proveedor de servicios puede escaparse de la aplicación del RGPD y ventilarse por el Reglamento Roma I; pero al final, el resultado será el mismo: 1) el Reglamento Roma I permite que la ley aplicable sea la ley del Estado de residencia habitual del consumidor, a) siempre que ejerza sus actividades comerciales o profesionales en el país donde el consumidor tenga su residencia habitual, o b) por cualquier medio dirija estas actividades a ese país o a distintos países, incluido ese país, siempre y cuando el contrato tenga que ver con dichas actividades. Como se ha visto anteriormente, se permite el acuerdo de la ley aplicable, pero siempre especificando que nunca perderá el usuario el derecho a aplicar la ley de su Estado de residencia, y 2)

70 STJUE de 28 de enero de 2015, *Kolassa*, C-375/13, EU:C:2015:37.

71 DOCE L 177/6, de 4 de julio de 2008.

72 En este sentido se pronuncia la STJUE *Amazon EU Sàrl* (pár. 71).

no podemos entender al artículo 3 del RGPD como una norma de Derecho internacional privado de la misma manera que el artículo 4 de la Directiva 46/95, puesto que el fin del RGPD es determinar la sujeción del tratamiento al propio reglamento, sin entrar en determinar el Derecho nacional como hacía la Directiva.

En la práctica, parece todavía existir cierta confusión en cuanto a cuál es la base jurídica para determinar la legislación aplicable en el ámbito de la protección de datos[73]. Mientras que el TJUE en el caso Google Spain no se refirió a los Reglamentos de Roma I o II ni a la cuestión de la relación entre estos reglamentos y el artículo 4 de la Directiva sobre protección de datos, la decisión del tribunal administrativo del Estado alemán Schleswig-Holstein[74] en un supuesto de determinación de la ley de protección de datos aplicable al contrato de términos y servicios de Facebook, determinó que era de aplicación el Derecho irlandés (Estado en el que está establecida la filial europea encargada del tratamiento de datos), y no el alemán (Estado en el que está establecida la filial encargada de los servicios publicitarios) por considerar las disposiciones sobre protección de datos son imperativas y obligatorias en virtud del artículo 9 del Reglamento Roma I.

Pero hay supuestos de responsabilidad extracontractual –como es el caso de las transferencias internacionales de datos–[75] que plantean importantes problemas en cuanto al Derecho aplicable. La ley que resuelve esta controversia es el Reglamento (CE) 864/2007 "Roma II"[76].

El Reglamento "Roma II" es un texto legal con carácter universal[77]; es decir, la ley designada por el Reglamento se aplica aunque no sea de un Estado miembro, la cual permite una mayor y mejor unificación del mercado interior[78]; pero que excluye de su aplicación en su artículo 1.2.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", por tanto, las acciones extracontractuales relativas a los daños y perjuicios sufridos por un interesado como consecuencia

73 Brkan, M.: "Data Protection", pp. 26-27.

74 *VG Schleswig-Holstein*, Beschluss vom 14.02.2013, Az. 8 B 60/12.

75 Se ha discutido sobre la posibilidad de admitir como transmisiones internacionales de datos personales los supuestos de acceso internacional; es decir, las meras publicaciones de datos personales en páginas web. Históricamente el TJUE ha rechazado esta posibilidad mediante la STJUE de 6 de noviembre de 2003, *Bodil Lindqvist*, C-101/01, pero el nuevo el nuevo artículo 49.1.g), que considera válida la transferencia cuando se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar la información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés, pero solo en la medida en el que se cumplan las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta. Es decir, bastaría con la puesta a disposición de los datos. Pinar Mañas, J. L.: "Transferencias de datos personales a terceros países u organizaciones internacionales", en AA.VV. (Dir. por J. L. Pinar Mañas), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2017, p. 433.

76 DOCE L 199/40, de 31 de julio de 2007.

77 Artículo 3.

78 Ortega Giménez, A.: *Transferencias internacionales de datos de carácter personal ilícitas*, Civitas, Madrid, 2017 p. 138.

del tratamiento de sus datos personales por un responsable o encargado están excluidas de la norma, exclusión muy criticada por la doctrina[79]. Debemos destacar que actualmente existe una propuesta de reforma del Reglamento Roma II en el que pretende incluir estos supuestos motivada por la STJUE *eDate Advertising* tendente a unificar la norma de conflicto y desplazar a la legislación interna[80].

Esto se traduce en una serie de consecuencias positivas[81]:

1º) Las partes en un litigio privado internacional derivado de la vulneración del derecho fundamental a la protección de datos no tendrán que conocer las normas de conflicto de los Estados miembros de la UE y su aplicación jurisprudencial sino que puedan acudir a un régimen único.

2º) Reducción de costes para la persona perjudicada.

3º) Seguridad jurídica. Se eliminarían un sistema que interesados utilicen la norma de conflicto para buscar la ley que les resulte más favorable (*lex shopping*).

4º) Se evitarían las desigualdades entre el causante del daño y la persona perjudicada.

La reforma del Reglamento Roma II incluye un nuevo artículo 5 bis en el que introduce dos nuevos supuestos: 1) 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", o 2) "la ley del país de residencia habitual del demandado, en su defecto, si el demandado no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país"[82].

El supuesto del primer inciso adopta los criterios de la *lex loci damni* (la ley del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del daño) o *lex loci delicti commissi* (la ley del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del hecho lesivo).

79 Dickinson, A.: *The Rome II Regulation. The Law Applicable to Non-Contractual Obligations*, OUP, Oxford, 2008. p. 240; Sancho Villa, D.: *Negocios internacionales de tratamiento de datos personales*, Civitas, Madrid, 2010, pp. 97-98; Ortega Giménez, A.: "La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español", *Diario La Ley*, 2015, núm. 8661º, p. 8; Brkan, M.: "Data protection", cit, pp. 27-28; De Miguel Asensio, P.A.: "Competencia", cit, pp. 41-42.

80 P7_TA-PROV(2012)0200.

81 De Miguel Asensio, P.A.: "Competencia", cit, p. 66.

82 Una redacción similar la encontramos en el artículo 99 § 2. 1º del *Code de droit international privé* belga [C – 2004/09511] en los supuestos de daños contra los derechos de la personalidad, salvo que en este artículo permite la elección entre las dos opciones de la ley aplicable si el demandado no podía predecir que el daño se produciría en ese Estado.

El segundo supuesto resulta más confuso, en el sentido de que, más que proteger al posible afectado, favorece a la parte fuerte del litigio[83]. Permite aplicar la ley del país de residencia del demandado cuando a) resulte imposible determinar el elemento o los elementos más significativos del daño o perjuicio (elemento objetivo); y b) que el causante del daño no hubiera podido haber previsto razonablemente consecuencias importantes de su acto en dicho país (elemento subjetivo).

La adición de este doble criterio a la hora de la determinación de la ley aplicable puede llegar a prejuzgar el caso en una fase muy temprana del proceso, además de favorecer al presunto responsable del daño con la opción de litigar con la ley del país de residencia.

La inclusión del futuro artículo 5 bis (que esperemos que se aplique con una debida reforma del texto), debe ponerse en relación con el artículo 14 del Reglamento Roma II, que ofrece al perjudicado y al causante del daño la posibilidad de poder elegir la ley aplicable, en virtud del principio de autonomía de la voluntad. Aunque en la práctica es difícilmente aplicable; puesto que el acuerdo debe hacerse con posterioridad al hecho generador del daño, en esos momentos es complicado que ambas partes se pongan de acuerdo. Pero la consecuencia de la no regulación conlleva a la aplicación de normas autónomas como el artículo 10.9 del Código Civil, que hace que apliquemos la ley del lugar donde se ha cometido el hecho (*lex loci delicti commissi*)[84]. La *lex loci delicti commissi* es una conexión de carácter territorial cuya aplicación en los supuestos de ilícitos en los elementos constitutivos (acto y resultado) se encontraban en un mismo Estado[85]. Pero en este ámbito, la precisión del lugar en el que se produce el daño puede resultar controvertida en situaciones en las que las consecuencias lesivas del hecho dañoso no son de carácter material, y esta norma no precisa cuál es el lugar del daño en las situaciones en las que el hecho causal y el resultado lesivo se producen en distintos países[86].

El artículo 10.9 del CC nos otorga dos opciones para determinar la ley aplicable: 1) la aplicación de la *lex loci actus* (Ley del Estado en el que se produce el hecho del que deriva la responsabilidad); o 2) la aplicación de la *lex loci damni* (aplicación de la ley del lugar donde se materializa el daño para las víctimas). Esta doble

83 Ortega Giménez, A.: "La (des)protección", cit, p. 8.

84 "Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven".

85 Vinaixa Miquel, M.: *La responsabilidad civil por contaminación transfronteriza derivada de residuos*, USC, Santiago, 2006, p. 147.

86 De Miguel Asensio, P.A.: *Derecho privado de* Internet, Civitas, Madrid, 8ª ed., 2015, p. 201.

interpretación –o ambigüedad– puede ser solventada mediante la separación de ambos criterios en la Ley, como hacen algunos países de nuestro entorno[87].

En la primera opción (*lex loci actus*), el mayor problema que encontramos es determinar cuál es el Estado en el que se ha realizado el hecho dañoso, puesto que el hecho ilícito deriva de una cadena de ilícitos que se suelen desarrollar en otros Estados, el cual debemos verificar el Estado donde refleja sus efectos lesivos; 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[8889]. Entonces, para poder aplicar la legislación española, a) el responsable del fichero tuviera su domicilio fuera de la UE y, b) el tratamiento de datos se hubiera realizado en España.

Respecto a la segunda opción (*lex loci damni*), y en concreto en los supuestos de mero acceso, debe rechazarse que cualquier lugar de recepción de los contenidos o la información transmitidos por Internet sea por esa simple circunstancia lugar del daño debido a 1) que muchas veces ese acto no genera un daño "real" al titular, y 2) la aplicación de la ley de cada uno de los múltiples lugares de manifestación del daño puede conducir a una excesiva fragmentación normativa[90]. Es por ello que se afirma que el lugar donde se manifiesta la consecuencia directa para la víctima, se corresponde con el lugar de su residencia habitual como 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; como ya comentamos a raíz de la STJUE e*Date Advertising*, no solo se materializa el perjuicio en el Estado de residencia habitual, también en aquel Estado en el que existan un vínculo estrecho con ese otro Estado.

Debido a los ya resaltados problemas, conviene que ahondemos en una crítica al precepto[91]:

87 P. ej. el artículo 62.1 de la LEGGE 31 maggio 1995, n. 218. *Riforma del sistema italiano di diritto internazionale privato*, que estipula que las obligaciones extracontractuales se regirán por la ley del Estado en el que se haya producido el evento (*lex loci actus*); aunque el segundo inciso habilita al demandante a solicitar la aplicación de la ley del Estado en el que se haya producido el daño (*lex loci damni*). Otros países con este mismo sistema son: Alemania (artículo 40 del *Einführungsgesetz zum Bürgerlichen Gesetzbuche*); Portugal (artículo 45 del *Código Civil*, que permite la aplicación de la ley del lugar donde se hay producido el daño, siempre y cuando: a) el autor del daño haya podido prever que su acto podría causar daños en ese estado; y, b) que la ley del Estado donde transcurre la actividad principal causante del daño no considere responsable al autor de ese daño.); Países Bajos (artículo 3 de la *wet conflictenrecht onrechtmatige daad*, permitiendo aplicar la ley de un Estado en el que se manifiesten las consecuencias de un acto ilícito distinto al del que se hubiese producido el acto, siempre que el demando no previese razonablemente la acción).

88 Ortega Giménez, A.: *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, AEPD, Madrid, 2015, p. 143.

89 Respecto al caso BGH NJW 2011, 2059 comentado anteriormente, el *Bundesgerichtshof* señaló explícitamente que la aceptación de la jurisdicción también conduciría a la aplicación del derecho alemán (artículo 40.1 del EGBGB).

90 De Miguel Asensio, P.A.: *Derecho privado*., cit, p. 203.

91 Ortega Giménez, A.: "La (des)protección", cit, p. 7.

1º) 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.

2º) Adolece de una rigidez relevante, puesto que solo 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), con la ambigüedad que ello supone.

3º) La neutralidad de la norma. 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.

A todo esto, debemos resaltar las precisiones del RGPD, ya que la tendencia que genera el artículo 79.2 del RGPD invita a aplicar aplicar "la ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado"[92]. Su postura se basa en el objetivo que tiene la norma de proteger al afectado, el cual una de las maneras de plasmarlo es la aplicación de un Derecho que sea familiar al afectado que se correspondan con el del Estado de la residencia habitual (o del centro de intereses del afectado); y que entendemos que esta deba ser la opción que mejor puede llegar a proteger los intereses del afectado en función del principio de *favor laesi*[93]. Y en la práctica podemos prever que el demandante inicie las acciones en o bien el el Estado de la residencia habitual, o bien en el centro de intereses del afectado, se aplicará la ley del Estado que asumió la competencia (*lex fori*), la cual conlleva una serie de beneficios[94] tales como 1) la reducción del tiempo y los costes de los litigios; 2) la mejora de la calidad de los juicios, y 3) Tenencia en cuenta las preocupaciones de política pública del foro, porque los derechos de la personalidad, la privacidad, la protección de datos, etc., están arraigados en los valores constitucionales. Aunque el principal problema lo encontraríamos en el arraigo del *forum shopping,* siempre y cuando el Reglamento Roma II no cubra los derechos de la personalidad. El principal problema lo encontraríamos en el arraigo del *forum shopping,* siempre y cuando el Reglamento Roma II no cubra los derechos de la personalidad.

V. CONCLUSIÓN Y SUPUESTO PRÁCTICO.

El legislador ha observado los problemas de aplicación de la ley de protección de datos a los supuestos actuales planteados con la Directiva 95/46, la cual se

92 De Miguel Asensio, P.A.: "Competencia", cit, p. 42.

93 Ortega Giménez, A.: "Propuestas ante un futuro incierto para la protección en la unión europea del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: ¿unificación de la norma de conflicto vs. Armonización a través de unos principios comunes?", *Revista Aranzadi Unión Europea*, 2016, núm. 10, p. 6.

94 Von Hein, J.: "Social Media", cit, p. 23.

veía superada por el avance de nuevas tendencias tecnologías como el *Big Data*, el *Cloud Computing*, o el *Internet of Things*; cuyas tendencias están marcadas por la deslocalización del tratamiento de los datos. El nuevo artículo 3 del RGPD trata este fenómeno con la obligatoriedad de la aplicación de la legislación europea cuando los datos tratados en terceros países involucren a residentes de la Unión, además de contemplar un supuesto específico dedicado al *Big Data* en el artículo 3.2 b), el cual no entendemos la exclusión que realiza la doctrina en cuanto a la aplicación de este supuesto a los productos o servicios diferentes a los servicios de Internet. Con este nuevo artículo, 1) se asegura que los datos personales de los ciudadanos de la Unión estén protegidos incluso más allá de del territorio, 2) y se protegen los tratamientos de datos que controlen el comportamiento, objeto del *Big Data*.

La estipulación de un régimen específico del derecho a la indemnización por daños y perjuicios supone un gran avance para la protección del individuo. El nuevo régimen supera con creces la regulación contenida en la Directiva 95/46, y unificando al máximo las disposiciones que deben cumplir los Estados miembros. La adición de indemnizar los daños inmateriales supone la culminación de una doctrina jurisprudencial europea que ya venía reconociendo los daños morales como un elemento más de la indemnización. A esto, hay que sumarle los nuevos criterios otorgados por nuestro Tribunal Supremo, que añaden seguridad jurídica a la cuestión.

El sistema de Derecho internacional privado que instaura el RGPD cumple "a medias" la función protectora que debe tener el titular del Derecho fundamental a la protección de datos. El nuevo RGPD ha demostrado tener una función clara: facilitar al afectado poder efectuar sus derechos en el Estado miembro que desee, en especial, en el propio Estado de residencia del afectado. La compatibilidad relativa de foros con el Reglamento Bruselas I bis a la luz de su interpretación conjunta con el RGPD permite suplir la falta de foros especiales para el responsable, aparte de añadir una mayor disposición de foros para el afectado. Aunque esta dualidad normativa crea un efecto complejo de interpretación entre ambos textos, cuyo problema pudo haberse resuelto trasladando las cuestiones relacionadas con la competencia judicial internacional al Reglamento Bruselas I bis. Debemos lamentar la inexistencia de avances en cuanto a la determinación de la ley aplicable en los casos de ejercicio de la acción del artículo 82 del RGPD, la cual nos sigue llevando a una aplicación heterogénea de las normas autónomas de los diferentes Estados miembros de la Unión Europea que, en nuestro caso, se sigue rigiendo por la *lex loci delicti commissi*. Es por ello que se debe avanzar en una norma de conflicto unificada a través de la modificación del Reglamento "Roma II" que estipule una norma de conflicto que favorezca a la parte débil del litigio en función

del *favor laesi*, como es la persona perjudicada, como la ley del Estado del Estado de residencia habitual del afectado o del "centro de intereses de la víctima".

Supuesto práctico

1. Competencia judicial internacional

El afectado, residente en España, busca emprender la acción de responsabilidad del artículo 82 del RGPD por una difamación de datos personales que ha alcanzado a los países centroeuropeos ante el responsable del tratamiento, con domicilio en Polonia, y con establecimientos en Reino Unido, Irlanda, Bélgica, Austria, y Francia. Partiendo de este supuesto, pueden darse varias situaciones:

Que las partes, ya habiendo nacido el conflicto, acuerdan someter el litigio ante los tribunales de un Estado miembro concreto (Sumisión expresa. Art. 25 Bruselas I bis).

Que el afectado demande en primer lugar en cualquier Estado miembro, y que el responsable decida discutir sobre el fondo del asunto (Sumisión Tácita. Art. 26 Bruselas I bis).

Que decida demandar en en los Estados en los que el responsable posea un establecimiento (foro del establecimiento del responsable. Art. 79.3 RGPD).

Que demande en su Estado de residencia (Foro de la residencia habitual del demandante. Art. 79.2 RGPD).

En este caso, no cabe invocar el foro del artículo 7.3 del Reglamento Bruselas I bis sobre responsabilidad extracontractual, puesto que dicho foro decae por el principio de especialidad del RGPD.

2. Ley aplicable

Suponiendo que haya decidido demandar en España, puesto que no existe una norma ni institucional ni convencional, será de aplicación el artículo 10.9 del CC, al no poder aplicarse el Reglamento Roma II. 1) Si entendemos la *lex loci delicti commissi* como «la ley del lugar donde se materializa el daño para las víctimas» (*lex loci damni*); 2) nos atenemos a la tendencia generada por el RGPD y por la jurisprudencia del TJUE de aplicar la "ley del lugar donde sufren el daño o lesión los bienes o derechos del perjudicado", y vemos que el afectado no tiene intereses más allá de España, se aplicaría el Derecho sustantivo español a la controversia.

BIBLIOGRAFÍA

Albrecht, J. P., y Jotzo, F.: *Das neue Datenschutzrecht der EU*, Nomos, Baden-Baden, 2017.

Albrecht, J. P.: "How the GDPR Will Change the World", *European Data Protection Law Review*, 2016, núm. 3º, vol. 2.

Álvarez Hernando, J., y Cazurro Barahona, V.: *Practicum Protección de datos 2016*, Aranzadi, Cizur Menor, 2017.

Brkan, M.:

- "Data protection and conflict-of-laws: a challenging relationship", *European Data Protection Law Review*, 2016, núm. 3º, vol 2.

- "Data Protection and European Private International Law", *Robert Schuman Centre for Advanced Studies,* 2015, Research Paper Nº RSCAS 2015/40.

- "Data protection and European private international law: observing a bull in a China shop", *International Data Privacy Law*, 2015, núm. 4º, vol. 5.

Buonaiuti, F. M.: "La disciplina della giurisdizione nel Regolamento (UE) n. 2016/679 concernente il trattamento dei dati personali e il suo coordinamento con la disciplina contenuta nel regolamento 'Bruxelles i-bis'", *Cuadernos de Derecho Transnacional*, 2017, núm. 2, vol. 7.

Bu-Pasha, S.: "Cross-border issues under EU data protection lawwith regards to personal data protection", *Information & Communications Technology Law*, 2017, vol. 0.

Carrascosa González, J., y Calvo Caravaca, A. L.:

- *Derecho internacional privado*, Vol. II Comares, Granada, 16ª ed, 2016.

- *Derecho internacional privado*, Vol. II Comares, Granada, 17ª ed., 2017.

De Miguel Asensio, P. A.:

- "Aspectos internacionales de la protección de datos: las sentencias *Schrems* y *Weltimmo* del Tribunal de Justicia", *La Ley Unión Europea*, 2015, núm. 31º.

- "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea", *Revista Española de Derecho Internacional*, 2015, núm. 1º, vol. 69, 2017.

- *Derecho privado de* internet, Civitas, Madrid, 4ª ed., 2015.

- "La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google", *Diario La Ley*, 2016, núm. 8773º.

Dickinson, A.: *The Rome II Regulation. The Law Applicable to Non-Contractual Obligations,* OUP, Oxford, 2008.

Erdozáin López, J. C.: "La protección de los datos de carácter personal en las telecomunicaciones", *Revista Doctrinal Aranzadi Civil-Mercantil*, 2007, núm. 1º.

Ernst, S.: "Allgemeine Bestimmungen", en AA. VV. (Coord. Por B. Paal, y D. Pauly), *Datenschutz-Grundverordnung*, Beck, Munich C.H. 2017.

Geist, M.: "Is There a There There? Toward Greater Certainty for Internet Jurisdiction", 2001, *Berkeley Technology Law Journal*, núm. 3º, vol. 16.

Hoeren, T. *et al.*: *Legal Aspects of Digital Preservation*, Edward Elgar Publishing, Cheltenham, 2013.

Hijmans, H.: *The European Union as Guardian of Internet Privacy: The Story of Artículo 16 TFEU*, Springer, Bruselas, 2016.

Jiménez-Benítez: W. G.: "Rules for offline and online in determining internet jurisdiction. Global overview and colombian cases", *Reviesta Colombiana de Derecho Internacional*, 2015, núm. 26º.

Kuner, C.:

- "The European Union and the Search for an International Data Protection Framework", *Groningen Journal of International Law*, 2015, vol. 2, ed. 1.

- "The Internet and the Global Reach of EU Law", *Legal studies research. Paper series*, 2017, núm. 24.

López Álvarez, L. F.: *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, Madrid, 2016.

Moerel, L.: "The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *International Data Privacy Law*, 2011, núm 1º, vol. 1.

Orejudo Prieto De Los Mozos, P.: "La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia", *La Ley Unión Europea*, 2013, núm. 4º.

Ortega Giménez, A.:

- "Imagen y circulación internacional de datos", *Revista boliviana de Derecho*, 2013, núm. 15º.

- "La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español", *Diario La Ley,* 2015, núm. 8661º.

- *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, AEPD, Madrid, 2015.

- "Propuestas ante un futuro incierto para la protección en la unión europea del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: ¿unificación de la norma de conflicto vs. Armonización a través de unos principios comunes?", *Revista Aranzadi Unión Europea*, 2016, núm. 10.

- *Transferencias internacionales de datos de carácter personal ilícitas*, Civitas, Madrid, 2017.

Oster, J.:

- *European and International Media Law*, Cambridge, Cambridge University Press, 2017.

- "Rethinking Shevill. Conceptualising the EU private international law of Internet torts against personality rights", *International Review of Law, Computers & Technology*, 2012, núm. 2-3º, vol. 26.

Páez Mañá, J.: "Responsabilidades derivadas del tratamiento nominativo de datos", *Informáticos europeos expertos*, s/f. Disponible en: http://www.iee.es/pages/bases/articulos/derint026.html

Pirodi, P. "profili internacional-privatistici della responsabilità delgestore di un motore di ricerca per li trattamento dei dati personali", en AA. VV. (dirigido por

Resta, G., y Zeno-Zencovich, V.), *Il Dirito all' oblio su internet dopo la sentenza Google Spain*, Roma TrE-Press, Roma, 2015.

Pinar Mañas, J. L.: "Transferencias de datos personales a terceros países u organizaciones internacionales", en AA. VV. (dir. por J. L. Pinar Mañas), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2017.

Recio Gayo, M.: "Acerca de la evolución de la figura del encargado del tratamiento", *Revista de Privacidad y Derecho Digital,* 2015, nº 0.

Revolidis, I.: "Judicial jurisdiction over internet privacy violations and the GDPR: a case of "privacy tourism"?", *Masaryk University Journal of Law and Technology*, 2017, núm. 1, vol. 11.

Sancho Villa, D.: *Negocios internacionales de tratamiento de datos personales*, Civitas, Madrid, 2010.

Schiedermair, S.: "The new General Data Protection Regulation of the European Union-Will it widen the gap between Europe and the U.S?", en AA. VV. (coord. por Dörr, Dieter, y Weaver, Russell, *Perspectives on Privacy: Increasing Regulation in the USA, Canada, Australia and European Countries*, De Gruyter, Berlín, 2015.

Svantesson, D. J.: *Extraterritoriality in Data Privacy Law*, Ex tuto Publishing, Copenhague, 2013.

Taylor, M.: "Permissions and prohibitions in data protection jurisdiction", *Brussels Privacy* Hub *working paper*, 2016, núm. 6, vol. 2.

Vinaixa Miquel, M.: *La responsabilidad civil por contaminación transfronteriza derivada de residuos*, USC, Santiago, 2006.

Von Hein, J.: "Social Media and the Protection of Privacy", *European Data Science Conference*, 2016.

Zell, A-M.: "Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field", *German Law Journal*, 2014, 2014, vol. 15.