FACULTAD DE DERECHO

PROBLEMAS DE DERECHO INTERNACIONAL PRIVADO RELATIVOS A LA PROTECCIÓN DE DATOS

Autor: Itziar Damborenea Trigueros

5º E5

Derecho internacional privado

Tutora: María José Lunas Díaz

Madrid

Abril 2020

Resumen

El presente trabajo de investigación explora la cuestión problemática de la protección de los datos de carácter personal en el ámbito del Derecho internacional privado. El desarrollo de internet y de las nuevas tecnologías ha supuesto el aumento de complejas controversias internacionales en materia de protección de datos. Esta investigación examina esta problemática y propone la creación de una norma de Derecho internacional privado común capaz de unificar las soluciones a estos problemas. Con ese objetivo, el primer capítulo introduce la relevancia del objeto de la investigación y delimita su complejo ámbito de estudio. El segundo capítulo examina los distintos intentos de crear tanto una regulación sustantiva como una norma de Derecho internacional privado común en materia de protección de datos. Asimismo, se identifican los obstáculos que han impedido que esto se produzca y se presenta un análisis de la regulación existente actual. Los tres capítulos posteriores analizan los foros tradicionales de determinación de la competencia judicial internacional, los sistemas de resolución de conflictos de leyes existentes y los distintos planteamientos a la hora de regular las transferencias internacionales de datos. Una vez examinadas estas cuestiones, tres modelos de armonización son presentados con el objetivo de proponer una solución comprensiva, desde un mismo instrumento, a los problemas previamente expuestos.

Palabras clave

Protección de datos, privacidad, competencia judicial internacional, ley aplicable, transferencia internacional de datos.

Abstract

This research paper explores the problematic issue of personal data protection in the field of private international law. The development of the Internet and the advancement of new technologies has led to an increase in complex international data protection disputes. This investigation examines these problems and proposes the creation of a common private international law standard capable of unifying the solutions to these issues. With this aim, the first chapter introduces the relevance of the object of the investigation and delimits its complex matter of study. The second chapter examines the different attempts to create both a substantive regulation and a common private international law rule on data protection. It also identifies the obstacles that have

prevented this from taking place and presents an analysis of the existing regulation. The three subsequent chapters analyse the traditional forum for determining international jurisdiction, the existing systems for resolving conflicts of law and the different approaches to regulating international data transfers. Once examined, three models of harmonization are proposed with the aim of proposing a comprehensive solution, from the same instrument to the problems previously exposed.

Keywords

Data protection, privacy, international jurisdiction, applicable law, international data transfers.

Lista de abreviaturas

APD	Agencia de protección de datos o autoridad de control
ASEAN	Asociación de Naciones del Sudeste Asiático
CBPR	Cross Border Privacy Rules
CCI	Cámara de comercio internacional
CJI	Competencia judicial internacional
CL	Convención de Lugano
Convención 108	Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal
DIPr	Derecho internacional privado
Directiva 95/46/CE	Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
EEE	Espacio económico europeo
EEUU	Estados Unidos
HCCH	Conferencia de La Haya de Derecho Internacional Privado
LA	Legislación aplicable
LOPDGDD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales
NCV	Normas corporativas vinculantes
OECD	Organización para la Cooperación y el Desarrollo Económico
PIPEDA	Personal Information Protection and Electronic Documents Act
RBIb	Reglamento Bruselas I bis
RR-I	Reglamento Roma I
RR-II	Reglamento Roma II
TJCE	Antiguo Tribunal de Justicia de las Comunidades Europeas
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea
UNCTAD	Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

CAPÍTULO I: INTRODUCCIÓN

Hoy en día vivimos en un mundo que cada vez se encuentra más globalizado y conectado a las redes. El desarrollo de la tecnología e internet ha mejorado considerablemente nuestros estándares de vida a la par que ha contribuido a la comodidad en nuestro día a día. Asimismo, el avance de la sociedad de la información y las redes sociales ha aumentando nuestra conectividad y facilitado el alcance a toda clase de información. Este desarrollo tecnológico, que involucra la combinación de las tecnologías y su interacción a través de los dominios físicos, digitales y biológicos constituye lo que los expertos denominan como la cuarta revolución industrial (Schwab, 2016). En ésta los datos personales juegan un papel importante en cuanto sirven como base para el desarrollo de tecnologías disruptivas, como el IoT o la inteligencia artificial, que cambiarán radicalmente nuestro modo de vida. Ahora bien, acompañando a los beneficios que ha supuesto y supone el avance de la tecnología en general, también se encuentran una serie de riesgos a los cuales hemos quedado expuestos. Respecto de los mismos, los que resultan relevantes de cara a esta investigación son los problemas que surgen como resultado del tratamiento informatizado de los datos de carácter personal en el ámbito internacional. El desarrollo de la tecnología significa que en muchas ocasiones se realice un uso ilícito de los datos en cuanto adquieren un valor utilitario. Esto es, distintos agentes presentes en internet se aprovechan de los mismos con finalidad lucrativa, lo que comporta un gran riesgo para los derechos fundamentales de las personas físicas y en concreto, para el derecho de la privacidad, la intimidad personal y familiar y el honor. Así, la protección de los datos de carácter personal, en sentido estricto, no resulta exclusivamente una cuestión internacional, pero en muchas ocasiones lo es a razón de la conectividad, la internacionalización del internet y el desarrollo de las nuevas tecnologías, generando una serie de problemas de Derecho internacional privado («DIPr»). Por tanto, el objetivo de la presente investigación es el de identificar los problemas propios de DIPr de la protección de datos de carácter personal y aportar soluciones a los mismos.

1. ¿POR QUÉ ES RELEVANTE ESTA INVESTIGACIÓN?

La materia objeto de análisis de esta investigación resulta de gran relevancia principalmente por tres razones. En primer lugar, porque el propio desarrollo de la

tecnología y el uso de internet[1] se sustenta en la recopilación y utilización de datos. Por tanto, en cuanto vivimos en un mundo globalizado en expansión, los conflictos que puedan surgir a nivel internacional respecto de la protección de datos aumentarán exponencialmente conforme transcurran los años[2]. En segundo lugar, esta discusión apela a distintos acontecimientos que han ocupado los medios internacionales y han provocado la concienciación de una gran parte de la población mundial acerca de la importancia de la protección de los datos personales. El caso más notorio lo constituyó el escándalo de Cambridge Analytica, empresa que se hizo con los datos recogidos por Facebook de aproximadamente 87 millones de personas para apoyar las campañas de elección de Trump y del Brexit. Los datos sirvieron para crear modelos de comportamiento y seleccionar votantes individuales con el objetivo de predecir e influenciar sus decisiones de voto (Privacy International, 2019). Este acontecimiento generó una gran repercusión internacional en cuanto Facebook no evitó ni informó a sus usuarios de la utilización de sus datos con fines políticos. Así, este caso representa más que ningún otro, la importancia que debe darse a la protección de datos en cuanto estos pueden ser utilizados con finalidades que pueden llegar hasta a propiciar importantes cambios en la gobernanza mundial. Por último, tras un análisis exhaustivo de la bibliografía disponible resulta sorprendente la escasez de trabajos[3], actualizados[4], que hagan referencia al ámbito de estudio aquí expuesto.

2. UNA CUESTIÓN PROBLEMÁTICA

Antes de proceder a presentar el grueso de esta investigación debe delimitarse su objeto de estudio. Esta delimitación no debe entenderse como un compartimiento estanco si no como parte de la problemática general de la protección de datos desde la perspectiva del DIPr.

[1] Como explica De Miguel Asensio (2017, p.76) la utilización de información sobre personas físicas se construye como elemento esencial de las actividades ofertadas o prestadas a través de Internet.
[2] En concreto, el desarrollo del "cloud computing" implica un flujo transfronterizo constante de datos.
[3] Opina de igual manera el experto Chritopher Kuner (2010, p.246) "*los organismos internacionales que se ocupan de cuestiones de jurisdicción internacional (como la Conferencia de La Haya de Derecho Internacional Privado) han mostrado poco interés en la legislación sobre protección de datos; la mayoría de los artículos y libros académicos que tratan de la jurisdicción en Internet han dedicado poco espacio a las cuestiones de protección de datos; y los reguladores de la protección de datos han mostrado poca comprensión de las cuestiones de jurisdicción internacional*".
[4] La mayoría de trabajos fueron publicados antes de que entrara en vigor el importante Reglamento General de Protección de Datos europeo.

2.1. ¿Derecho internacional privado o público?

De cara a delimitar el ámbito de estudio, la primera incógnita que hemos de despejar es la de determinar si la regulación en materia de protección de datos es considerada como parte del derecho público, privado[5] o una como una combinación de ambos. Esta distinción resulta relevante en cuanto normalmente los tribunales de un Estado no aplican el derecho público de una jurisdicción extranjera. Por tanto, si se considera que la regulación en materia de protección de datos constituye una materia propia del derecho público, los órganos jurisdiccionales o la agencia de protección de datos (o «APD»)[6] de un determinado Estado aplicarán su propia ley y nunca la extranjera (Bing, 1999). Asimismo, el aclarar esta distinción permite esclarecer cuando resultan de aplicación importantes instrumentos jurídicos como el Reglamento Bruselas I[7]. Pues bien, las leyes sobre protección de datos no pueden clasificarse como pertenecientes en su totalidad al derecho público o privado en cuanto estas derivan de una pluralidad de fuentes legales, como son el derecho de protección de los consumidores, las leyes sobre derechos humanos o leyes sobre comercio, entre otras (Kuner, 2010). Como explica el profesor Bing (1999, 3) "*La legislación sobre protección de datos contendrá normalmente disposiciones de derecho público, relativas a una autoridad y a sus deberes y decisiones. Pero la ley también incluirá a menudo disposiciones de derecho civil, típicamente sobre la responsabilidad por violaciones de la protección de datos. Por consiguiente, las disposiciones de la legislación de protección de datos pueden tener que calificarse como pertenecientes a diferentes ámbitos del derecho, a los que se asignan diferentes criterios de conexión pertinentes"*. Por tanto, la protección de datos no debe considerarse en su totalidad como un asunto de derecho público o privado, sino que esto se deberá determinar ad hoc. De esta manera, a grandes rasgos podemos afirmar que si una APD adopta una medida que comporta un elemento internacional, esta debe considerarse desde el derecho público internacional. Por otro lado, si se

[5] El objeto del DIPr lo constituye las situaciones de naturaleza privada y carácter internacional (Campuzano Díaz et al, 2018). Por tanto, para que la cuestión de la protección de los datos de carácter personal se trate dentro del ámbito del DIPr deberá cumplir con dos características. Por un lado, (a) tendrá que existir una situación privada. Esto es, una relación entre sujetos privados, una relación horizontal en un plano de igualdad entre sujetos. Además, (b) la controversia surgida entre los dos sujetos privados deberá revestir un carácter internacional, lo que significa que deberá vincular a dos o más Estados.

[6] Estas también pueden conocerse con el nombre de autoridades de control, pero de cara a unificar su denominación se ha optado por utilizar el término APD.

[7] Según el primer artículo del mismo, "*el presente Reglamento se aplicará en materia civil y mercantil con independencia de la naturaleza del órgano jurisdiccional*". Por tanto, solo se aplicará a materias propias del DIPr.

genera una controversia internacional entre dos sujetos privados[8] respecto de la protección de datos de carácter personal, esta se enmarcará dentro del DIPr.

2.2. ¿Qué actos hacen que surjan disputas internacionales en el ámbito de la protección de datos personales?

En segundo lugar, cabe preguntarse acerca de que actos, acciones o actividades ejercidas sobre los datos de carácter personal hacen que surjan problemas en el ámbito internacional. Pues bien, las controversias internacionales surgen como consecuencia de un tratamiento o uso indebido de los datos personales. Si bien la denominación concreta que se le da al término utilizado para definir la utilización de los datos difiere, esta abarca un gran número de actividades, en cuanto la mayoría de textos regulatorios protegen a los datos de un gran abanico de actividades. De esta manera, la Unión Europea (o «UE») a través del Reglamento General de Protección de Datos (o «RGPD») se refiere a este término como "tratamiento" el cual constituye una categoría amplia que abarca "*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*". Por su parte, Canadá a través del *Personal Information Protection and Electronic Documents Act* (o «PIPEDA») reconoce la protección de los datos personales respecto de las actividades de recopilación, utilización y divulgación de información personal. Por otro lado, Australia a través del Privacy Act de 1988 no se refiere como tal a las actividades que quedan protegidas, sino que se refiere a la protección de datos personales en sentido general. Por consiguiente, de cara a una mayor claridad expositiva se procederá a utilizar el término tratamiento para hacer referencia a todas las actividades a las cuales pueden ser sometidos los datos. Por ende, grosso modo los problemas que surgen respecto de los datos de carácter personal se originan cuando a estos se les da un tratamiento o utilización inadecuada en virtud de las distintas normas legales. De esta

[8] Respecto de estas controversias internacionales, como explicó el juez de la Corte Internacional de Justicia (o «CIJ»), Hersch Lauterpacht (1958), los derechos de las partes no deberán determinarse en función de los misterios controvertidos de la distinción entre el derecho privado y el derecho público. Por tanto, la presente investigación no ahondará en esta distinción entre ordenamientos jurídicos, sino que directamente pasará a conocer de las controversias surgidas entre las partes.

manera, pueden surgir problemas de DIPr generados por distintas causas como pueden ser la recogida indebida de datos, la selección ilegal de los mismos, la publicidad indebida, los tratamientos transfronterizos o las acciones difamatorias relacionas con los mismos, entre otras muchas causas. Si bien esta investigación se refiere al tratamiento en general de los datos personales, se realiza una especial referencia o hincapié en las transferencias internacionales de datos, por constituir esta la actividad de tratamiento que más intensamente representa los problemas de DIPr[9].

2.3. ¿Una materia contractual o extracontractual?

En tercer lugar, debe determinarse si las disputas que surgen en el ámbito de la protección de datos de carácter personal tienen un origen contractual o extracontractual[10]. La diferencia radicaría en si el conflicto surge a raíz de un contrato entre las partes o no. Pues bien, señalan Calvo Caravaca y Carrascosa González (2017) que la mayor parte de reclamaciones relacionadas con la protección de datos personales tienen un origen extracontractual[11], en cuanto no existe un contrato entre las partes sino una serie de obligaciones creadas por la ley que debe respetar aquel que trata o almacena esos datos. Así, en caso de que la víctima considere que se ha hecho un uso indebido de sus datos podrá solicitar una reclamación por daños y perjuicios ante un juez del orden civil[12]. Ahora bien, podrán también surgir controversias respecto del incumplimiento de obligaciones contractuales. Estas se suscitarán a raíz del incumplimiento de contratos cuyo objeto o previsiones se refieran a la protección de datos de carácter personal[13]. Asimismo, en materia contractual, cuando el interesado además sea un consumidor deberán aplicarse las normas de DIPr destinadas a la protección del mismo. Por ende, el daño que surja respecto de un tratamiento indebido de los datos de carácter personal tendrá la consideración de contractual cuando entre las partes hubiera existido una previa relación contractual y se hubiera incumplido lo

[9] Afirma Ortega Giménez (2014, p.27) que las transferencias internacionales son "*terreno abonado para la aparición de problemas que son objeto de estudio por parte del Derecho internacional privado*" y constituyen un "*autentico desafío para el Derecho internacional privado*" (2014, p.29).

[10] Se refiere la literatura anglosajona a la rama del derecho de los "Torts".

[11] Por ejemplo, una empresa china compra a una empresa belga de marketing unos ficheros de datos personales que esta última ha elaborado sin el consentimiento de los titulares de los mismos. La empresa China utiliza los ficheros para enviar multitud de publicidad. Los titulares de los datos podrán reclamar una indemnización por responsabilidad extracontractual.

[12] Podrá asimismo interponer reclamación ante una APD, no obstante no tendrá derecho a indemnización.

[13] Respecto del ejemplo anterior, el contrato de compraventa de los ficheros que contienen datos de carácter personal, suscrito entre la empresa belga y la china constituye una relación contractual cuyo objeto se encuentra relacionado con la protección de datos de carácter personal.

pactado. Por el contrario, en caso de que no exista vínculo contractual entre las partes o la disputa surja, entre las mismas, por cuestiones distintas al cumplimiento del contrato supondrá que la disputa tenga carácter extracontractual y se prevea la exigencia de una indemnización por daños y prejuicios.

Respecto del caso concreto de las transferencias internacionales de datos nos encontramos con una relación triangular[14] entre los sujetos que podrá ser contractual o no dependiendo de las circunstancias (véase el anexo nº.1). Con carácter general, el cedente[15] transmitirá los datos al cesionario[16] en virtud de una relación contractual y por tanto cualquier controversia que surja entre ellos revestirá la condición de contractual. Respecto del titular de los datos[17], este podrá haber firmado o no un contrato con el cedente de los datos. Por tanto, entre ellos podrán surgir obligaciones de naturaleza contractual o extracontractual. Por último, entre el cesionario y el titular surgirá responsabilidad extracontractual en cuanto resulta improbable que medie contrato entre ellos.

2.4. ¿Una cuestión de privacidad, internet, comercio electrónico o una rama del derecho diferenciada?

Por último, nos encontramos ante el problema de la inexistencia en muchos países del derecho a la protección de datos de carácter personal per se. Si bien la Unión Europea (o «UE») ha reconocido en el artículo 8 de su Carta de Derechos Fundamentales la protección de los datos de carácter personal como un derecho fundamental[18], países como Estados Unidos (o «EEUU») o Canadá u organizaciones supra-nacionales como la Asociación de Naciones del Sudeste Asiático («ASEAN») no reconocen este derecho como tal, sino que se limitan a proteger el derecho a la privacidad y por asociación a la intimidad personal y familiar y en cierta medida al honor. Por lo tanto, el derecho a la

[14] En virtud de esta, en caso de que una transferencia no cumpla con los requisitos necesarios, el interesado podrá dirigirse contra el cedente de los datos, pudiendo acudir a los tribunales de lo civil o interponiendo una reclamación administrativa ante la ADP correspondiente. Por otro lado, en el supuesto que la transferencia sí resulte válida pero el tratamiento por parte del cesionario resulte ilícito podrá el interesado dirigirse contra este o contra el cesionario, dependiendo del régimen de transferencia ante el cual nos encontremos.

[15] El cedente entendido como el responsable de tratamiento de los datos del individuo particular. También puede conocerse como exportador.

[16] También puede conocerse con el término importador.

[17] El titular de los datos entendido como la persona cuyos datos están siendo transferidos.

[18] De esta manera la UE, construye el derecho a la protección de los datos de carácter personal como un derecho autónomo respecto del derecho al respeto de la vida privada y familiar, reconocido en el artículo anterior.

protección de datos no existe como un área del derecho diferenciada sino que se incluye en el cajón de sastre de la privacidad. Como explica Kuner (2010, 309) los conceptos de privacidad y protección de datos son "*gemelos pero no idénticos*". Si bien ambos conceptos pueden superponerse, la privacidad constituye un concepto mucho más amplio. Por tanto, no siempre una controversia sobre la protección de datos versará sobre una cuestión de privacidad, ni viceversa. La existencia de un derecho a la protección de datos diferenciado de la categoría de la privacidad significa una protección más efectiva para los individuos, que podrán controlar el uso que se le da a sus datos. Asimismo, la inexistencia de la protección de datos como rama autónoma del derecho supone que muchos autores fuera del contexto europeo[19] – sobretodo los norteamericanos – se refieran a las cuestiones propias del DIPr de la protección de datos de carácter personal por relación y de manera subsidiaria respecto de internet. Es decir, fuera del ámbito de estudio europeo, existe multitud de bibliografía que hace referencia a las cuestiones propias de la determinación de la competencia judicial internacional (o «CJI») y legislación aplicable (o «LA») en internet en un sentido general, y poca que hace referencia concretamente a la protección de datos de carácter personal. Por ende, la protección de datos se trata de manera accesoria respecto de otras cuestiones como son el comercio electrónico[20], las acciones difamatorias realizadas a través de las redes o respecto de la propiedad intelectual e industrial. Es por ello, que reviste de especial dificultad el encontrar jurisprudencia, doctrina y legislación tratando la cuestión de los datos de carácter personal como tal fuera del ámbito europeo.

CAPÍTULO II: REGULACIÓN DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

1. AUSENCIA DE UN MARCO GLOBAL

Actualmente, no existe un marco global vinculante que regule de manera más o menos uniforme el tratamiento de los datos de carácter personal ni proponga soluciones a los problemas de DIPr. Si bien este no evitaría que surgieran la mayor parte de los problemas, sí simplificaría y unificaría las soluciones. No obstante, en cuanto la disciplina no es necesariamente joven (Yu & Zhao, 2019) se han realizado varios

[19] Sostiene Christopher Kuner (2009) que la legislación en materia de protección de datos como tal constituye una creación europea.

[20] Estableció la HCCH en 1999 que la recopilación de datos, incluidos los datos personales, y su procesamiento son inherentes al comercio electrónico. En el mismo sentido, un año más tarde, la HCCH (2000) afirmó que los temores de los usuarios de Internet respecto a la recopilación y utilización de sus datos personales tienden a frenar el desarrollo del comercio electrónico.

intentos destinados a construir este marco. En orden cronológico, el origen lo encontramos en 1973, cuando un comité asesor del gobierno de EEUU propuso los denominados *Fair Information Principles*. Estos constituyen cinco principios[21] que tienen el objetivo de garantizar la protección de la privacidad y la seguridad de la información almacenada en sistemas computarizados (Reidenberg, 1999). Cinco años más tarde, la Organización para la Cooperación y el Desarrollo Económico (o «OECD») se sirvió de los mismos para construir ocho principios[22] que serían codificados en las "Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales"[23]. Estos principios revisten de una gran importancia por dos razones. En primer lugar, han servido como base para el desarrollo de la regulación en materia de protección de datos de órganos supra-nacionales como la UE o APEC y de leyes nacionales como la de Nueva Zelanda. En segundo lugar, representan el consenso internacional sobre la orientación general relativa al tratamiento de datos personales (Wu, 2010). En 1981, el Consejo de Europea celebró en Estrasburgo, la "Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal"[24] (o «Convención 108»). Si bien este tratado se encuentra inspirado en los principios desarrollados por la OECD, ofrece una mayor protección, una regulación más completa y resulta obligatoria para sus signatarios (Reidenberg, 1999). Desde 2008 se encuentra abierto para la firma de Estados no miembros de la UE, convirtiéndose así en "*el primer y único instrumento jurídico internacional vinculante que protege la privacidad de los datos*" (Electronic Private Information Center, s.f.).

1.1. La problemática falta de consenso acerca de los problemas de DIPr

Tanto los principios elaborados por la OECD como por el Consejo Europeo gozan de gran importancia en cuanto en base a ellos se han construido las leyes de protección de datos actuales. No obstante, ninguno de estos instrumentos hacen referencia alguna a las

[21] Estos son el principio de: (1) publicidad. (2) accesibilidad, (3) consentimiento, (4) rectificación y (5) responsabilidad. Veáse: "The Code of Fair Information Practices" https://simson.net/ref/2004/csg357/handouts/01_fips.pdf. [Último acceso: 7/04/2020].

[22] Estos son el principio de: (1) colección limitada, (2) calidad, (3) especificación del propósito, (4) uso limitado, (5) salvaguardia de la seguridad, (6) publicidad, (7) accesibilidad y (8) responsabilidad.

[23] Véase "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data": https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [Último acceso: 6/04/2020].

[24] Véase "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108. [Último acceso 6/04/2020].

cuestiones propias del DIPr. Es más, en 2013[25] la OECD revisó los principios de privacidad[26] y señaló que si bien el grupo de expertos había dedicado una gran atención a esclarecer las cuestiones propias de la determinación de la CJI y LA, la complejidad del asunto[27], acompañado del rápido desarrollo de la tecnología y el carácter no vinculante de las directivas, había resultado en la decisión de no proponer soluciones detalladas[28]. Del mismo modo, la Conferencia de la Haya de Derecho Internacional Privado (o «HCCH») no ha podido esclarecer las cuestiones propias de DIPr. En 1999, la HCCH organizó la denominada "mesa redonda de Ginebra sobre comercio electrónico y Derecho internacional privado"[29]. Durante la misma se consideraron diversos temas relacionados con el comercio electrónico, siendo uno de estos la protección de datos. Respecto a la determinación de la jurisdicción en los casos de responsabilidad extracontractual, el HCCH no pudo llegar a ninguna conclusión definitiva, sosteniendo que "*es difícil apartarse de uno de los dos factores de conexión: el foro de residencia habitual del demandado o de la víctima. Algunos participantes exigirían que el foro de residencia habitual de la víctima coincidiera con al menos parte de la lesión"*. Asimismo, sobre la ley aplicable a la protección de datos, la mesa sostuvo que "*es necesario realizar un estudio sobre el sistema más pertinente de derecho aplicable que permita también dar un mayor papel a la autorregulación y a los contratos tipo como los propuestos por la Cámara Internacional de Comercio (o «CCI»)[30] y de acuerdo con los principios recomendados por el Consejo de Europa[31]*". Un año más tarde, Catherine Kessedjian (2000) como secretaria general de la HCCH,

[25] En 1980 la OECD ya había prestado atención a la determinación de la CJI y LA respecto del flujo transfronterizo de datos y la protección privacidad, pero no llegó a ninguna conclusión. Únicamente se emitió una recomendación que hacia referencia a que los Estados miembros debían trabajar en la elaboración de principios, nacionales e internacionales, que rigieran el derecho aplicable (véase el párrafo 22 de los principios de 1980).

[26] Véase "The OECD Privacy Framework" https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [Último acceso el 6/04/20].

[27] Véase página 46 del OECD Privacy Framework.

[28] Véase página 63 del OCED Privacy Framework.

[29] Véase la nota de prensa sobre la misma: https://www.hcch.net/es/news-archive/details/?varevent=63. [Último acceso: 30/03/2020].

[30] La CCI, en consonancia con los requisitos establecidos por la Unión Europea para permitir la transferencia de datos a terceros estados, ha elaborado un modelo de clausulas contractuales alternativas. Véase "Final Approved Version of Alternative Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries (controller to controller transfers)" https://iccwbo.org/content/uploads/sites/3/2010/05/ICC-Alternative-Standard-Contractual-Clauses-for-the-Transfer-of-Personal-Data-from-the-EU-to-Third-Countries.pdf. [Último acceso 7/04/2020].

[31] Estos son los de la Convención 108. Si bien, cuando se produjo este pronunciamiento por parte de la HCHH la UE ya había promulgado la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos dato (o «Directiva 95/46/CE»).

elaboró un documento refiriéndose en detalle al intercambio electrónico de datos, internet y comercio electrónico, desarrollando y completando la labor de la mesa un año antes. Kessedjian (2000, 21) sostuvo que la falta de acuerdo acerca de la determinación de la CJI sobre las materias de responsabilidad extracontractual se debía a la disparidad de opiniones sobre el artículo 10[32] del anteproyecto de la Convención sobre la jurisdicción y las sentencias extranjeras en materia civil y comercial[33]. Parte de los expertos sostenían que el foro fuera el del domicilio del demandante, normalmente la víctima. Para otros miembros de la Comisión, el foro se debía referir al lugar del acto o de la omisión causante del perjuicio – que se situaría en el lugar de residencia habitual del demandado o del autor del acto – y al lugar donde se produjo el perjuicio – que se situaría en el lugar de residencia habitual del demandante o de la víctima, o en el lugar donde se produjo el perjuicio más importante –. Respecto de la LA en materia extracontractual, aconteció la misma división. Parte de los expertos consideraron que debía aplicarse la *lex fori* por razones pragmáticas, en cuanto el conflicto de jurisdicción absorbe el conflicto de leyes. La otra parte, consideró que debía ofrecerse al interesado la elección entre la ley del país en el que se produjo el acto perjudicial o la ley del país en el que se produjo el perjuicio.

Existen varias razones que explican tanto la falta de acuerdo respecto de una regulación sustantiva común sobre la protección de datos, como sobre una norma de DIPr común. En primer lugar, como mencionó la OECD el rápido desarrollo de la tecnología dificulta la tarea de construir marcos de regulación comprensivos. Asimismo, existen grandes diferencias entre Estados respecto de la noción de la protección de los datos. Es decir, si bien algunos Estados optan por proteger de manera más intensa la libre circulación de

[32] Artículo 10: "*Variante 1 (Trabajo. Doc. 86). El demandante puede presentar su demanda, en asuntos de responsabilidad extracontractual: a) en el lugar donde se produjo el hecho que causó el daño; o b) en el lugar donde se produjo inicialmente el perjuicio, siempre que el comportamiento del demandado tuviera por objeto producir efectos en el Estado de que se trate. Si el perjuicio se produjo en el territorio de varios Estados, la reclamación puede presentarse en el lugar de un Estado en el que se produjo una parte significativa del perjuicio. El demandante puede entablar una acción para obtener un mandamiento judicial de cesación de una actividad que podría causarle un perjuicio, ya sea en el lugar de esa actividad o en el lugar en que podría producirse el perjuicio. Variante 2 (Trabajo. Doc. 89, Nº 2) El demandado estará sujeto a la jurisdicción de un Estado para las reclamaciones derivadas de actividades en cualquier lugar si la reclamación... a) se relaciona con la actividad comercial del demandado que se lleva a cabo en el marco de la venta, la compra o el uso de bienes o servicios en ese Estado o en relación con ellos; y b) i) En el caso de un supuesto de responsabilidad extracontractual, el perjuicio se produjo en ese Estado; o [(ii)...] siempre y cuando la demanda no surja de un negocio o profesión del demandante*".

[33] Véase "preliminary draft outline to assist in the preparation of a convention on international jurisdiction and the effects of foreign judgments in civil and commercial matters" de 1998: https://assets.hcch.net/docs/0cbb3742-8964-4c0d-9dd4-3e4e186138d8.pdf. [Último acceso 7/04/2020].

los mismos, otros prefieren aportar una mayor protección a los individuos. Por ejemplo, EEUU posee una regulación sectorial que favorece la protección de los intereses comerciales y por ende apuesta por una circulación de datos menos restrictiva, mientras que en Europa se protege de manera más intensa a los individuos. Igualmente, la Comisión de Derecho Internacional de Naciones Unidas ha admitido que la protección de datos es una esfera "*en la que la práctica de los Estados todavía no es extensa ni está plenamente desarrollada*" (ILC, 2006). Por último, la dicotomía entre los intereses del sector público y privado también contribuyen a la falta de acuerdos. Los empresarios y aquellos que ejercen el comercio electrónico siempre van a optar por una regulación más flexible que favorezca sus intereses y propulse el libre intercambio de datos, mientras que los individuos, de manera habitual buscarán la protección de sus datos como extensión de su personalidad. Es decir, la necesidad de llegar a un consenso es innegable pero reviste de una evidente complejidad en cuanto deben conciliarse intereses cómo la protección de la intimidad personal, las aspiraciones comerciales de las empresas involucradas en el tratamiento internacional de datos y la libertad de la información y comunicación.

2. ESTATUS DE LA REGULACIÓN ACTUAL

De acuerdo con las estadísticas elaboradas por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo («UNCTAD») (2020)[34] el 64%[35] de los países, o 107 países, poseen legislación en materia de privacidad o protección de datos[36]. De esta manera, a modo enunciativo, nos encontramos con PIPEDA (2000) en Canadá, el Privacy Act (1988) en Australia, el *Federal Law Regarding Personal Data* (2006) en Rusia, la Ley Orgánica de Protección de Datos Personales y la garantía de los derechos digitales (o «LOPDGDD») (2018) en España o la Ley de Protección de Datos Personales (2000) en Argentina. A nivel supraestatal, encontramos el RGPD (2016) en Europa, el *Framework on Personal Data Protection* (2016) de ASEAN o la Convención en ciberseguridad y la protección de datos personales (2019) de la Unión Africana (o «UA»).

[34] Véase https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. [Último acceso: 30 de marzo de 2020].

[35] Respecto del 36% de países restantes; el 8% se encuentran en proceso de adoptar una legislación, 18% no poseen ningún tipo de legislación en la materia y sobre el 11% de los países no se poseen datos (UNCTAD, 2020).

[36] Como ha sido explicado anteriormente, si bien numerosos ordenes jurisdiccionales no reconocen el derecho a la protección de datos de carácter personal como tal, sí ofrecen un marco que regula el tratamiento de los mismos desde la protección de la privacidad y derivados.

De todas ellas, el marco de regulación más completo y detallado (Carey, 2018) y por ende restrictivo es el europeo. El RGPD que comenzó a aplicarse el 25 de mayo de 2018, derogó la Directiva 95/46/CE. Por ende, la Unión Europea ha pasado de armonizar las legislaciones europeas a directamente unificarlas a través de un reglamento único supra-nacional[37]. El Reglamento construye un marco favorable para los individuos en cuanto protege efectivamente el derecho a la protección de datos de carácter personal a la par que restringe las actividades de los responsables del tratamiento. Por tanto, constituye una ventaja para los ciudadanos europeos y al mismo tiempo una carga para las empresas que prestan servicios en la UE. Esto es, no resulta del todo claro si ofrece en puridad una ventaja competitiva o constituye un obstáculo internacional. Es decir, si sitúa en general a los europeos en una mejor o peor posición. La respuesta, en mi opinión, dependerá de a quien se pregunte. Para los responsables de tratamiento, las fuertes restricciones legales impuestas por Europa suponen un gran impedimento a la hora de competir con otras áreas del planeta, como Asia. Por otro lado, los individuos se benefician de un régimen más seguro. Por tanto, el régimen regulatorio Europeo constituye tanto una ventaja como un obstáculo.

No obstante, lo que está claro a mi juicio, y en consonancia con la opinión de muchos expertos como Ana Gascón (2019, 416), es que la característica principal del RGPD es su efecto de propagación, por el cual el nivel de protección de datos de carácter personal aumenta también fuera de la UE. Es decir, como consecuencia del amplio ámbito de aplicación y carácter restrictivo del Reglamento, los distintos actores públicos y privados se ven obligados a aumentar el nivel de protección respecto del tratamiento de los datos europeos, lo que puede causar que este aumento del nivel de protección se extienda al tratamiento de datos en terceros Estados. Es decir, en cuanto el RGPD establece las normas del mayor mercado de consumidores del mundo presiona a las entidades que operan a nivel mundial a adaptar sus principios para todos sus clientes (Bendiek & Römer, 2018). Por tanto, la importancia del RGPD radica en su potencial de aumentar a nivel global el nivel de protección de datos[38].

[37] El RGPD se aplica al conjunto de tratamientos de datos relativos a personas físicas identificadas o identificables.

[38] Anu Bradford (2012) se ha referido al denominado "efecto Bruselas" por el cual la UE participa en la regulación unilateral de los mercados mundiales. Esto puede verse de manera clara en la influencia que la legislación de protección de datos de la UE ha tenido en la elaboración de la legislación de numerosos terceros países (Kuner, 2009, p.14).

2.1. Notas comunes y diferencias

Como ha sido mencionado anteriormente, 107 países poseen algún tipo de regulación que protege el tratamiento de los datos de carácter personal (UNCTAD, 2020). De su análisis pueden extraerse la presencia de tres notas o características comunes y una multitud de diferencias.

En primer lugar, como ha sido explicado previamente, en cuanto la mayoría de regulaciones se basan en los mismos instrumentos[39], comparten los mismos principios informadores generales. Si tomamos como ejemplo PIPEDA[40], la LOPDGDD, la regulación de Asean y la Convención de la UA encontramos que los principios son:

PIPEDA	**LOPDGDD**	**Framework on Personal Data Protection**	**Convención en ciberseguridad y la protección de datos personales**
CANADÁ	ESPAÑA	ASEAN	UA
1. Responsabilidad 2. Identificación 3. Consentimiento 4. Recogida limitada 5. Limitar uso, divulgación y retención 6. Exactitud 7. Garantías 8. Apertura 9. Acceso 10. Responsabilidad	1. Exactitud 2. Confidencialidad 3. Consentimiento 4. Tratamiento limitado 5. Categorías especiales	1. Consentimiento, notificación y propósito 2. Exactitud 3. Garantías de seguridad 4. Acceso y corrección 5. Transferencias 6. Retención 7. Responsabilidad	1. Consentimiento y legitimidad 2. Legalidad y justicia 3. Propósito, relevancia y almacenamiento 4. Exactitud 5. Confidencialidad y seguridad

[39] Los principios de la OECD (1980) y de la Convención 108 (1981).
[40] Véase los "PIPEDA fair information principles" https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/. [Último acceso: 30 de marzo de 2020].

Por tanto, sin entrar a valorar los mismos, podemos confirmar que la primera nota o característica común de los distintos regímenes regulatorios es la presencia de los mismos principios fundamentales (Reidenberg, 1999), en cuanto ha quedado probado que estos son similares entre regiones y sistemas jurídicos. Ahora bien, aun siendo estos similares, los detalles de las distintas leyes difieren sustancialmente. En este sentido se manifiesta Yuehua Wu (2010, 158) que afirma que "*en general, aunque los principios generales de protección de datos son en gran medida idénticos, la forma en que se aplican esos principios para poner en práctica la protección difiere considerablemente de un país a otro*". Es decir, si bien los principios informadores se asemejan a nivel global esto no significa que exista el mismo nivel de protección de los datos personales en todo el mundo[41]. Existen regulaciones más estrictas o más laxas, más completas o más simples o incluso cuya finalidad es distinta. Como explica Marilyn Prosch (2008) estas diferencias son producto de dos factores: (a) distintos planteamientos por parte de los gobiernos y organismos reguladores que buscan o proteger al individuo (como ocurre en la UE) o proteger a las empresas (como ocurre en EEUU) y (b) las diferencias culturales en cuanto estas pueden afectar a las expectativas y las expectativas pueden, en cierta medida, dar forma a la legislación. Por tanto, como explica el profesor Joel L. Reidenberg (1999), en cuanto el grado de protección varía sustancialmente entre Estados, los datos personales en su dimensión internacional generan el enfrentamiento y el conflicto entre los diferentes regímenes nacionales de protección de la información personal, generando problemas de DIPr.

En segundo lugar, la mayoría de Estados que han adoptado una regulación en materia de protección de datos o privacidad han establecido agencias estatales encargadas de supervisar el cumplimiento de la misma[42]. Por ejemplo, en España nos encontramos con la Agencia Española de Protección de Datos, en Inglaterra con la Information Commisioner's Office, la Office of Privacy Comissioner en Canadá o Roscomnadzor en Rusia. En el otro lado de la balanza se encuentra EEUU, país donde no existe una APD central sino distintas agencias sectoriales o estatales. La mayoría de APD funcionan

[41] Ejemplo de ello es que si bien tanto la regulación en materia de protección de datos de APEC y la UE se basan en los principios de la OECD, Europa considera que muchos países miembros de la organización no ofrecen un nivel de protección adecuado.

[42] Esto se debe a que la existencia de una autoridad independiente de protección de datos se considera en general como un requisito previo para el establecimiento de un régimen adecuado de protección de datos (Kuner, 2009). De igual manera, Reidenberg (1999) sostiene que los organismos de supervisión de la protección de datos son una característica común de las democracias, pero las facultades de los organismos suelen ser específicas de cada país.

como órganos consultivos y de control que poseen poderes sancionadores y ante los cuales pueden ejercerse derechos y presentarse reclamaciones. La autoridad y competencias de las mismas dependerá de cada régimen jurídico[43]. Esta disparidad en sus funciones e importancia queda reflejada en la distintas potestades sancionadoras que se les reconoce a estas agencias[44]. En la UE en virtud del artículo 83.5 del RGPD las sanciones por infracciones muy graves pueden alcanzar "*hasta los 20 millones de euros como máximo o tratándose de una empresa de una cuantía equivalente al 4% como máximo del volumen del negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía*". Respecto de las infracciones graves, las sanciones pueden alcanzar hasta los 10 millones de euros o un 2% del volumen del negocio. En Canadá, el artículo 28 de PIPEDA establece multas de entre 6.500 o 65.400 euros[45] a aquellos que incumplan con ciertas disposiciones de la ley. En Argentina el artículo 31 de la Ley 25.326 de protección de los datos personales reconoce la facultad del organismo de control de interponer multas de entre 100 y 1.400 euros[46]. Por último, el Privacy Act (1974) de EEUU no menciona la posibilidad de interponer multas a aquellos que incumplan la misma[47].

Como una última nota común, la totalidad de las leyes en materia de protección de datos cuentan con sistemas destinados a limitar las transferencias de datos a terceros países (Bing, 1999). Si bien estos sistemas difieren considerablemente entre países, todos poseen la misma finalidad que es la de garantizar la protección efectiva de los datos de sus ciudadanos.

3. SOLUCIÓN

Como ha sido mencionado, en la actualidad ni existe un marco global de regulación sustantiva de la protección de datos de carácter personal ni tampoco un consenso sobre las normas de DIPr. Asimismo, existen Estados que ni si quiera poseen legislaciones

[43] En Europa es donde las APD gozan de mayores potestades. Los artículos 57 y 58 del RGPD reconocen un largo elenco de funciones y poderes a estas.

[44] Contra las acciones de las distintas ADP podrán interponerse distintos recursos contenciosos administrativos propios del ordenamiento jurídico público.

[45] El artículo 28 de PIPEDA recoge multas de hasta 10.000 o 100.000 dólares canadienses. Tasa de conversión a fecha 7/04/2020 según https://www1.oanda.com/lang/es/currency/converter/.

[46] El artículo 31 de la Ley 25.326 establece multas de entre 1.000 y 100.000 pesos argentinos. Tasa de conversión a fecha 7/04/202 según https://www1.oanda.com/lang/es/currency/converter/.

[47] Véase "Judicial remedies and penalties for violating the Privacy Act": https://www.justice.gov/jm/eousa-resource-manual-142-judicial-remedies-and-penalties-violating-privacy-act. [Último acceso 7/04/2020].

reguladoras de la protección de datos[48]. Respecto de aquella regulaciones nacionales y supra-nacionales que sí existen, si bien poseen varias notas o características en común, sus contenidos y por ende niveles de protección difieren sustancialmente. La combinación de estas cuatro realidades actúa como un generador de complejos conflictos de DIPr. Si bien no existe manera de evitar que surjan estos, sí podrían unificarse y simplificarse las soluciones que se dan a los mismos. Lo verdaderamente idóneo sería la promulgación de una regulación sustantiva común sobre la protección de datos[49]. Ahora bien, lo más factible a día de hoy y aún así difícil de conseguir, sería la creación de una norma global de DIPr común referida al ámbito de la protección de datos. Esta solución supondría la creación de una acuerdo vinculante capaz de unificar las normas estatales de DIPr a través de la utilización de criterios subjetivos, flexibles y particulares que permitirían conocer de la vinculación de un supuesto concreto con un país determinado, para así evitar la relatividad de las soluciones (Ortega Giménez, 2018). Ahora bien, para llegar a este acuerdo, se deberá: (a) superar la división entre los intereses del sector público y privado, (b) acercar las posturas de los distintos Estados, (c) construir un marco de regulación "tecnológicamente neutral" (Geist, 2001) y por lo cual capaz de adaptarse a los cambios de la tecnología, (d) encontrar un equilibrio entre la protección de los derechos de las personas y la libre circulación de la información y (d) llegarse a un consenso sobre la resolución de los problemas de DIPr per se. Para alcanzar este acuerdo debe hacerse uso de foros internacionales como la OECD o el HCCH[50], capaces de albergar distintas posiciones e intereses. Otra opción, podría ser que los Estados se unieran a la Convención 108[51] en cuanto instrumento jurídico internacional ya existente[52] y abierto para ser firmado. No obstante, debe partirse sobre la base de que cualquier intento internacional de aglutinar a todos los Estados nunca

[48] La ausencia de leyes reguladoras de la protección de datos puede dar lugar al fenómeno que Rafael Velázquez Bautista (1993, p.184) denomina como "paraísos de datos". En estos, los datos se tratan sin ningún tipo de restricción, vulnerando los derechos de sus titulares.

[49] La tensión entre el carácter mundial del tratamiento datos, por una parte, y el carácter nacional o regional de la legislación de protección de datos, por otra, revela la necesidad de construir un marco jurídico mundial para la protección de datos.

[50] La HCCH en el seno de su "Jurisdiction Project" ha realizado varios intentos para armonizar las normas sobre CJI y LA. Véase https://www.hcch.net/es/projects/legislative-projects/jurisdiction-project/ [Último acceso: 7/04/2020]. Ahora bien, todavía no lo ha conseguido. Asimismo, en el año 2006, la Comisión de Derecho Internacional de las Naciones Unidas incluyó en su programa de trabajo a largo plazo la "protección de los datos personales en el flujo transfronterizo de información", lo que podría conllevar en el futuro a la redacción de un convenio internacional. Véase el párrafo nº. 257 https://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf. [Último acceso: 30 de marzo de 2020].

[51] Países como Francia han abocado por esta opción (Kuner, 2010).

[52] Toy Alan y Gehan Gunaserkara (2019) sostienen que este deber ser el instrumento a utilizar en cuanto la creación de un nuevo marco resulta improbable.

será global. Sin embargo, esto no implica que deban abandonarse las pretensiones acerca de crear una norma común de DIPr. Para superar las dificultades propias de cualquier negociación internacional, debe diseñarse un marco flexible capaz de atraer a los Estados que a su vez sea lo suficientemente específico para aportar soluciones comunes a problemas globales. Por otro lado, otra posibilidad propuesta por distintos autores[53], es la de construir un orden jurisdiccional distinto de cara a resolver los problemas que surgen respecto del DIPr. Es decir, construir una jurisdicción propia, separada y distinta, libre de límites geográficos físicos. Según estos autores el crear este orden jurisdiccional supondría la resolución de la mayoría de problemas. No obstante, en mi opinión esta opción resulta demasiado compleja y por ende la creación de una norma común de DIPr parece una solución más plausible.

CAPÍTULO III: COMPETENCIA JUDICIAL INTERNACIONAL

Como resultado de la falta de un acuerdo sobre una norma común de DIPr nos encontramos ante lo que Ortega Giménez (2014, p.139) describe como un laberinto normativo de intrínseca complejidad, en cuanto se acumulan fuentes de origen diverso. Para poder salir de este "laberinto"[54] podemos servirnos de tres bloques de herramientas o instrumentos. En primer lugar, encontramos los instrumentos Europeos referidos a la determinación de la CJI en materia civil y mercantil – estos son el Reglamento Bruselas I bis (o «RBIb») y el Convenio de Lugano (o «CL») – y las normas de CJI incluidas en el RGPD como norma sectorial. Respecto del RBIb y el CL, mientas el primero resulta de aplicación a los Estados miembros de la UE, el segundo se aplica a la UE, Noruega, Suiza e Islandia. Por tanto, si bien estos tres instrumentos se refieren únicamente al ámbito europeo, nos proporcionan un punto de partida que resulta representativo de las normas de DIPr globales y nos permitirá exponer y resolver los problemas que surgen en el ámbito de la protección de datos de carácter personal[55]. Tanto el RBIb como el CL, no resultan de aplicación, en principio[56], cuando el demandado esté domiciliado en

[53] Como Damon Andrews y John Newman (2013) o David R. Johnson y David Post (1996).
[54] El internet se caracteriza por su "*naturaleza global, plurilocalizada y frecuentemente desvinculada de un determinado lugar*" (Palao Moreno, 2006, p.280), lo que dificulta sobremanera la determinación del foro de CJI.
[55] Es decir, estas normas, acompañadas por la jurisprudencia de los tribunales europeos, nos permitirán solucionar los problemas de DIPr que surgen a nivel global en cuanto ofrecen soluciones a problemas que no son únicamente europeos, sino mundiales.
[56] Podría darse el caso de que el demandado no estuviera domiciliado en un Estado miembro pero aun así resultara de aplicación el RBIb o el CL, como ocurre en el caso de los consumidores cuando la contraparte dirige sus actividades al Estado donde radica el domicilio del mismo.

un tercer Estado, por tanto en estos casos el interesado deberá acudir a las normas de DIPr de su propio Estado[57]. Por esa razón, en segundo lugar, a razón de un criterio de proximidad y por la lógica imposibilidad de analizar todas las normas de DIPr, se hará uso de la Ley Orgánica del Poder Judicial (o «LOPJ») para realizar matices[58]. Por último, la jurisprudencia estadounidense nos ofrece instrumentos de cara a resolver los problemas derivado de la determinación de la CJI, en especial respecto del foro característico de la responsabilidad extracontractual.

Por tanto, con el objetivo de determinar la CJI en materia de protección de datos se resolverá la problemática que surge respecto de los foros sustraídos de las distintas fuentes. El primero de ellos ejerce como foro general. El segundo constituye el foro propio en materia extracontractual. El tercero constituye el foro de la responsabilidad contractual y por último se encuentra el foro de la autonomía de la voluntad.

a) Relación entre normas europeas

Como breve aclaración, antes de entrar de lleno en los problemas de determinación de la CJI en materia de protección de datos, debe resolverse el problema inicial que surge como resultado de la existencia de varios preceptos normativas a nivel Europeo. Esto es, debe aclararse cual es la relación entre los foros de CJI del RBIb, RGPD y aquellos establecidos en las normativas de cada Estado miembro. En primer lugar, y de manera más clara, en virtud del artículo 6.1. del RBIb y 4.1. del CL, cuando el demando carezca de domicilio en el territorio de un Estado miembro o de Suiza, Noruega e Islandia, no resultará de aplicación ni el RBIb ni el CL, sino las normas de DIPr de cada Estado miembro. Asimismo, como explica De Miguel Asensio (2017), las normas de CJI recogidas en el artículo 79.2 del RGPD resultan complementarias respecto de las normas de CJI de cada Estado y del RBIb y el CL. Es decir, si bien el artículo 67 del RBIb, el Considerando 147 del RGPD y el propio artículo 79.2 del RGPD[59] podrían hacer pensar que las normas de CJI del RGPD priman sobre el resto, estas deben entenderse de forma complementaria.

[57] Así ocurre también respecto de los ciudadanos no miembros de la UE, que a falta de convenios supra-nacionales deberán acudir a las normas nacionales para determinar la CJI.
[58] La LOPJ nos sirve como plataforma para ofrecer soluciones desde la perspectiva estatal.
[59] Argumenta De Miguel Asensio (2017), que si bien el artículo 79.2 establece que *"[...] las acciones [...] deberán ejercitarse [...]*", en virtud del contexto, contenido y función de la norma, así como de su redacción en otras lenguas, no debe entenderse esta expresión de manera imperativa.

1. FORO DEL DOMICILIO DEL DEMANDADO

Reconocen tanto el artículo 4 del RBIb, como el artículo 2 del CL que serán competentes para conocer, como criterio general, de una controversia en materia civil y mercantil, los tribunales del domicilio del demandado. Asimismo, el artículo 22.3 de la LOPJ establece que serán competentes los tribunales españoles cuando el demandado tenga su domicilio en España. En el ámbito de la protección de los datos de carácter personal este foro conduce a hacer competentes a los tribunales del Estado donde tenga su establecimiento el responsable del tratamiento de los datos personales (Calvo Caravaca y Carrascosa González, 2017, p.1527). En este sentido se pronuncia el RGPD, que reconoce en su artículo 79.2. que "*las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento*".

1.1. Problemas

1.1.1. Identificación del sujeto infractor

Un importante problema que puede surgir en materia extracontractual[60], lo constituye el hecho de que el interesado desee emprender una acción judicial por un daño derivado de un acto de tratamiento ilícito, pero desconozca de la identidad del sujeto infractor[61] y por ende de su domicilio. Esto ocurre en mayor medida cuando aquel que realiza un acto de tratamiento ilícito es un sujeto particular que no se identifica con una entidad mayor[62]. Ante este problema la solución lógica resulta que el demandante acuda al foro del lugar del hecho dañoso propio de la responsabilidad extracontractual[63].

1.1.2. La correcta identificación del establecimiento del sujeto infractor

Aunque se conozca la identidad del sujeto infractor, podría darse el caso de que este se identifique con un establecimiento aparente y no con su establecimiento real. Ante este problema considera Ortega Giménez (2014) que la solución pasaría por permitir al interesado presentar demanda en cualquiera de los dos órdenes jurisdiccionales. No

[60] Cuando media contrato entre las partes, lógicamente a priori el interesado conocerá de la identidad del sujeto infractor.

[61] Por ejemplo, podría ocurrir que los datos médicos sobre un ciudadano alemán aparecieran en una página web, sin que el ciudadano alemán conozca la identidad del titular de la web.

[62] Peter Swire (1998) introdujo la metáfora de los elefantes y los ratones para explicar que los criterios de determinación de CJI y LA resultaban poco efectivos respecto de aquellos que pueden esconder su identidad con mayor desempeño, a diferencia de los "elefantes" que son grandes entidades que resultan fácilmente identificables.

[63] Respecto del ejemplo anterior, el ciudadano alemán podrá acudir a los tribunales alemanes.

obstante, parece más acertado seguir la lógica del Tribunal de Justicia de la UE (o «TJUE») en la sentencia del 1 de octubre de 2015, asunto C‑230/14, Weltimmo, de cara a determinar cual de los establecimientos es el real. Así, para identificar de manera correcta el establecimiento del sujeto infractor, este debe cumplir con dos características: (a) presencia de una actividad real y efectiva y (b) que esta sea ejercida mediante una instalación estable. De la misma manera se expresa el considerando 22 del RGPD que establece 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, el TJUE en la sentencia de 5 de septiembre de 2019, asunto C-28/18, Verein für Konsumenteninformation, aclaró que podrá existir un establecimiento aunque la entidad no posea una filial ni una sucursal en un Estado miembro, siempre y cuando se valore el grado de estabilidad de la instalación y la efectividad del desarrollo de las actividades en ese Estado. No obstante, esclareció que esto no significa que el mero acceso a la página web de una entidad constituya un establecimiento del responsable en un determinado Estado. Por tanto, la accesibilidad a una página web no es un foro suficiente para determinar la CJI.

1.1.3. Múltiples establecimientos y filiales

En caso de que existan varios establecimientos, de cara a determinar la CJI debemos determinar donde radica el establecimiento principal. Para ello, podemos servirnos del artículo 4, 16º del RGPD que establece que el establecimiento principal será; "*el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal*".

Respecto de las filiales, los artículos 7.5 del RBIb, 5.5 del CL y 22 quinquies c) de la LOPJ se refieren al foro de la sucursal. De esta manera, la CJI recaerá sobre el órgano jurisdiccional del lugar donde se halle la sucursal, agencia o cualquier otro establecimiento de la persona. En el ámbito concreto de la protección de datos, para determinar cuando una filial constituye un verdadero establecimiento secundario sobre el cual determinar la CJI podemos servirnos de la importante sentencia del TJUE de 13

de mayo de 2014, C‑131/12, Google Spain, S.L. En esta, el Tribunal estableció que la filial que existía de la empresa norteamericana en España constituía un verdadero establecimiento en cuanto en esta se realizaban actividades – mayoritariamente la captación de clientes – que financiaban a la empresa matriz. Por tanto, en cuanto esta filial "*constituye una parte esencial de la actividad comercial del grupo de Google y puede considerarse que está estrechamente vinculada a Google Search*"[64] constituye un verdadero establecimiento. Por ende, para determinarse cuando una filial resulta un verdadero establecimiento se deberá atender al criterio de unidad económica de las actividades (Calvo Caravaca y Carrascosa González, 2017).

1.1.4. Disociación entre el lugar del establecimiento y el lugar de tratamiento

Por último, podría ocurrir que el lugar donde radica el establecimiento no coincida con el lugar donde se realice el tratamiento de datos. A este supuesto se refirió el Tribunal Supremo de España de manera contradictoria respecto del mencionado caso Google Spain S.L. Por un lado, la sala de lo contencioso-administrativo, en la sentencia 574/2016, de 14 de marzo de 2016, sostuvo que independientemente de que una filial constituya un establecimiento, esto no implica automáticamente que en esta se realice el tratamiento de datos. Es decir, si bien a razón del dictamen del TJUE la filial en España constituía un verdadero establecimiento, desde esta no se realizaba el tratamiento de datos y por ende Google Spain no constituía el verdadero responsable del mismo, puesto que los fines y medios del mismo eran determinados por la empresa ubicada en California. Por otro, la sala de lo civil, en la sentencia 3269/2014, de 5 abril 2016, indicó que Google Spain S.L. podía ser demandada en España en cuanto el concepto de responsable de tratamiento debe entenderse en un sentido amplio. Por tanto, siguiendo la línea jurisprudencial civil, aunque el tratamiento de datos se produzca en lugar distinto a donde radica el establecimiento, la CJI podrá atribuirse al Estado donde radique ese establecimiento si el tratamiento se ha realizado en el contexto de sus actividades.

2. FORUM DELICTI COMMISSI

El artículo 7.3 del RBIb y 5.3 del CL reconocen la existencia del foro "*del lugar donde se hubiere producido o pudiere producirse el hecho dañoso*" para las controversias de

[64] Véase el Fundamento de Derecho nº46 de la sentencia.

origen extracontractual[65]. Asimismo, el artículo 22 quinquies c) de la LOPJ establece que en materia de obligaciones extracontractuales serán competentes los tribunales españoles cuando el hecho dañoso se haya producido en territorio español. Este foro comprende tanto el lugar donde se produce el hecho causal (o *locus deliciti*) como el lugar donde sobreviene el daño o resultado lesivo (o *locus damin*i) (Ortega Giménez, 2014, 169). Por tanto, aplicado al ámbito de la protección de datos personales, este foro debe entenderse como el lugar donde se haya producido o se extiendan los efectos de un tratamiento contrario a las obligaciones legales (Calvo Caravaca & Carrascosa González, 2017). La doctrina norteamericana se refiere a este foro a través del test de los efectos, considerándolo como el foro a aplicar respecto de aquellas controversias surgidas a través de internet.

2.1. Problemas

2.1.1. Determinación del lugar donde se produce el hecho dañoso[66]

La propia naturaleza de la protección internacional de los datos personales hace que resulte complejo el determinar donde se producen o materializan los efectos de un acto de tratamiento ilícito. Para resolver este problema, podemos servirnos del concepto del "centro de intereses" elaborado por la jurisprudencia europea. Encontramos su origen en la sentencia, de 7 de marzo de 1995, del antiguo Tribunal de Justicia de las Comunidades Europeas (o «TJCE»), asunto C-68/93, Shevill. En esta, el TJCE aclaró que constituirá un lugar de interés para la victima aquel lugar donde la victima sea conocida y tenga una reputación que defender. Si aplicamos este argumento a la protección de datos de carácter personal, este criterio apunta al lugar donde la victima tenga un especial interés de proteger sus datos. Varios años después, el TJUE en la sentencia de 25 de octubre de 2011, asuntos acumulados C‑509/09 y C‑161/10, eData se volvió a pronunciar para aclarar cuando la sentencia Shevill resultaba de aplicación respecto de aquellos casos en los cuales se violaba un derecho de la personalidad a través de internet. En esta sentencia el Tribunal entendió que el foro del centro de

[65] El artículo hace referencia a las "*materias delictuales o cuasidelictuales*". El TJUE en su sentencia de 27 de septiembre de 1988, asunto C-189/87, Kalfelis definió estos concepto como aquellos que abarcan todas las demandas dirigidas a exigir la responsabilidad de un demandado y que no están relacionadas con la materia contractual.

[66] Si bien la mayoría de sentencias a las que se va a hacer referencia tratan supuestos de difamación, en cuanto estas se relacionan tangencialmente con la protección de los datos (Toy & Gunasekara, 2019), nos sirven para dar solución a los problemas tratados.

intereses[67] radica en el Estado donde el dañado tiene su residencia habitual o en el Estado sobre el cual existan indicios, como el ejercicio de una actividad profesional, que manifiesten la existencia de un vínculo especialmente estrecho con el mismo. Esta decisión del TJUE se encuentra basada en el Considerando 16 del RBIb que recalca la importancia de la conexión entre el órgano jurisdiccional y el litigio para así garantizar la seguridad jurídica, en especial respecto de los " [...] *litigios relativos a obligaciones no contractuales derivadas de vulneraciones del derecho a la intimidad y de los derechos de la personalidad* [...]". Asimismo, de cara a proteger los intereses del demandado deberá entenderse este foro desde el principio de previsibilidad de las normas de CJI. Es decir, como aclaró el Abogado General Cruz Villalón, el lugar donde radica el centro de intereses será el territorio donde se ha podido prever que dicha lesión pudiera eventualmente producirse. Del mismo modo, el TJUE manifestó en la sentencia, de 17 de octubre de 2017, C-194/16, Ilsjan que "*el criterio del centro de intereses es conforme con el objetivo de la previsibilidad de las reglas para determinar la competencia, ya que permite, al mismo tiempo, al demandante identificar fácilmente el órgano jurisdiccional ante el cual puede ejercitar una acción y al demandado prever razonablemente ante qué órgano jurisdiccional puede ser demandado*"[68].

a) Tests Zippo y Calder

Igualmente, de cara a resolver el problema de la determinación del lugar donde se produce el hecho dañoso podemos servirnos de los tests Zippo y Calder[69] [70]. En la sentencia Zippo Manufacturing Co. v. Zippo Dot Com, Inc se estableció el denominado Test Zippo que tiene el objetivo de determinar cuando una página web cumple con el requisito de contactos mínimos respecto de un determinado Estado[71]. Es decir, este test busca determinar el grado de interactividad entre una página web y un determinado territorio de cara a establecer la competencia judicial. De esta manera, las páginas web son categorizadas como activas o pasivas. Cuando una página web es activa respecto de

[67] En palabras del Abogado General Cruz Villalón, la justificación de este foro la encontramos en que el orden jurisdiccional que conozca en virtud de este estará *"en mejor situación para analizar la tensión de los intereses de juego"*.

[68] Véase el punto nº 35 de la citada sentencia.

[69] Ambos tests fueron desarrollados por la jurisprudencia americana de cara a determinar la CJI respecto de los casos de responsabilidad extracontractual derivados de daños producidos a través de internet.

[70] Estos tests deben entenderse como enmarcados dentro del concepto de "contactos mínimos" que el *Due Process Clause* de la Constitución Americana establece para determinar la competencia de los tribunales (Gladstone, 2003). En Canadá se hace referencia a una "conexión real y sustancial" (Geist, 2001).

[71] Este test también fue aplicado por los tribunales canadienses, como por ejemplo en el caso Braintech Inc. contra Kostiuk.

una determinada jurisdicción, esta podrá conocer de las controversias surgidas respecto de la misma. Por el contrario, cuando la página sea considerada como pasiva no podrán entrar a conocer los distintos órganos jurisdiccionales. La importancia de este test radica en que determina que la mera accesibilidad a cierto contenido en internet no equivale a CJI. No obstante, este test no resulta muy esclarecedor respecto de la protección de datos de carácter personal por dos razones. En primer lugar, porque tiene un ámbito de aplicación limitado que se refiere únicamente a la información y contenido publicado en las páginas web. Y en segundo lugar, porque la responsabilidad extracontractual que surge respecto de la protección de datos no tiene porque ser visible. Es decir, la vulneración del derecho a la protección de datos de carácter personal no siempre se produce a través de la publicación de información en una página web. Como explican Damon Andrews y John Newman (2013), el daño que se produce respecto de los datos en la mayoría de los casos responde a acciones que se producen sobre los mismos. Esto es, los daños derivan de los actos de tratamiento per se. En consecuencia, el test de los efectos o test de "Calder"[72] nos ofrece una mejor herramienta de cara a determinar donde se producen los efectos respecto de un acto de tratamiento ilícito. Este test no se centra en determinar el grado de interactividad de las páginas web sino en determinar donde se producen los efectos de un hecho dañoso. Si bien este caso se refería a una acción de difamación, nos sirve igualmente para determinar el lugar donde se producen los efectos de un acto de tratamiento dañoso[73]. Esta doctrina sostiene que la competencia judicial recaerá sobre el foro al cual se dirigieron los actos ilícitos del demandado, sabiendo que estos causarían un daño al demandante en este lugar (Geist, 2001, p.27). Es decir, será competente para conocer de una determinada controversia el orden jurisdiccional donde se producen los daños para el demandante. Por tanto, podemos observar un paralelismo entre el criterio del centro de intereses europeo y el test de Calder estadounidense[74].

[72] Este test tiene su origen en la decisión del Tribunal Supremo de los EEUU de 1984 en el caso Calder c. Jones.

[73] Señala Michal Geist (2001) que esta doctrina en un sentido amplio está siendo aplicada a otras áreas como la propiedad intelectual y las disputas comerciales, lo que significa que también podrá ser aplicada al ámbito de la protección de datos.

[74] El test de Calder también está siendo aplicado fuera de EEUU. En la sentencia Dow Jones & Co. contra Gutnick, el Tribunal Superior de Australia se declaró competente para conocer de una difamación producida en una web americana en cuanto el señor Gutnick desarrollaba su vida social y empresarial en Victoria (Toy y Gunasekara, 2019).

2.1.2. Disociación entre el locus delicti y el locus damni

No resulta extraño en el contexto de las actividades realizadas a través de internet que el lugar donde se hubiera producido el acto de tratamiento ilícito y el lugar donde se materialicen los efectos del mismo difieran. En estas ocasiones surge el problema de determinar que orden jurisdiccional resultará competente para conocer de la responsabilidad extracontractual. El TJCE se refirió a este problema en la sentencia de 30 de noviembre de 1976, C-21/76, Mines de potasse. En esta se acogió la tesis de la ubicuidad (o *Principle of Ubiquity*) que viene a establecer que el demandante podrá optar por presentar la demanda o bien en el lugar donde se ha materializado el daño o en el lugar donde se realizó el hecho causal que lo generó. Ahora bien, cuando la demanda se interpone en el lugar del hecho causal, el tribunal designado podrá conocer de la totalidad del daño, independientemente de donde se materialice el mismo. Sin embargo, si se opta por el foro del lugar donde se produce el daño, distinto de donde se produjo el hecho causal, el órgano jurisdiccional correspondiente solo podrá conocer de los daños producidos en ese país exclusivamente[75]. Por consiguiente, podrá el demandante optar por presentar reclamación por la totalidad del daño en el Estado miembro donde se produjo el hecho dañoso o de manera parcial en cada Estado donde se materialice el daño. De esta manera, la jurisprudencia europea traspuesta al ámbito de la protección de los datos, significaría que el interesado podría interponer demanda por la totalidad del daño causado en el lugar donde se realizó el acto de tratamiento ilícito, o en caso de que los efectos se extendieran en varios Estados podrá optar por presentar demanda en cada uno de esos Estados hasta el límite de los efectos que se hayan producido en cada uno.

2.1.3. El problemático efecto expansivo

Un importante problema que surge como consecuencia de la naturaleza de internet constituye el hecho de que puede argumentarse que los efectos de un hecho dañoso pueden extenderse a cualquier rincón del mundo[76] (Schultz, 2008). Es decir, en cuanto la mayoría de actos de tratamiento ilícito se realizan a través de internet, podría argumentarse que debido a la inexistencia de fronteras en la red, los efectos de tal acto pueden extenderse a cualquier país del mundo. Esto se debe a que resulta muy complejo

[75] Del mismo modo se pronunció el TJUE en la mencionada sentencia Shevill.
[76] Esto daría lugar a que se diera el fenómeno de *forum shopping*, en cuanto el demandante optaría por presentar demanda en aquel Estado donde el régimen le resultara más favorable.

el trazar una línea para determinar donde se producen efectos y donde no[77]. Para resolver y evitar este problema podemos servirnos de los criterios de *targeting*[78] y *filtering* propuestos por Thomas Schultz (2008). El criterio de *targeting* establece que para que una actividad produzca efectos en un determinado territorio debe estar destinada a producir efectos en el mismo. Por tanto, cuando se produzca un acto de tratamiento ilícito de datos deberá determinarse donde esta destinado a producir efectos. Este criterio también puede ser entendido desde el principio de la razonabilidad (HCCH, 2002). Es decir, donde resulta razonable o previsible que un determinado acto ilícito de tratamiento produzca efectos. Respecto del criterio de *filtering*, Schultz (2008) considera que para evitar que surja el problema del efecto expansivo del foro *delicti comissi* los distintos operadores de internet deberán aplicar filtros destinados a limitar el alcance de sus acciones. No obstante, este último criterio resulta contrario a la libre circulación de datos garantizada dentro del EEE por el RGPD respecto de los datos personales y por el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la UE. Del mismo, a nivel global el sistema de *filtering* restringe la libre circulación de datos, por tanto parece más adecuado limitar el efecto expansivo de este foro a través únicamente del *targeting*.

2.1.4. ¿Falta de utilidad?

Sostiene parte de la doctrina[79] que parte de este foro no posee efecto útil en cuanto en muchas ocasiones hace competentes de manera sistemática a los tribunales del Estado donde el responsable tiene su domicilio, desembocando en los problemas anteriormente expuestos. Es decir, este foro puede superponerse al foro del lugar del establecimiento del responsable en cuanto resulta lógico que se suponga que el lugar donde se produce el hecho dañoso coincide con el lugar del establecimiento del responsable, en cuanto se presupone que es el lugar donde se realiza el tratamiento de datos. Por tanto, este foro no debe entenderse desde la perspectiva del domicilio del demandado, sino en

[77] Por ejemplo, en el supuesto de que una empresa utilizará los datos que ha recabado de un cliente sin obtener su consentimiento para elaborar anuncios publicados en sus páginas web, accesibles desde cualquier parte del mundo, resulta complejo determinar en que Estado en concreto se están materializando los efectos de tal acto ilícito o si los efectos se extienden a la totalidad del planeta.

[78] Este criterio es aplicado por la jurisprudencia americana (Geist, 2001) por ejemplo, en la sentencia Bancroft Masters, Inc. contra Augusta National Inc. Asimismo, el proyecto de jurisdicción en internet del colegio de abogados de EEUU (2000) propuso este sistema para abordar la cuestión de la jurisdicción en internet.

[79] Así lo creen Calvo Caravaca, Carrascosa González (2017) y Ortega Giménez (2014).

consonancia con el concepto del centro de intereses. Lo que supondrá, de acuerdo con el principio *favor laesi*, que en la mayoría de las casos la CJI recaerá sobre el foro del domicilio del demandante[80]. Este, se encuentra reconocido de manera subsidiaria en el artículo 79.2 del RGPD[81].

3. FORO DEL LUGAR DEL CUMPLIMIENTO DE LA OBLICACIÓN

El artículo 7.1 a) del RBIb y 5.1 a) del CL reconocen el foro del lugar "*en el que se haya cumplido o deba cumplirse la obligación que sirva de base a la demanda"* en materia contractual. Respecto de la protección de los datos de carácter personal, los criterios de conexión en materia contractual solo podrán implementarse cuando el objeto del contrato o alguna de las cláusulas del mismo hagan referencia a la protección de datos de carácter personal[82].

3.1. Problemas

3.1.1. Determinar el tipo de contrato

El primer problema lo constituye el hecho de determinar si los contratos en materia de protección de datos constituyen en general contratos de compraventa de mercaderías, de prestación de servicios u otro tipo de contratos. Esto resulta relevante en cuanto en virtud del artículo 7.1 del RBIb y 5.1 del CL el foro resultará bien el lugar donde hayan sido o deban ser entregadas las mercaderías, el lugar donde hayan sido o deban ser prestados los servicios o el lugar en el que se haya cumplido o deba cumplirse la obligación. Ante esta incógnita, con carácter general puede afirmarse que la mayoría de contratos en materia de protección de datos de carácter personal se refieren a servicios contratados que implican el tratamiento de los mismos. No obstante, nada impediría que el foro del contrato quedará enmarcado dentro de los supuestos del artículo 7.1 a) o 5.1 a) del RBIb y CL.

---

[80] Como ha sido mencionado anteriormente, puede darse el caso de que el centro de intereses se encuentre en un lugar distinto donde exista un vínculo, como puede ser el lugar donde se realice la actividad profesional.

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

[82] Por ejemplo, el cedente y cesionario de datos suscriben contrato para la transferencia internacional de datos. Este contrato hace referencia a la protección de datos y a la responsabilidad de las partes. Si se incumple el mismo, el interesado aún sin ser parte de este contrato podrá interponer demanda por incumplimiento contractual.

3.1.2. Contratos de consumo

Asimismo, puede ocurrir que se suscriba contrato de consumo cuyo objeto o disposiciones se refieran a la protección de datos de carácter personal. Los artículos 17.1 del RBIb y 15.1 del CL reconocen la condición de consumidor a la persona que adquiere un bien o un servicio "*para un uso que pueda considerarse ajeno a su actividad profesional*". El concepto de consumidor debe entenderse de manera restrictiva, lo que significa que no constituye una cualidad subjetiva sino que para determinarse debe atenderse a la posición de las partes y a la finalidad del contrato[83]. Por tanto, como ejemplo respecto de la protección de datos, será un consumidor aquel que contrata un servicio de análisis genético que involucra el tratamiento de datos de carácter personal.

Respecto de la identificación de un interesado como consumidor en materia de protección de datos surgen principalmente dos problemas. En primer lugar, la mayoría de contratos de suscripción a redes sociales son duales, es decir tienen tanto fines personales como profesionales. Respecto de los mismos, solo cuando la finalidad profesional constituya una parte marginal del contrato, el contratante tendrá la consideración de consumidor (Garcimartín Alférez, 2019, p.128). Asimismo, el TJUE en la sentencia de 25 de enero de 2018, C‑498/16, Schrems contra Facebook, afirmó que si un individuo contrata un servicio como consumidor, independientemente de que a posteriori su actividad pase a ser profesional, mantendrá su condición como consumidor. En segundo lugar, resulta complejo el determinar cuando de conformidad con el artículo 17.1 c) del RBIb, el titular de datos ha contraído contrato con un profesional que dirige su actividad al Estado miembro donde tiene su domicilio. Para hacer frente a esta incógnita, el TJUE en sentencia de 7 de diciembre de 2010, C-585/08, Pammer, redactó una lista[84] no exhaustiva de criterios destinados a aclarar cuando un profesional dirige sus actividades a un determinado Estado.

---

[83] Así lo estableció el TJUE en la sentencia de 14 de febrero de 2019, C-630/17, Milivojević.

[84] Párrafo nº 93 de la citada sentencia: [...] *el carácter internacional de la actividad, la descripción de itinerarios desde otros Estados miembros al lugar en que está establecido el vendedor, la utilización de una lengua o de una divisa distintas de la lengua o la divisa habitualmente empleadas en el Estado miembro en el que está establecido el vendedor, con la posibilidad de reservar y de confirmar la reserva en esa otra lengua, la mención de números de teléfono con indicación de un prefijo internacional, los gastos en un servicio de remisión a paginas web en Internet con el fin de facilitar el acceso al sitio del vendedor o al de su intermediario a consumidores domiciliados en otros Estados miembros, la utilización de un nombre de dominio de primer nivel distinto al del Estado miembro en que está establecido el*

En conclusión, si finalmente el interesado cumple con todos los requisitos y es considerado como consumidor, en virtud del artículo 18 del RBIb y 16 del CL, este podrá elegir entre interponer demanda en el lugar del establecimiento del demandado o en el lugar de su domicilio, mientras que la contraparte solo podrá presentar demanda en el domicilio del consumidor.

4. SUMISIÓN EXPRESA O TÁCITA

El RBIb en sus artículos 25 y 26 y el CL en sus artículos 22 y 23 se refieren al foro de la sumisión tácita y expresa. Asimismo, la LOPJ en su artículo 22 bis establece que serán competentes los tribunales españoles cuando las partes así lo hayan pactado, expresa o tácitamente. La diferencia entre los tipos de sumisión radica en que mientras en la sumisión expresa existe un acuerdo entre las partes anterior o posterior al surgimiento de la controversia, la sumisión tácita se produce como consecuencia del comportamiento procesal de las partes[85]. En cuanto estos foros derivan del principio de la autonomía de las partes, priman sobre el resto.

4.1. Problemas

4.1.1. Falta de relevancia de la sumisión expresa respecto del ámbito extracontractual

En primer lugar, resulta debatible la falta de relevancia de la sumisión expresa respecto de los supuestos de responsabilidad extracontractual derivados de un tratamiento ilícito de los datos. Esto se debe a la naturaleza de la relación entre las partes, en cuanto como no media contrato entre las mismas, resulta improbable (Ortega Giménez, 2014, p.145) pero no imposible[86] que se produzca un acuerdo entre las mismas sobre donde litigar. No obstante, nada impediría que se produjera la sumisión tácita de alguna de las partes una vez surgida la controversia.

---

vendedor y la mención de una clientela internacional formada por clientes domiciliados en diferentes Estados miembros".

[85] Es decir, si el demandante presenta demanda y esta es contestada por el demandado se entiende que ha aceptado tácitamente la jurisdicción de ese órgano judicial.

[86] Podría ocurrir por ejemplo que, sin mediar contrato, el responsable del tratamiento utilizará los datos personales de un individuo para una finalidad no autorizada. En caso de que el interesado tuviera conocimiento de ello podrán las partes acordar que tribunales conocerán de la controversia.

4.1.2. Particularidades de los contratos de consumo

En aquellos casos en los cuales exista un contrato de consumo, solo resultarán válidas las clausulas de sumisión que cumplan con los requisitos del artículo 19 del RBIb. Es decir, las cláusulas deberán: (i) ser acordadas con posterioridad al nacimiento del litigio, (ii) referirse a órganos jurisdiccionales distintos de los indicados en la sección 4ª del Reglamento y (iii) si ambas partes poseen residencia o domicilio habitual en el mismo Estado miembro, la CJI deberá recaer en los tribunales de este, salvo que se encuentre prohibido por ley. Por ende, si no se cumplen con estos requisitos, no cabrá la sumisión y la CJI, en virtud del artículo 18 RBIb, recaerá sobre el foro del domicilio del consumidor.

4.1.3. La protección de la parte más débil

Grandes empresas, como Facebook, Google o Amazon, utilizan de manera recurrente cláusulas de elección de foro y ley para limitar la capacidad de los tribunales de conocer las demandas relacionadas con los servicios que prestan (Toy & Gunaserkara, 2019). Por ejemplo, las condiciones de servicio[87] de Facebook establecen que si no eres considerado como consumidor "*aceptas que la reclamación debe resolverse en un tribunal competente en la República de Irlanda y que las leyes de dicho país regirán estas Condiciones y cualquier reclamación (independientemente de las disposiciones relativas a conflictos de derecho)".* Pues bien, para determinar si las cláusulas de sumisión resultan válidas o no deberá acudirse al derecho del Estado designado en el acuerdo, como sostiene el considerando número 20 del RBIs. Por ejemplo, en España el artículo 54 de la Ley de Enjuiciamiento Civil establece que "*No será válida la sumisión expresa contenida en contratos de adhesión, o que contengan condiciones generales impuestas por una de las partes, o que se hayan celebrado con consumidores o usuarios*". Por tanto, desde el punto de vista del sistema español esta cláusula no resultaría válida. Asimismo, deberá atenderse al método utilizado para determinar la sumisión a un determinado foro, debiendo este resultar claro para las partes. Así lo establecieron los tribunales del distrito central de California, en la sentencia Ticketmaster Corp. c. Tickets.com. En esta, los tribunales instauraron que la mera inclusión de una cláusula de selección de foro u otra cláusula jurisdiccional dentro de

[87] Véase https://www.facebook.com/legal/terms. [Último acceso 9/04/2020].

los términos y condiciones no resulta válido si no genera una suficiente atención en el usuario.

5. MODELO DE ARMONIZACIÓN Nº1

Como ha sido probado, los foros de CJI en su concepción tradicional adolecen de numerosos problemas en relación con la protección de datos de carácter personal (véase un esquema de los problemas y soluciones en el anexo nº 2.). Esto se produce a razón de la naturaleza del propio derecho, en cuanto constituye un derecho personalísimo que se desarrolla en relación con las actividades de internet donde las fronteras entre países quedan desdibujadas. Por ello, el sistema de determinación de la CJI debe ir más allá de la concepción territorial de Estado. De esta manera, no debe excluirse por completo la utilización de los foros tradicionales, sino que deben adaptarse para responder a las necesidades especificas de la protección de datos de carácter personal. Asimismo, en consonancia con autores como Ortega Giménez (2014), (2018) y Reema Shah (2015) el foro del centro de intereses debe fomentarse como foro más apropiado en el ámbito de la protección de datos en cuanto: (i) resulta previsible[88] para las partes y por ende aporta seguridad jurídica, (ii) es justo[89], (iii) ofrece una mejor protección del derecho personalísimo del interesado y (iv) favorece la unidad de acciones. Asimismo, este foro conforme a la teoría general de Lowenfeld (1994) posee un carácter más razonable y equitativo. El resto de foros, si bien pueden ser utilizados como complementarios al foro del centro de intereses, adolecen de mayores deficiencias. En primer lugar, el foro de los efectos entendido en sentido general, resulta demasiado amplío[90] y fomenta la multiplicidad de procedimientos[91]. Por su parte, el foro del domicilio del demandado, podría suponer que el interesado tenga que litigar en un foro lejano, con todo lo que ello

[88] El propio TJUE en la sentencia eData estableció que "l*a competencia del órgano jurisdiccional del lugar en el que la presunta víctima tiene su centro de intereses es conforme con el objetivo de la previsibilidad de las normas de competencia […] también con respecto al demandado, dado que el emisor de un contenido lesivo puede, en el momento de la publicación en Internet de ese contenido, conocer los centros de intereses de las personas que son objeto de éste […]".*

[89] A razón de las más habituales relaciones extracontractuales, el demandante no puede realizar a priori ningún acto para evitar que se produzca el daño.

[90] En especial, respecto del desarrollo del Cloud Computing en cuanto consideran Calvo Caravaca y Carrascosa González (2017, p.1534), apoyándose en la sentencia de 19 de septiembre 1995, asunto C-364/9, Marinari, que resultará muy complejo el determinar el lugar donde se ha producido el tratamiento de los datos.

[91] Este foro puede dar lugar a que se interpongan varias demandas en caso de que los efectos de un determinado acto se extiendan por varios países. Por ello en virtud del principio de acumulación de acciones debe promoverse el foro del centro de intereses.

supone[92]. Por otro lado, el foro de la sumisión expresa supone el riesgo de que el interesado pueda quedar desprotegido. Por último, el foro de las responsabilidad contractual, no resulta apropiado para los contratos en materia de protección de datos.

En conclusión, en cuanto este ensayo promueve la creación de una regulación sustantiva común en materia de protección de datos y en su defecto una norma común de DIPr, de conformidad con la International Law Association (2018) y Maja Brkan (2015), se aboga por la redacción de un instrumento internacional que se refiera a la determinación de la CJI de la siguiente manera:

> **Artículo A. Competencia judicial internacional en materia de protección de datos de carácter personal.**
>
> 1. La presente disposición resulta de aplicación para la determinación de la jurisdicción en materia civil y mercantil por violaciones del derecho a la protección de datos o privacidad tanto respecto de las obligaciones contractuales como de las extracontractuales.
>
> 2. Podrá el interesado interponer demanda contra el responsable o encargado de tratamiento en el foro de su centro de intereses, siempre y cuando el demando pudiera haber previsto razonablemente el mismo. En su defecto, será competente para conocer de la controversia el tribunal donde radique el establecimiento principal del responsable del tratamiento.
>
> 3. Por su parte, el responsable o encargado de tratamiento podrá interponer demanda sólo en el foro del lugar en el cual la contraparte se encuentre domiciliada.
>
> 4. Respecto de la elección del foro, esta se permitirá siempre y cuando resulte favorable para el interesado.

CAPÍTULO IV: LEGISLACIÓN APLICABLE

En el DIPr, entendido en un sentido amplio, existe una clara distinción entre el ámbito de la determinación de la CJI y LA. No obstante, en el ámbito de la protección de datos, como materia administrativa, esta distinción resulta particularmente estrecha (Kuner, 2010, p.179), lo que significa que en muchas ocasiones resulta de aplicación la *lex fori*.

[92] El interesado podría verse obligado a litigar en un Estado donde desconoce el idioma y las normas procesales. Asimismo, supondría un aumento de costas para el demandante el hecho de tener que desplazarse hacia Estados lejanos.

En otra nota, en cuanto muchos problemas tratados en el capítulo anterior se repiten respecto de la LA, no se hará referencia a los mismos, procediéndose a exponer únicamente los problemas propios relacionados con la determinación de la LA.

1. DETERMINACIÓN DE LA LEY APLICABLE

Al igual que en el capítulo anterior, el proceso para determinar la LA en el ámbito de la protección de datos resulta complejo. Para dar respuesta a la incógnita de que ley en materia de protección de datos deberá aplicarse al fondo de un asunto deberán analizarse tres bloques complementarios entre sí. En primer lugar, se expondrá, grosso modo, el ámbito de aplicación de las leyes en materia de protección de datos. En segundo lugar, se analizará el sistema de resolución de conflictos de leyes europeo, como ilustrativo de los problemas que surgen a nivel global en materia de protección de datos. Por último, se analizarán los sistemas de determinación de la LA español y estadounidense, para así intentar representar a grandes rasgos distintos sistemas de conflictos de leyes nacionales.

1.1. Ámbito de aplicación de las leyes de protección de datos

Antes de entrar a analizar los distintos sistemas de determinación de la LA, deben analizarse los ámbitos de aplicación de las leyes de protección de datos de cara a comprender como surge una parte de los conflictos de leyes. De esta manera, se ha observado que existe una "*tendencia a que las reglamentaciones locales de protección de datos traten de captar cualquier actividad dirigida a los residentes locales, independientemente de la ubicación real del negocio*" (UNCTAD, 2016). Es decir, de manera más o menos intensa, la mayoría de legislaciones en materia de protección de datos poseen cierta tendencia extraterritorial. Si bien este fenómeno ha sido ampliamente criticada por los expertos, cuenta con cierta legitimidad. Es decir, si los Estados no extienden su protección de datos a la conducta de las partes extranjeras, no están proporcionando una protección efectiva a sus ciudadanos (Svantesson, 2015, p.21). Esto es, la aplicación extraterritorial de las normas de protección de datos

pretende proteger los derechos fundamentales[93] de los ciudadanos de un determinado Estado en un mundo globalizado[94].

En concreto, el artículo 3 del RGPD establece que el Reglamento resultará de aplicación cuando: (a) el tratamiento se haga en en el contexto de las actividades de un establecimiento en la Unión, (b) el tratamiento se refiera a residentes en la Unión por parte de un responsable ubicado en un tercer Estado si sus actividades; están relacionadas con la oferta de bienes o servicios[95] o controlan su comportamiento[96] o (c) el responsable se encuentre en un lugar en el que el derecho de los Estados miembros sea de aplicación en virtud del derecho internacional público. Por tanto, de la lectura de este artículo puede deducirse claramente la dimensión extraterritorial del mismo. Ahora bien, como ha sido mencionado, esta característica no es solo propia de la legislación europea. En EEUU, el *US Children's Online Privacy Protection* se aplica a cualquier página web que recopile información sobre niños americanos, independientemente de la ubicación de los responsables del tratamiento. Asimismo, el *US Federal Trade Comission's Telemarketing Sales Rule* también se aplica a vendedores y tele operadores que operen fuera de los EEUU si estos contactan con un consumidor ubicado en EEUU. Igualmente, el artículo 5B del Privacy Act (1988) de Australia establece que el Acto resulta de aplicación respecto de "*un acto realizado, o una práctica llevada a cabo, fuera de Australia y los Territorios exteriores por una organización, o un pequeño operador empresarial, que tenga un vínculo australiano*".

Por ende, si bien en cierta medida puede justificarse el ámbito de aplicación amplio de las normas sobre protección de datos, una aplicación extraterritorial abusiva de las

[93] Cedric Ryngaert, (2015) afirma que la UE puede llegar a tener hasta una obligación de proteger de manera extraterritorial el derecho a la protección de datos en cuanto este constituye un derecho fundamental reconocido en su Carta.

[94] Explicado en otras palabras, Ana Gascón (2019, p.415) establece que "*el objetivo de este amplio alcance territorial es que la protección "viaje" con los datos personales a donde quiera que vaya en una sociedad globalizada donde los datos cruzan las fronteras con un simple clic".*

[95] El considerando 23 aclara que la mera accesibilidad no constituye un criterio para determinar la aplicación del Reglamento, sino que opta por un criterio de *targetting* por el cual en virtud de ciertos indicadores (como la lengua o la moneda) debe poder deducirse que efectivamente el responsable de tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

[96] Asimismo, el considerando 24 establece que "*para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes".*

mismas no resulta razonable por dos razones. En primer lugar, porque en virtud de la misma surgen numerosos conflictos de leyes. Es decir, en cuanto los ámbitos de aplicación de las normas resultan muy amplios, respecto de una misma controversia surgiría la incógnita de determinar qué ley resultará de aplicación al fondo del asunto. Asimismo, la aplicación extraterritorial abusiva de las normas no resulta razonable en cuanto no es posible que los responsables del tratamiento de datos ajusten su conducta a todas las leyes de todos los países del mundo con los que entran en contacto. Si este fuera el caso, se produciría el fenómeno que Thomas Schultz (2008, p.811) denomina como el "*slowest ship in the convoy problem*". Este supondría que los distintos responsables del tratamiento acabarían cumpliendo con la ley más restrictiva del mundo (*the slowest ship*) para así evitar futuras disputas. Por tanto, sería el orden jurisdiccional más restrictivo el que acabaría por regular la protección de datos a nivel global. No obstante, de acuerdo con la opinión de reputados autores como Thomas Schultz (2008) y Maja Brkan (2016), considero que este último problema no resulta tan conflictivo en la práctica en cuanto los Estados no pueden hacer cumplir sus leyes fuera de su territorio. Es decir, como afirma Svantesson (2015, p.232) respecto del caso concreto del RGPD, éste "*muerde más de lo que puede masticar*".

En conclusión, de cara a reducir las conflictos de leyes, los Estados deben abogar por alcanzar un equilibrio que permita garantizar un nivel de protección adecuado pero que a su vez limite la aplicación excesivamente extraterritorial de sus normas. Una manera de llevar a cabo esto sería a través de una definición más concreta y específica de los ámbitos de aplicación de las normas[97], para evitar así que una ley regional o nacional se convierta básicamente en una norma global[98]. Como consecuencia, el nivel de protección de los datos de los individuos decaería hasta cierto punto, pero la seguridad de los operadores internacionales aumentaría, lo que de alguna manera equilibraría la balanza.

[97] Consideran Paul de Hert y Michal Czerniawski (2016) que en particular el artículo 3.2 a) del RGPD necesita de una mayor especificación.
[98] Shakila Bu-Pasha, (2017, p.7) se refiere en concreto al RGPD, sosteniendo que resulta de gran importancia el definir su ámbito de aplicación pues en virtud el mismo tiene el potencial de convertirse en una ley internacional.

1.2. Determinación de la LA en la Unión Europea

La entrada en vigor del RGPD supuso que la UE pasará de tener múltiples leyes en materia de protección de datos armonizadas por una directiva, a que existiera una única ley común a nivel europeo. Por tanto, si bien la derogada Directiva 95/46/CE, recogía en su artículo 4[99] un sistema de determinación de la LA, este no fue incluido en el Reglamento puesto que *prima facie* no deberían surgir problemas respecto de la determinación de la *lex causae*[100]. No obstante, aun existiendo esta ley común, en determinados supuestos todavía resulta necesario determinar la LA. La organización pública europea, European Digital Rights (2016) ha identificado 51[101] "flexibilidades"[102]. Éstas, se refieren a cuestiones o asuntos sobre los cuales los Estados pueden legislar, lo que supone que serán puntos donde las legislaciones nacionales podrán entrar en conflicto. Como ejemplo, el artículo 82 del RGPD reconoce el derecho a recibir una indemnización en caso de incumplimiento de las disposiciones del Reglamento. No obstante, no especifica el método de cálculo de esta, ni los criterios de relación causal. Por tanto, deberá acordarse que ley nacional resultará de aplicación para determinar estos extremos. Así pues, el problema lo constituye el hecho de que una vez determinada la aplicación del RGPD, respecto de determinados aspectos surgirá la incógnita de determinar la ley del Estado miembro que resultará de aplicación. Esta incertidumbre resulta especialmente problemática y puede llegar a socavar la labor

[99] Este establecía: "*Derecho nacional aplicable. 1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable; b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público; c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea. 2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento*".

[100] Es decir, si surge una controversia internacional en materia de protección de datos y la CJI recae sobre un órgano judicial o administrativo de la UE, si se verifica que esa actividad de tratamiento entra dentro del ámbito de aplicación del RGPD, a priori el Reglamento resultará de aplicación para resolver del fondo el asunto sin que surjan problemas mayores respecto de la determinación de la LA.

[101] El número exacto varía, dependiendo de que criterio se escoja. Por ejemplo, Jiahong Chen (2016) identificó 37 asuntos donde los Estados pueden legislar. De otra manera, Amberhawk Training (2016) identificó 61.

[102] Estas flexibilidades podrán suponer un mayor o menor riesgo de conflicto. Asimismo, podrán ser de tres tipos: (i) especificar, (ii) complementar o (iii) reemplazar (Yuliyanova Charakova, 2019).

unificadora del RGPD. Ante este problema, existen tres posibles soluciones: (i) realizar un ejercicio de analogía respecto de las disposiciones que regulan la competencia de las APD, (ii) acudir a las normas generales de conflicto de la UE o (iii) directamente proceder a analizar las normas de conflictos de leyes de los Estados miembros.

1.2.1. Solución nº1: Interpretación del RGPD

Una posible solución a falta de una norma de conflictos de leyes la podemos encontrar a través de una interpretación extensiva de los términos del Reglamento. Para ello, debemos acudir al artículo 56 del RGPD el cual establece que "*la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado*". Por tanto, en consonancia con Lukas Feiler, Nikolaus Forgó y Michaela Weigl (2018, p.577), en aquellos casos en los cuales exista una autoridad de control principal en virtud del artículo 56.1, será la ley donde radique la misma la LA al fondo del asunto. Mientras que en aquellos casos, en los cuales la controversia no verse sobre transferencias internacionales de datos y por ende no se haya estipulado la existencia de una autoridad de control principal deberá atenderse a las normas nacionales de cada Estado miembro de cara a determinar la LA. No obstante, Jiahong Chen (2016, p.322) va un paso más allá y sostiene que con carácter general, independientemente de que la controversia verse o no sobre una transferencia internacional de datos, por analogía la LA será la del Estado donde radique el establecimiento principal del responsable de tratamiento[103] por radicar en éste la ADP competente. Es decir, como afirma Kuner (2010, p.180) en cuanto en la práctica la mayoría de APD equiparan su jurisdicción a la LA[104], los criterios de determinación de la competencia de estas servirán para determinar la LA.

[103] El RGPD construyó el sistema de "ventanilla única" de cara a resolver los supuestos de choque de competencias entre APD. Este otorga competencia a la ADP donde radique el establecimiento principal (en virtud de los artículos 4.16º y considerando 36). Por otro lado, el resto de autoridades recibirán la consideración de interesadas (conforme al artículo 4.22º del RGPD). Sí aún así no se llega a un acuerdo para determinar que APD resultará competente, será el Comité Europeo de Protección de Datos quien adopte una decisión vinculante (en virtud del artículo 63 del RGPD).

[104] La sentencia Weltimmo del TJUE estableció que en relación con la aplicación jurídico-publica de la legislación sobre protección de datos, y en particular del ejercicio de la potestad sancionadora, el criterio de base es la correlación entre la LA y la ADP nacional competente. Por tanto, la capacidad de actuación de una ADP de un Estado miembro será limitada cuando resulte de aplicación la ley de otro Estado miembro por estar establecido sólo allí el responsable de tratamiento.

En conclusión, en virtud de la opinión de estos autores, para determinar la LA deberá estarse a los criterios de determinación de la APD competente, los cuales apuntan al criterio de conexión del establecimiento del responsable. Por tanto, en principio, resultará aplicable la ley del lugar donde radique el establecimiento del responsable. De esta manera, resultaría conveniente agrupar la cuestión de la determinación del derecho aplicable con la precisión de la competencia de la autoridad supervisora principal, eligiendo el establecimiento principal como único factor de conexión. No obstante, el TJUE todavía no se ha pronunciado al respecto, en cuanto no ha transcurrido un lapso de tiempo suficiente desde la entrada en aplicación del Reglamento y asimismo, no han surgido problemas sustantivos relativos a esta interpretación extensiva.

1.2.2. Solución nº2: Reglamentos Roma I y II

A nivel europeo encontramos dos Reglamentos referidos a la determinación de la LA, el Reglamento (CE) No 593/2008 del Parlamento Europeo y del Consejo de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales (o «RR-I») y el Reglamento (CE) No 864/2007 del Parlamento Europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales (o «RR-II»).

a) Obligaciones contractuales

Como regla general, el artículo 3 del RR-I reconoce la libertad de las partes para elegir la LA. A falta de elección, se deberá estar a lo dispuesto por el artículo 4, siempre y cuando el contrato no constituya un contrato de consumo. Respecto a estos últimos, la LA será la del lugar donde el demandado tenga su residencia habitual[105] excepto que las partes eligieran otra ley que resultará más favorable para el consumidor.

Ahora bien, la relación entre el ámbito de aplicación del RGPD y las disposiciones del RR-I puede hacer que surjan problemas. Por ejemplo, en el caso de que una empresa americana ofreciera servicios online dirigidos a niños irlandeses, el RGPD regularía el tratamiento de datos. Si surgiera una controversia respecto de la edad mínima de los niños irlandeses para dar su consentimiento[106], en virtud del artículo 6.1 del RR-I, sería

[105] Por tanto, en materia de consumidores, la LA resultará la *lex fori*. En el resto de los casos, en virtud del artículo 4 del RR-I, con carácter general resultará aplicable la ley del país donde tenga su residencia habitual la parte que deba realizar la prestación característica del contrato.

[106] El artículo 8 del RGPD, reconoce la facultad de los Estados para establecer la edad mínima de consentimiento siempre y cuando no sea inferior a 13 años.

la ley irlandesa la cual determinará la edad mínima. No obstante, si niños alemanes accedieran también a este servicio, resultaría de aplicación el RGPD al tratamiento de sus datos, pero de cara a determinar la edad mínima de consentimiento en virtud del artículo 4.1 b) del RR-I, la LA será la americana. Es decir, en cierta medida los criterios esbozados en el RR-I no resultan del todo adecuados en materia de protección de datos, en cuanto carece de lógica que el tratamiento quede regulado por el RGPD pero al mismo tiempo la ley de terceros Estados regule determinados aspectos del mismo. Ante esta problemática, resultaría pertinente establecer unos criterios de determinación de la LA propios del ámbito de la protección de datos.

Respecto de las cláusulas de elección de LA, la doctrina se encuentra dividida acerca de la posibilidad de que las partes acuerden, en el marco de un contrato, la ley de protección de datos aplicable al tratamiento de datos (Brkan, 2016, p.333). Por un lado, podría argumentarse que nada en el RR-I impide que las partes acuerden la ley de protección de datos a aplicar. Por otro, podría razonarse que, en virtud del artículo 9.1. del RR-I, las leyes de protección de datos constituyen leyes de policía[107] y por tanto las partes no pueden pactar la LA. En consonancia con la opinión de Maja Brkan (2016) parece más adecuada la segunda postura en cuanto el RGPD protege dos derechos fundamentales[108]: el derecho a la protección de los datos de carácter personal y el derecho a la libre circulación de los datos dentro del EEE. Sin embargo, como ha sido mencionado anteriormente, en la práctica, muchos contratos contienen cláusulas de elección de LA que el TJUE no ha limitado. No obstante, el TJUE sí se ha mencionado sobre las cláusulas insertadas en contratos negociados de manera colectiva. En la sentencia de 28 de julio de 2016, Verein für Konsumenteninformation, el TJUE estableció que estas resultan abusivas si no informan al consumidor de sus derechos.

b) Obligaciones extracontractuales

Respecto de los supuestos de responsabilidad extracontractual, el RR-II no resulta de aplicación al tratamiento de datos en cuanto su artículo 1.2.g establece que "*Se*

[107] En virtud del artículo 9.1. del RR-I, una ley de policía es "*una disposición cuya observancia un país considera esencial para la salvaguardia de sus intereses públicos, tales como su organización política, social o económica, hasta el punto de exigir su aplicación a toda situación comprendida dentro de su ámbito de aplicación, cualquiera que fuese la ley aplicable al contrato según el presente Reglamento"*.

[108] Las sentencias del TJCE de 11 de diciembre de 2007 C-438/05, Viking Line y sentencia de 18 de diciembre de 2007, C‑341/05, Laval establecieron que la protección de derechos fundamentales constituían razones imperiosas de orden público.

excluirán del ámbito de aplicación del presente Reglamento: [...] g) las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación"[109].

De cara a paliar esta laguna, en 2012[110] el Parlamento Europeo propuso introducir un nuevo artículo[111] para prever la protección frente a la violación de la intimidad y de los derechos de la personalidad y por ende, garantizar la protección de los datos personales. Esta propuesta establece que resultará de aplicación 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 *lex loci delicti comissioni*. Ahora bien, el artículo establece dos matices a esta regla general. En primer lugar, resultará de aplicación la ley del lugar de la residencia habitual del demandado si este no pudo haber previsto que el daño causado por la violación de la privacidad o de los derechos de la personalidad se fuera a producir en ese Estado. Asimismo, en caso de que la violación se produzca como consecuencia de una publicación o emisión, resultará aplicable la ley del lugar donde radique la editorial en caso de que no se hubiera podido prever el lugar donde se producen los daños. Por tanto, si bien esta posible reforma supliría un gran vacío, también adolece de varios problemas. En primer lugar, el criterio general resulta incierto. Como ha sido explicado anteriormente respecto de la CJI, resulta complejo el determinar donde se ha producido un determinado daño. Por tanto, como ha sido

[109] Esta categoría entiende la doctrina que incluye a las acciones extracontractuales relativas a los daños y perjuicios sufridos por un interesado como consecuencia del tratamiento de sus datos personales.

[110] Véase "Resolución del Parlamento Europeo, de 10 de mayo de 2012, con recomendaciones destinadas a la Comisión sobre la modificación del Reglamento (CE) no 864/2007 relativo a la ley aplicable a las obligaciones extracontractuales (Roma II) (2009/2170(INI))" https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012IP0200&from=EN. [Último acceso 8/04/2020].

[111] Este nuevo artículo, versa así: "*Artículo 5 bis: Privacidad y derechos relacionados con la personalidad. 1. La ley aplicable a las obligaciones extracontractuales derivadas de violaciones de la privacidad o de los derechos relacionados con la personalidad, incluida la difamación, será la del país en el que se produzcan o sea más probable que se produzcan el elemento o los elementos más significativos del daño o perjuicio. 2. No obstante, la ley aplicable será la del país de residencia habitual del demandado si esta persona no puede haber previsto razonablemente consecuencias importantes de su acto en el país designado en el apartado 1. 3. Cuando la violación tenga su origen en una publicación impresa o en una emisión de radio o televisión, el país en el que se produzcan o sea más probable que se produzcan el elemento o elementos más significativos de los daños y perjuicios será considerado el país al que va principalmente dirigida la publicación o emisión, o, si esto no fuese evidente, el país en el que se efectúe el control editorial, siendo la legislación de ese país la ley aplicable. En particular, se determinará el país al que se dirija la publicación o emisión por el idioma de la publicación o emisión, o por las ventas o el tamaño de la audiencia de un determinado país como proporción del total de ventas o del tamaño de la audiencia, o por una combinación de esos factores. 4. La leyaplicable al derecho de réplica o medidas equivalentes ,ya toda medid acautelar o interdicto prohibitorio contra un editor u organismo de radiodifusión o teledifusión respecto al contenido de una publicación o emisión y respecto a las violaciones de la privacidad o de los derechos relacionados con la personalidad derivadas del tratamiento de datos personales será la del país en que el emisor o editor tenga su residencia habitual*".

argumentado previamente, resultaría más lógico matizar este criterio de conexión mediante la remisión al criterio del centro de intereses. Asimismo, respecto del lugar del domicilio del demandado y lugar de establecimiento de la editorial, surgen otra vez los problemas anteriormente identificados, y es que resulta complejo el determinar exactamente donde radican los mismos. No obstante, esta reforma nunca llegó a realizarse. Por tanto, de cara a determinar la LA en materia extracontractual deberá acudirse a la normativa nacional de los Estados miembros sobre conflictos de leyes.

1.2.3. Solución nº3: Sistemas de resolución de conflictos de leyes nacionales

Como ha sido mencionado, a falta de convenios supra-nacionales o internacionales reguladores de la determinación de la LA deberá acudirse a las normas de conflicto nacionales. Por razones obvias, no pueden analizarse todos los sistemas existentes de determinación de LA. Por tanto, a modo representativo y en continuidad con la discursiva del capítulo anterior, se presenta dentro del marco comunitario el régimen español y fuera de él, el sistema estadounidense.

a) España

El artículo 10.5 del Código Civil (o «CC») establece, como criterio general, para las obligaciones contractuales la aplicación de "*la ley a que las partes se hayan sometido expresamente, siempre que tenga alguna conexión con el negocio de que se trate; en su defecto, la ley nacional común a las partes; a falta de ella, la de la residencia habitual común, y, en último término, la ley del lugar de celebración del contrato*".

Por otro lado, respecto de las obligaciones extracontractuales, la mayoría de los países siguen la norma de la *lex loci delicti comissi,* o ley del lugar donde se cometió el hecho dañoso. No obstante, existe disparidad a la hora de determinar si este criterio se refiere al lugar donde se produjo el acto o el lugar del daño (Swire, 1991). En España, el artículo 10.9 del CC nos apunta hacia dos posibilidades; (a) la aplicación de la ley del Estado en el que se produce el hecho del que deriva la responsabilidad – *lex loci actus* – o (b) la aplicación de la ley del lugar donde se materializa el daño – *lex loci damni* – (Ortega Giménez, 2014). La primera, se refiere a la aplicación de la ley respecto de cada actividad de tratamiento. Es decir, cada acto de tratamiento ilícito se regirá por la ley del lugar donde este se haya producido. Por tanto, este constituiría el lugar donde se produce el delito o *locus delicti.* Como explica Silvia Feliu (2005, p.226) la finalidad de

este criterio es la de "*restaurar el equilibrio roto por el acto dañoso, imponiendo la obligación de reparar el daño causado. Así la obligación está ligada al hecho que la ha causado, el cual se localiza en el lugar donde se ha producido*". La segunda posibilidad, apunta a la aplicación de la ley del lugar donde se materializan los efectos del daño. Este criterio, puede entenderse *favor laesi* a través del concepto del centro de intereses, que apuntaría a aplicar en la mayoría de las ocasiones la ley del Estado donde el demandante tenga su residencia habitual.

No obstante, en cuanto estas disposiciones contiene un supuesto de hecho demasiado genérico, resultan inadecuadas para regular el tratamiento ilícito de datos personales. Lo apropiado sería construir una norma específica para los supuestos de violación de la protección de los datos de carácter personal para así otorgar una efectiva protección al interesado.

b) Estados Unidos

Fuera del ámbito europeo encontramos el denominado *choice of law* desarrollado por la doctrina y jurisprudencia del *Common law*. En EEUU, el *Second Restatement of Conflict of Laws* (o «SR») constituye la metodología más ampliamente utilizada para determinar la LA (Andrews & Newman, 2013). Si bien esta a priori se utiliza para determinar que ley resultará de aplicación cuando surge un conflicto entre Estados dentro del mismo país, también ha sido aplicada para resolver conflictos de leyes entre EEUU y terceros Estados (Andrews & Newman, 2013, p.373). El SR establece que deberá aplicarse la ley del Estado que tenga la relación más significativa con los hechos y partes más relevantes de la controversia. Así, para determinar la LA, en primer lugar, deberá precisarse el tipo de controversia surgida. En el caso de la protección de los datos de carácter personal esta podrá ser o bien contractual[112] o extracontractual[113]. Una vez determinada, serán los jueces quienes haciendo uso de una serie de criterios determinarán la ley a aplicar por ser la más próxima al conflicto. Por tanto, podemos observar que el sistema de resolución de conflictos de leyes estadounidense es

[112] Para determinar la LA en materias contractuales deberá considerarse: (a) el lugar de la contratación, (b) el lugar de la negociación del contrato, (c) el lugar de ejecución, (d) el lugar del objeto del contrato, y (e) el domicilio, la residencia, la nacionalidad, el lugar de constitución y el establecimiento de las partes.

[113] Para determinar la LA en materias extracontractuales deberá tenerse en cuenta : (a) el lugar donde se produjo el perjuicio, (b) el lugar en que se produjo la conducta causante del daño, (c) el domicilio, la residencia, la nacionalidad, el lugar de constitución y el establecimiento de las partes, y (d) el lugar en que se centra la relación, si la hay entre las partes.

casuístico por tratarse de un sistema de Common law. En consecuencia, si surge un conflicto entre leyes de protección de datos, será el juez competente quien a razón de los criterios de conexión del SR determine la LA al fondo del asunto.

Este sistema en cuanto se basa en unos criterios muy abstractos y generales otorga una gran flexibilidad a los jueces de cara a determinar la LA, lo que resulta en altas dosis de incertidumbre. Por consiguiente, como indica De Miguel Asensio (2005, p.64), este planteamiento ha sido criticado por una gran parte de la doctrina. No obstante, el estatus actual de la jurisprudencia ha impedido que se desarrolle un sistema más concreto de determinación de la LA (Weintraub, 2000, p.679). Por consiguiente, a razón de su alto grado de incertidumbre, este sistema no resulta el más adecuado de cara a determinar la LA. Por tanto, y de acuerdo con Bruce Posnak (2000, p.561), debería optarse en su lugar por redactar una ley o cláusula modelo que sirva de guía para que los tribunales determinen la LA, cláusula que se expone a continuación.

2. MODELO DE ARMONIZACIÓN Nº2

Como ha podido observarse, la determinación de la LA reviste de una especial complejidad[114] (véase un esquema en el anexo nº 3). Jiahogan Chen (2016, p.319) afirma que las dificultades que afrontan las normas de conflicto de leyes a la hora de determinar la LA en el ámbito de la protección de datos, muestran claramente que el DIPr no es plenamente compatible con el derecho de la protección de datos. No obstante, si bien es cierto que en la actualidad la cuestión de la determinación de la LA respecto de la protección de datos reviste una especial dificultad, la adopción de un criterio unificado podría salvar la misma. De esta manera, del mismo modo que respecto de la determinación de la CJI, debe superarse el sesgo territorial que caracteriza a los sistemas de solución de conflictos de leyes, en cuanto estos no resultan idóneos de cara determinar la LA al fondo de una controversia sobre la protección de datos de carácter personal (Mantovani, 2017).

La norma común o cláusula de determinación de la LA debe proponer una respuesta unificada al conflicto de leyes y ser complementaria al ámbito de aplicación de las leyes en materia de protección de datos. Es decir, con miras a evitar que por ejemplo,

[114] Autores como Reidenberg (1999) y Bing (1999) corroboran que las normas clásicas de conflictos de leyes no resuelven los problemas propios de la protección de datos.

conforme al artículo 3 del RGPD esta normativa resulte aplicable pero de cara a regular un precepto concreto, las normas sobre conflictos de leyes apunten a su vez a la aplicación de las leyes de un tercer Estado, lo que no resultaría ni práctico ni lógico. Finalmente, como breve aclaración, si bien no debe caerse en la presunción de la *lex fori,* la naturaleza administrativa de la protección de datos apuntará a que en muchas ocasiones esta resulte de aplicación.

Por tanto, de conformidad de nuevo con la International Law Association (2018) y con lo previamente explicado, una posible cláusula de elección de LA podría versar de la siguiente manera:

Artículo B. Ley aplicable al tratamiento de datos de carácter personal.

1. La presente disposición resulta de aplicación para la determinación de la ley aplicable, tanto para las obligaciones contractuales como extracontractuales, en materia de protección de datos o privacidad.
2. Resultará de aplicación al fondo de una controversia, la ley del centro de intereses del interesado, siempre y cuando pruebe que el demandado conocía éste. En su defecto, resultará de aplicación la ley del lugar donde radique el establecimiento principal del responsable del tratamiento, a condición de que resulte compatible con el ámbito de aplicación de la ley de protección de datos correspondiente. Si este no fuera el caso, resultaría finalmente aplicable la ley del domicilio del interesado.
3. Las cláusulas de elección de foro resultarán inválidas cuando sean contrarias al ámbito de aplicación de las normas en materia de protección de datos.

En suma, tanto este modelo de cláusula, como el anterior, resultan lo suficientemente flexibles para ser aceptados por los Estados y al mismo tiempo específicos de cara a unificar las soluciones a los problemas en la determinación de la LA y CJI, a través de un único instrumento. Partiendo del foro o criterio del centro de intereses se ofrece una protección efectiva del derecho a la protección los datos de carácter personal del interesado. Asimismo, la protección del responsable del tratamiento de datos se encuentra garantizada a través del reconocimiento de la previsibilidad y en su defecto, la aplicación del foro o criterio de su establecimiento principal. De igual manera, respecto de la LA, la referencia al ámbito de aplicación de las leyes en materia de

protección de datos salva las controversias que pudieran existir entre este y las normas de conflicto. Por último, al acotar la sumisión, la parte débil no se ve desprotegida.

CAPÍTULO V: TRANSFERENCIAS INTERNACIONALES

Reviste de especial interés el tratar las transferencias internacionales de datos de carácter personal en un capítulo distinto en cuanto como explica Javier Carrascosa González (1992, p.11) "*la mayor parte de los actos que atentan contra la intimidad de las personas en DIPr por un tratamiento automatizado de datos personales tiene su origen en un flujo internacional de tales datos*". De igual manera, Dan Jerker B. Svantesson (2011, p.180) sostiene que una de las áreas más interesantes y conflictivas de la protección de datos es la regulación de los flujos transfronterizos. Por tanto, y en relación con el DIPr, en primer lugar debe determinarse que ley regulará las transferencias internacionales para después describir lo distintos sistemas de regulación de las mismas.

1. ¿QUÉ LEY REGIRÁ LAS TRANSFERENCIA INTERNACIONALES?

Las transferencias internacionales de datos de carácter personal involucran tres operaciones de tratamiento diferentes. En primer lugar se produce la recogida de los datos. En segundo, los datos son transferidos por el cedente al cesionario. En último lugar encontramos la actividad de tratamiento realizada por aquel que recibe los datos. Con carácter general, la LA a la transferencia de datos como tal será la ley del Estado donde radique el establecimiento del responsable de la transferencia, es decir, del cedente (Calvo Caravaca y Carrascosa González, 2017, p.1535). Por otro lado, la ley a aplicar una vez se han transferido los datos será la ley del lugar donde se traten. Es decir, la ley del establecimiento del cesionario. Si bien ambos expertos se refieren al ámbito europeo, este razonamiento puede extrapolarse a cualquier otro régimen. Esto se debe a que las transferencias internacionales de datos no son más que un tipo de actividad de tratamiento, por ello, para determinar la ley que resultará de aplicación deberá analizarse el ámbito de aplicación de las leyes nacionales o regionales, el cual mayoritariamente toma como criterio el establecimiento del responsable o de los interesados.

No obstante, a razón del amplio ámbito de aplicación de las normas en materia de protección de datos, puede darse el caso de que en determinadas ocasiones las normas

del Estado donde radica el cedente podrán regular las actividades de tratamiento del cesionario. Es decir, que la LA tanto a la transferencia como al tratamiento posterior sea la ley del cedente. Así, en la práctica la regulación de los flujos transfronterizos de datos y el régimen de derecho aplicable se encuentran entrelazados, y los países pueden utilizar normas sobre el derecho aplicable para proteger los datos transferidos más allá de sus fronteras (Kuner, 2011, p.25). Por ejemplo, la aplicación de cláusulas contractuales aprobadas por la UE pueden suponer la aplicación de la normativa europea al tratamiento ulterior de datos.

En conclusión, la transferencia internacional de datos se regirá por la ley reguladora de las actividades de tratamiento del cedente. No obstante, dependiendo del tipo de sistema de transferencia ante el que nos encontremos, el tratamiento posterior de los datos, una vez han sido transferidos, se regirá bien por la ley del Estado del cesionario o por la ley del Estado del cedente.

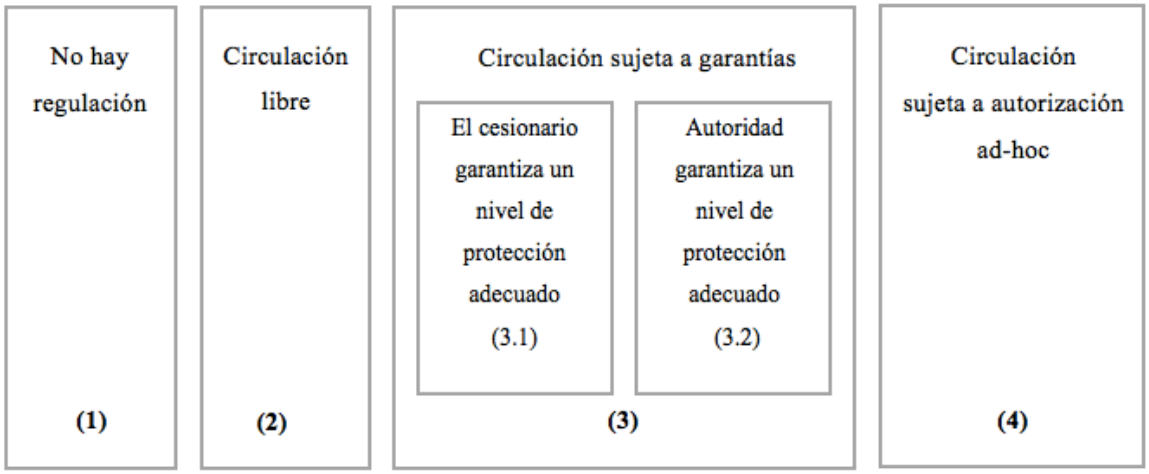
2. ¿QUÉ CRITERIOS DEBEN CUMPLIRSE?

Como ha sido mencionado anteriormente, todas las legislaciones en materia de protección de datos establecen ciertos límites de cara a permitir las transferencias internacionales. La razón se encuentra en que a través de estas limitaciones los países garantizan que los datos recopilados conforme a sus leyes no pierdan su protección una vez transferidos a otros Estados.

2.1. Marco global

Existe una pluralidad de sistemas o regímenes que regulan las transferencias internacionales de datos de carácter personal. De cara a analizar los mismos, resulta pertinente acudir a la división realizada por Francesca Casalini y Javier López González (2019, p.17) aportando ciertos matices. Esta distingue, a grandes rasgos, cuatro planteamientos a nivel mundial a la hora de regular la transferencia internacional de datos personales[115].

[115]Como aclaración, estos planteamientos no actúan como compartimentos estanco sino que se encuentran interrelacionados. De igual manera, un mismo Estado puede aplicar distintos planteamientos para diferentes tipos de datos o transferencias.



En primer lugar nos encontramos con los sistemas que no regulan las transferencias internacionales de datos. En la mayoría de ocasiones, esto se debe a una ausencia de regulación general en materia de protección de datos, en cuanto básicamente la totalidad de regulaciones en la materia se refieren a las transferencias. Países como Camboya, Venezuela o Egipto no poseen regulación en materia de protección de datos.

El segundo tipo de aproximación se refiere a la libre circulación de datos. En esta, los datos fluyen libremente y la protección de los individuos se da a posteriori, pudiendo estos reclamar por una infracción del derecho a la protección de datos o privacidad. En estos sistemas resulta común que los sujetos privados de manera voluntaria tomen medidas para garantizar una efectiva protección de los datos. Este sistema lo encontramos por ejemplo dentro del EEE o en EEUU.

En tercer lugar nos encontramos con los sistemas de regulación de las transferencias datos suscritas al cumplimiento de ciertas garantías. Bajo esta categoría se integran la mayoría de regímenes construidos alrededor de la noción de garantizar un nivel de protección adecuado. A grandes rasgos, esta protección podrá conseguirse a través de dos mecanismos. El primer mecanismo pone la carga de la protección en el cedente o exportador, que deberá garantizar un nivel de protección adecuado de los datos antes de realizar la transferencia. Esto podrá llevarse a cabo a través de la extensión de la responsabilidad del cedente, o través de la utilización de instrumentos jurídicos como cláusulas contractuales o normas corporativas vinculantes (o «NCV»), entre otros. Un ejemplo de ello sería el sistema de *accountability* de APEC. Por su parte, el segundo mecanismo hace referencia a los sistemas por los cuales se permiten las transferencias siempre y cuando la APD o las autoridades supra-nacionales correspondientes permitan

las transferencias en general a un determinado Estado. Por ejemplo, la UE reconoce la facultad a la Comisión de dictar decisiones de adecuación que permiten realizar transferencias libres a determinados Estados. Asimismo, dentro de esta tercera categoría, las transferencias estarán permitidas siempre y cuando medie una razón, como el cumplimiento de un contrato o que el interesado haya otorgado su cumplimiento, entre otras.

Por último, la última categoría se refiere a aquellos sistemas en los cuales el punto de partida es la prohibición de las transferencias internacionales de datos. Estas solo se permitirán cuando la autoridad competente las apruebe individualmente.

2.2. Sistemas de regulación de las transferencias internacionales de datos

Una vez analizado el marco general de regulación de las transferencias internacionales de datos, resulta pertinente examinar de manera específica los dos sistemas regionales más importantes.

2.2.1. APEC

El principio número 9[116] del Privacy Framework de APEC se refiere al sistema de *accountability* o responsabilidad. A través de este, se garantiza que el recopilador original de los datos personales siga siendo responsable del cumplimiento del marco original de protección. Por tanto, independientemente de a donde se transfieran los datos, el responsable del tratamiento original responderá del tratamiento ilícito que se produzca por parte de aquellos a los cuales transfirió los datos (Crompton, Cowper & Jefferis, 2009). Como mecanismo adicional, en 2011, APEC aprobó el "*Cross-Border Privacy Rules* (o «CBPR») *System*"[117]. Este sistema constituye un sistema de certificación al cual las empresas de los países de APEC pueden adherirse para probar que cumplen con las estipulaciones de protección de datos reconocidas internacionalmente. No obstante, el problema de este sistema radica en que es optativo para las economías de APEC e incluso cuando un país se adhiere al mismo, las empresas pueden elegir si desean obtener la certificación o no. Hasta la fecha, sólo

[116] Este principio establece: *"[...] Al transferir la información, los responsables de la información personal deben responsabilizarse de garantizar que el receptor proteja la información de conformidad con estos Principios cuando no obtenga el consentimiento. Así pues, los responsables del tratamiento de la información deben adoptar medidas razonables para asegurar que la información se proteja, de conformidad con estos Principios, después de su transferencia. [...]".*

[117] Véase http://cbprs.org [Último acceso 19/04/2020].

nueve de las 21 economías de APEC participan en este. Por tanto, este mecanismo ha visto un escaso desarrollo en la práctica.

Respecto de los países que conforman APEC, Canadá (Wagner, 2018) y Australia[118] regulan las transferencias internacionales de datos a través del sistema de responsabilidad y obligan a los responsables a adoptar medidas necesarias para garantizar un nivel de protección adecuado. El régimen de EEUU es distinto, en cuanto no cuenta con una legislación a nivel federal que regule la protección de datos, sino que esta emana de distintas legislaciones dictadas a nivel estatal. No obstante, el régimen americano en materia de protección de datos, se caracteriza desde la administración Clinton por la autorregulación (Svantesson, 2011). Esto es, la protección de datos y por ende, las transferencias internacionales se regulan principalmente a través de acuerdos voluntarios pactados entre uniones comerciales o grupos de empresas de un determinado sector.

En suma, la ventaja de los regímenes basados en la responsabilidad del cedente es que no limitan *prima facie* la transferencia de datos. No obstante, este sistema no ofrece una protección total para los interesados. De acuerdo con Stavensson (2011, p.194) el régimen de responsabilidad del cedente o exportador de datos debería constituirse como una capa más de protección, como ocurre en la UE, y no como un sistema alternativo per se. Asimismo, este sistema puede dar lugar a conflictos de leyes, en cuanto la ley del establecimiento del cedente entraría en conflicto con la ley del Estado donde se encuentra el cesionario.

2.2.2. Marco europeo

El marco más regulado y detallado a la hora de regular las transferencias internacionales de datos se encuentra en el RGPD. El Reglamento hace referencia al término "*nivel de protección adecuado*" como criterio para permitir las transferencias internacionales. El TJUE en la sentencia Schrems, párrafo 73 aclaró que "*debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel*

[118] Véase: "Chapter 8: APP 8 — Cross-border disclosure of personal information" https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information/ [Último acceso 19/04/2020].

de protección de las libertades y derechos fundamentales sustancialmente equivalente". Por tanto, cada vez son más los países que aplican los principios europeos de protección de datos con el fin de ajustar su propia legislación a la norma europea para ser considerados como garantes de un nivel adecuado de protección y así beneficiarse de la libre circulación de los datos con la UE (Wagner, 2018, p.319).

El capítulo V del RGPD (artículos 44 y ss.) regula los requisitos necesarios para permitir las transferencias internacionales de datos. De manera resumida, se permiten las transferencia internacionales de datos personales cuando: (a) el país al cual se transfieren los mismos haya sido reconocido como país garante de una protección adecuada por una decisión de adecuación dictada por la Comisión[119], (b) se suscriban garantías adecuadas[120] o (c) se cumpla con alguna de las condiciones del artículo 49. Todo ello teniendo en cuenta que en virtud del considerando 101 del RGPD, las transferencias ulteriores también deberán cumplir con el requisito del nivel de protección adecuado. Por razones de extensión y relevancia a efectos del objeto de este trabajo, no procede entrar a analizar todos estos mecanismos. No obstante, sí resulta pertinente realizar unos apuntes respecto de las NCV[121] reguladas en el artículo 47 del RGPD. Estas constituyen códigos de conducta conformados por normas jurídicas vinculantes o legalmente exigibles, que se aplican a las transferencias internacionales de datos dentro de grupos de empresas (Proust & Bartolli, 2012). La relevancia de estas radica en el hecho de que en principio no se limitan únicamente al ámbito europeo sino que su ámbito de aplicación lo constituye el propio grupo de empresas. Es decir, si un grupo de empresas establece unas NCV basadas en la normativa europea, esta protección de datos tiene el potencial de extenderse a países extra-comunitarios donde radiquen las empresas del grupo. Asimismo, de acuerdo con Lokke Moerel (2011, p.196), las NCV pueden funcionar también como una respuesta reguladora privada a las limitaciones inherentes de las normas sobre la determinación de la jurisdicción y ley aplicable. Por tanto, debe promoverse la utilización de las NCV como instrumento de regulación de las transferencias a nivel global a falta de un acuerdo común que regule la protección de datos o se refiera a las cuestiones propias de DIPr.

[119] Estos son: Andorra, Argentina, Canadá (organizaciones comerciales), Islas Feroe, Guernsey, Israel, Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza, Uruguay y EEUU (limitado al marco del *Privacy Shield*).

[120] Estas garantías pueden ser de cuatro tipos: instrumentos vinculantes, códigos de conducta o autorregulación, clausulas tipo y NCV.

[121] Estas constituyen el mismo instrumento que las CBPR en el marco de APEC.

3. MODELO DE ARMONIZACIÓN Nº3

A falta de una regulación sustantiva en materia de protección de datos y un acuerdo sobre las normas de DIPr, resultaría conveniente promover una mayor armonización entre los diferentes regímenes de transferencia de datos de cara a facilitar el flujo de los mismos y apoyar así las relaciones comerciales transnacionales, sin socavar al mismo tiempo la protección de los datos. Es decir, resultaría idóneo crear un sistema de transferencias internacionales de datos que garantice el derecho fundamental de las personas a la protección de sus datos pero que al mismo tiempo garantice la circulación de los mismos, en cuanto los datos constituyen un *input* esencial en la sociedad actual. No obstante, consciente de que la creación de este marco regulatorio resulta improbable, las NCV o CBPR pueden utilizarse como instrumentos que de manera acotada pueden ayudar a armonizar la regulación y esclarecer las cuestiones propias de DIPr.

CAPÍTULO VI: CONCLUSIÓN

En la sociedad actual los datos de carácter personal revisten una importancia especial en cuanto sirven como base para el desarrollo de la tecnología y las actividades realizadas a través internet. Como consecuencia, surge la especial necesidad de proteger el derecho a la protección de datos. Si bien esta protección no resulta necesariamente una cuestión internacional, en muchas ocasiones lo es a razón de la conectividad y la internacionalización del internet, lo que genera numerosos problemas propios del DIPr. El objetivo perseguido en esta investigación ha sido el de identificar y proponer soluciones a estos problemas. La adopción de una regulación sustantiva común global en materia de protección de datos constituye la solución más comprehensiva y utópica al problema. En su defecto, la creación de una norma común de DIPr parece una opción más plausible, aunque igualmente compleja. Para ello, tendrán que conciliarse distintos intereses y los Estados deberán ponerse de acuerdo sobre las normas de determinación de la CJI y LA. Esto resulta especialmente complejo en cuanto los criterios tradicionales utilizados no solo resultan inadecuados, sino además conflictivos. Para dar solución a esta complejidad, esta investigación ha matizado los distintos foros de determinación de la CJI y sistemas de conflictos de leyes para finalmente proponer la utilización del foro del centro de intereses como posible criterio de cara a determinar tanto la CJI como la LA. No obstante, este foro debe acompañarse de otros foros y criterios de conexión de cara a garantizar la protección efectiva de las partes. Así, en defecto de aplicación del foro del centro de intereses resultan igualmente relevantes los foros o criterio del

establecimiento principal del responsable y el lugar del domicilio del interesado. Por último, respecto de las transferencias internacionales, como un tipo de acto de tratamiento especialmente conflictivo desde la perspectiva del DIPr, a falta de un marco común regulador de las mismas, esta investigación ha abogado por el uso de las NCV, en cuanto de manera potencial, pueden servir para armonizar previsiones y esclarecer cuestiones propias de DIPr.

BIBLIOGRAFÍA

1. LEGISLACIÓN

African Union Convention on Cyber Security and Personal Data Protection (2014).

Carta de los Derechos Fundamentales de la Unión Europea. 18 de diciembre de 2000. (Diario Oficial de las Comunidades Europeas 2000/ C 364/1).

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981.

Convenio relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (2007). L 339/3.

Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. Federal Trade Commision.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Federal Law of 27 July 2006 N 152-FZ on personal data. Federación de Rusia.

Framework on personal data protection (2016). ASEAN Telecommunications And Information Technology Ministers Meeting (Telmin).

Guidelines for processing personal data across borders (2009). Office of the Privacy Comissioner of Canada.

Ley 25.326 de protección de los datos personales (2000). República Argentina.

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 8 de enero de 2000).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

Personal Information Protection and Electronic Documents Act. S.C. 2000, c. 5. Canadá.

Privacy Act 1988. No. 119, 1988. Compilation No. 82. Mancomunidad de Australia.

Reglamento (CE) No 593/2008 del Parlamento Europeo y del Consejo de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales («Roma I»).

Reglamento (CE) nº 864/2007 del Parlamento Europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»)

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

Resolución del Parlamento Europeo, de 10 de mayo de 2012, con recomendaciones destinadas a la Comisión sobre la modificación del Reglamento (CE) no 864/2007 relativo a la ley aplicable a las obligaciones extracontractuales (Roma II) (2009/2170(INI)).

The OECD Privacy Framework (2013).

US Federal Trade Comission's Telemarketing Sales Rule. Federal Trade Comission.

2. JURISPRUDENCIA

High Court of Australia (2002). Dow Jones & Company Inc. V, Gutnick, Joseph.

Internacional Court of Justice (1958). Guardianship of an Infant (Neth. V. Swed.), 1958 I.C.J. 55 (Nov. 28).

Sentencia del TJCE de 11 de diciembre de 2007, C-438/05, International Transport Workers' Federation yt Finnish Seamen's Union y Viking Line ABP y OÜ Viking Line Eesti.

Sentencia del TJCE de 18 de diciembre de 2007, C‑341/05, Laval un Partneri Ltd contra Svenska Byggnadsarbetareförbundet, Svenska Byggnadsarbetareförbundets avdelning 1, Byggettan y Svenska Elektrikerförbundet.

Sentencia del TJCE de 19 de septiembre de 1995, C-364/93, Antonio Marinari contra Lloyds Bank plc y Zubaidi Trading Company.

Sentencia del TJCE de 20 de enero de 2005, C-464/01, Johann Gruber y Bay Wa AG.

Sentencia del TJCE de 27 de septiembre de 1988, C-189/87, Athanasios Kalfelis contra Banco Schröder, Münchmeyer, Hengst & Co. y otros.

Sentencia del TJCE de 30 de noviembre de 1976, C-21/76, Handelskwekerij G. J. Bier BV contra Mines de potasse d'Alsace SA.

Sentencia del TJCE de 7 de marzo de 1995, C-68/93, Fiona Shevill, Ixora Trading Inc., Chequepoint SARL y Chequepoint International Ltd contra Presse Alliance SA.

Sentencia del TJUE 1 de octubre de 2015, C‑230/14, Weltimmo s.r.o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság.

Sentencia del TJUE de 13 de mayo de 2014, C‑131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.

Sentencia del TJUE de 14 de febrero de 2019, C-630/17, Anica Milivojević y Raiffeisenbank St. Stefan-Jagerberg-Wolfsberg eGen.

Sentencia del TJUE de 17 de octubre de 2017, C-194/16, Bolagsupplysningen OÜ e Ingrid Ilsjan contra Svensk Handel AB.

Sentencia del TJUE de 25 de enero de 2018, C‑498/16, Maximilian Schrems y Facebook Ireland Limited.

Sentencia del TJUE de 25 de octubre de 2011, C‑509/09 y C‑161/10, eData Advertising Martínez.

Sentencia del TJUE de 5 de septiembre de 2019, C-28/18, Verein für Konsumenteninformation y Deutsche Bahn AG.

Sentencia del TJUE de 7 de diciembre de 2010, C-585/08, Peter Pammer contra Reederei Karl Schlüter GmbH & Co. KG (C-585/08) y Hotel Alpenhof GesmbH contra Oliver Heller.

Sentencia del TJUE, de 28 de julio de 2016, C-191/15, Verein für Konsumenteninformation y Amazon EU Sàrl.

Sentencia del TS, Sala de lo Civil, de 5 abril 2016, 3269/2014.

Sentencia del TS, Sala de lo Contencioso, de 14 de marzo de 2016, 574/2016.

Supreme Court of Canada (1999). Braintech Inc. contra Kostiuk 171 D.L.R. (4th) 46 (CA).

United States Court of Appeals for the ninth circuit (2000). Bancroft Masters, Inc., v. Augusta National, 223 F.3d 1082.

United States District Court for the Central District of California (2003). Ticketmaster Corp. v. Tickets.com, Inc. Case No. 99-CV-07654.

United States District Court for the Western District of Pennsylvania (1997). Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

United States Supreme Court (1984). Calder v. Jones, 465 U.S. 783.

3. OBRAS DOCTRINALES

American Bar Association (2000). Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created By the Internet. *The Business Lawyer*, Vol. 55, No. 4. Pp. 1801 - 1946.

Andrews, D. C. & Newman, J. M. (2013). Personal jurisdiction and choice of law in the cloud. *Maryland Law Review*, 73(1). Pp. 313 - 388.

Bendiek, A. & Römer, M. (2018). Externalizing Europe: the global effects of European data protection. *Digital policy, regulation and governance*, Vol. 21 No. 1. Pp. 32 - 43.

Bradford, A. (2012). The Brussels Effect, 107 NW. U. L. REV. 1.

Brkan, M. (2015). Data protection and European private international law: observing a bull in a China shop. *International Data Privacy Law*, Vol. 5, No. 4. Pp. 257 - 278.

Brkan, M. (2016). Data protection and conflict-of-laws: a challenging relationship. *European Data Protection Law Review*, 2(3). Pp 324 - 341.

Bu-Pasha, S. (2017). Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*. Pp 213-228.

Calvo Caravaca, A. & Carrascosa González, J. (2017). *Derecho internacional privado, volumen II*. Granada: Comares. Pp. 1526 - 1536.

Campuzano Díaz, B., Rodríguez Benot, A., Rodríguez Vázquez, M.ª A. & Ybarra Bores, A (2018). *Derecho internacional privado, quinta edición*. Madrid: Tecnos.

Carey, P. (2018). *Data Protection: A Practical Guide to UK and EU Law*. Oxford: Oxford University Press.

Carrascosa González, J. (1992). Protección de la intimidad y tratamiento automatizado de datos de carácter personal en derecho internacional privado. *Revista Española de Derecho Internacional*, Vol. 44, No. 2. Pp. 417 - 441.

Casalini, F. & López González, J. (2019). Trade and Cross- Border Data Flows. *OECD Trade Policy Papers*, No. 220.

Committee on the Protection of Privacy in Private International and Procedural Law (2018). *Interim report and commentary to the draft guidelines on jurisdiction and applicable law*. International Law Association.

Crompton, M., Cowper, C. & Jefferis, C. (2009). The Australian Dodo Case: An Insight for Data Protection Regulation. *BNA Privacy & Security Law Report*.

Chen, J. (2016). How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation. *International Data Privacy Law*, Vol. 6, No. 4. Pp. 310 - 323.

De Hert, P. & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, Vol. 6, No. 3. Pp. 230 - 243.

De Miguel Asensio, P. A. (2005). Conflictos de leyes e integración jurídica: estados unidos y la unión europea. *Anuario Español de Derecho Internacional Privado* V. Pp. 43 - 102.

De Miguel Asensio, P. A. (2012). Internet, vida privada y redes sociales: nuevos retos. *Internet y el futuro de la democracia*. Pp. 97 - 118.

De Miguel Asensio, P. A. (2015). Aspectos internacional de la protección de datos: las setencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*, número 31. Pp. 1 - 10.

De Miguel Asensio, P. A. (2017). Competencia y derecho aplicable en el reglamento general sobre protección de datos de la unión europea. *Revista Española de Derecho Internacional*, Vol. 69, No. 1. Pp. 75 - 108.

Feiler, L., Forgó, N. & Weigl, M. (2018). The EU General Data Protection Regulation (GDPR): A Commentary. Woking, RU: Globe Law and Business. Pp. 575 - 577.

Feliu Álvarez de Sotomayor, S. (2005). Competencia judicial internacional y ley aplicable a los supuestos de responsabilidad extracontractual de los intermediarios básicos de Internet. En S. Cavanillas Múgica (ed.), *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*. Granada: Comares. P. 226.

Garcimartín Alférez, F. (2019). *Derecho internacional privado, quinta edición*. Madrid: Thomson Reuters Aranzadi.

Gascón Marcen, A. (2019). The extraterritorial application of European Union data protection law. *Spanish Yearbook of International Law*, 23. Pp. 413 - 425.

Geist, M. (2001). Is there a there there? Toward greater certainty for internet jurisdiction. *Berkeley Technology Law Journal*, Fall.

Gladstone, J. A. (2003). Determining Jurisdiction in Cyberspace: The "Zippo" Test or the "Effects" Test? *Informing Science*.

Kuner, C. (2009). An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law & Security Review*, Vol. 25. Pp. 307 - 317.

Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet. *International Journal of Law and Information Technology,* Vol. 18 No. 2.

Kuner, C. (2011). Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. *OECD Digital Economy Papers*, No. 187.

Lowenfeld, A. (1994). *International Litigation and the Quest for Reasonableness: General Course on Private International Law*. Oxford: Clarendon Press. Pp. 9.

Moerel, L. (2011). *Binding corporate rules: Fixing the regulatory patchwork of data protection*. Tilburg University.

Ortega Giménez, A. (2014). *La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español*. Universidad de Alicante.

Ortega Giménez, A. (2018). El impacto de las nuevas tecnologías en el derecho a la protección de datos desde la perspectiva del derecho internacional privado: redes sociales de internet y cloud computing. *Perfiles de las Ciencias Sociales*, Volumen 6, Número 11. Pp. 154 - 198.

Palao Moreno, G. (2006). Competencia judicial internacional en supuestos de responsabilidad civil en Internet. En J. Plaza Penadés (ed.), *Cuestiones actuales de Derecho y TICS*. Madrid: Aranzadi. Pp. 275 - 298.

Posnak, B. (2000). The Restatement (Second): Some Not So Fine Tuning for a Restatement (Third): A Very Well-Curried Leflar over Reese with Korn on the Side (Or Is It Cob?). *Indiana Law Journal*, Vol. 75: Iss. 2, Article 12. Pp. 561 - 573.

Prosch, M. (2008). Protecting personal information using Generally Accepted Privacy Principles (GAPP) and Continuous Control Monitoring to enhance corporate governance. *International Journal of Disclosure and Governance,* Vol, 5, No. 2. Pp. 153-166.

Proust, O. & Bartolli, E. (2012). Binding Corporate Rules: a global solution for international data transfers. *International Data Privacy Law*, Vol. 2, No. 1. Pp 35 - 39.

Reidenberg, J. (1999). Resolving Conflicting International Data Privacy Rules in Cyberspace. *Stanford Law Reviews*.

Ryngaert, C. (2015). Symposium issue on extraterritoriality and EU data protection. *International Data Privacy Law*, Vol. 5, No. 4. Pp. 221 - 225.

Schultz, T (2008). Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface. *European Journal of International Law*, Vol. 19 No. 4. Pp. 799 - 839.

Shah, R. (2015). Law Enforcement and Data Privacy: A Forward-Looking Approach. *Yale Law Journa*l, Vol. 125, No. 2. Pp. 547 - 553.

Svantesson, D. J. (2007). *Private international law and the internet*. Holanda: Wolters Kluwer Law International.

Svantesson, D. J. (2011). The regulation of cross border data flows. *International Data Privacy Law*, Vol. 1, No. 3. Pp. 180 - 198.

Svantesson, D. J. (2015). Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation. *International Data Privacy Law*, Vol. 5, Issue 4. Pp. 226 - 234.

Swire, P (1998). Of Elephants, Mice, And Privacy: International Choice of Law and the Internet. *The International Lawyer,* Vol. 32, No. 4. Pp. 991 - 1025.

Velázquez Bautista, R (1993). Protección jurídica de datos personales automatizados. Madrid: Colex. Pp. 182 - 189.

Wagner, J (2018). The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection? *International Data Privacy Law*, Vol. 8, No. 4. Pp. 318 - 337.

Weintraub, R. J. (2000). The Restatement Third of Conflict of Laws: An Idea Whose Time Has Not Come. *Indiana Law Journal*, Vol. 75: Iss. 2. Pp. 679 - 686.

Wu, Y. (2010). *Personal data protection in e-government: globalization or glocalization? A comparative study of the United States, Germany and China*. Morrisville, CN: Pro Quest. Pp. 137 - 187.

Yuliyanova Chakarova, K (2019). General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues. *European Union Law Working Papers,* No. 41.

4. RECURSOS DE INTERNET

Amberhawk Training (2016). How 'flexible' can the UK actually be on EU data protection law?. The Register. Obtenida el 18/04/2020 de https://www.theregister.co.uk/2016/05/04/will_the_uks_approach_to_the_gdpr_be_harmonised

Bing, J (1999). Data Protection, Jurisdiction and the Choice of Law. Privacy Law & Policy. Obtenida el 29/03/2020 de http://www.austlii.edu.au/au/journals/PLPR/1999/65.html

Electronic Private Information Center (s.f.). Council of Europe Privacy Convention. Obtenida el 7/04/2020 de https://epic.org/privacy/intl/coeconvention/

European Comission (s.f.). Adequacy decisions. Obtenida el 26/03/2020 de https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

European Digital Rights (2016). PROCEED WITH CAUTION: Flexibilities in the General Data Protection Regulation. Obtenida el 18/04/2020 de https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf

HCCH (1998). Preliminary draft out line to assist in the preparation of a convention on international jurisdiction and the effects of foreign judgments in civil and commercial matters". Obtenida el 17/04/2020 de https://assets.hcch.net/docs/0cbb3742-8964-4c0d-9dd4-3e4e186138d8.pdf.

HCCH (2000). Catherine Kessedjian on Electronic data interchange, internet and electronic commerce. Hague Conference on Private International Law. Obtenida el 3/04/2020 de https://assets.hcch.net/docs/5bc8b14e-d26c-4c65-9a7b-ca349dfe048e.pdf

HCCH (2002). Avril D. Haines on The impact of the internet on the judgments project: thoughts for the future. Hague Conference on Private International Law. Obtenida el 3/04/2020 de https://assets.hcch.net/docs/66cde760-d2bc-4007-9459-cebb39b87851.pdf

HCCH (2003). Electronic Commerce and the Internet (Press release including a synthesis of the Round Table's recommendations). Obtenida el 25/03/2020 de https://www.hcch.net/es/news-archive/details/?varevent=63.

HCCH (2010). Cross-border data flows and protection of privacy - Note submitted by the Permanent Bureau. Obtenida el 17/04/2020 de https://assets.hcch.net/upload/wop/genaff2010pd13e.pdf

Johnson, D. R. & Post, D. (1996). Law and Borders - The rise of law in Cyberspace. First Monday. Obtenida el 8/10/2020 de https://firstmonday.org/ojs/index.php/fm/article/view/468/824

Mantovani, M. (2017). Jurisdiction, Conflict of Laws and Data Protection in Cyberspace. Conflictoflaws.net. Obtenida el 2/04/2020 de https://conflictoflaws.net/2017/jurisdiction-conflict-of-laws-and-data-protection-in-cyberspace/

Naciones Unidas (2006). Report of the International Law Commission. Obtenida el 23/03/2020 de https://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf

Privacy International (2019). Cambridge Analytica, GDPR - 1 year on - a lot of words and some action. Obtenida el 20/02/20 de https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action.

Schwab, K. (2016). La Cuarta Revolución Industrial. World Economic Forum. Obtenida el 25/03/2020 de http://40.70.207.114/documentosV2/La%20cuarta%20revolucion%20industrial-Klaus%20Schwab%20(1).pdf.

Toy, A. & Gunasekara, G. (2019). Is there a better option than the data transfer model to protect data privacy?. UNSW Law Journal. Obtenida el 27/03/2020 de http://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2019/06/11-UNSWLJ-422-Toy-and-Gunasekara-Final.pdf.

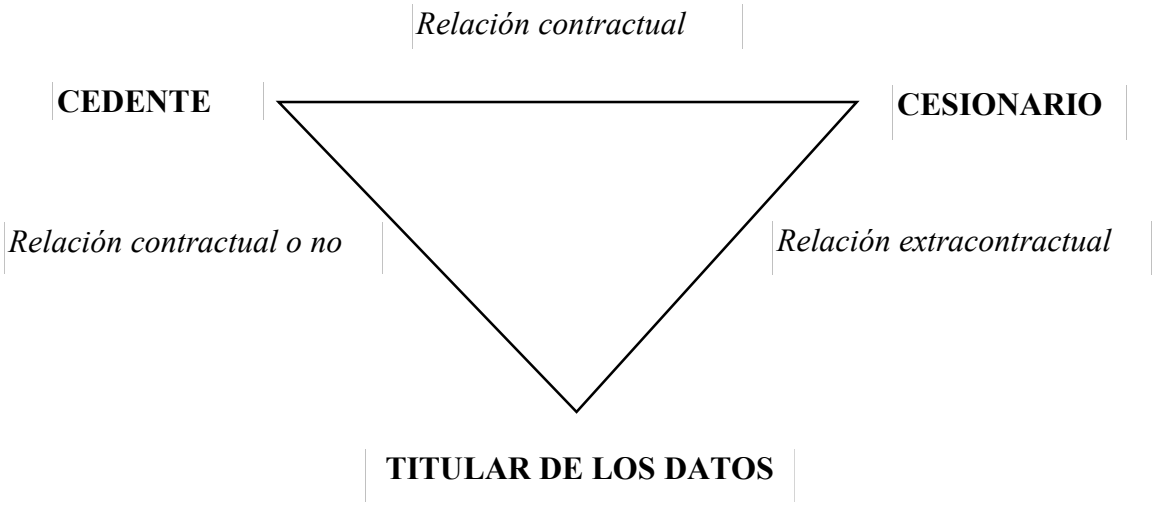
UNCTAD (2016). Data protection regulations and international data flows: Implications for trade and development. United Nations Publication. Obtenida el 20/03/2020 de https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

UNCTAD (2020). Data Protection and Privacy Legislation Worlwide. Obtenida el 25/03/2020 de https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx.

Yu, X. & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. Computer Law & Security Review. Obtenida el 27/03/2020 de https://www.sciencedirect.com/science/article/pii/S0267364918304369?via%3Dihub.

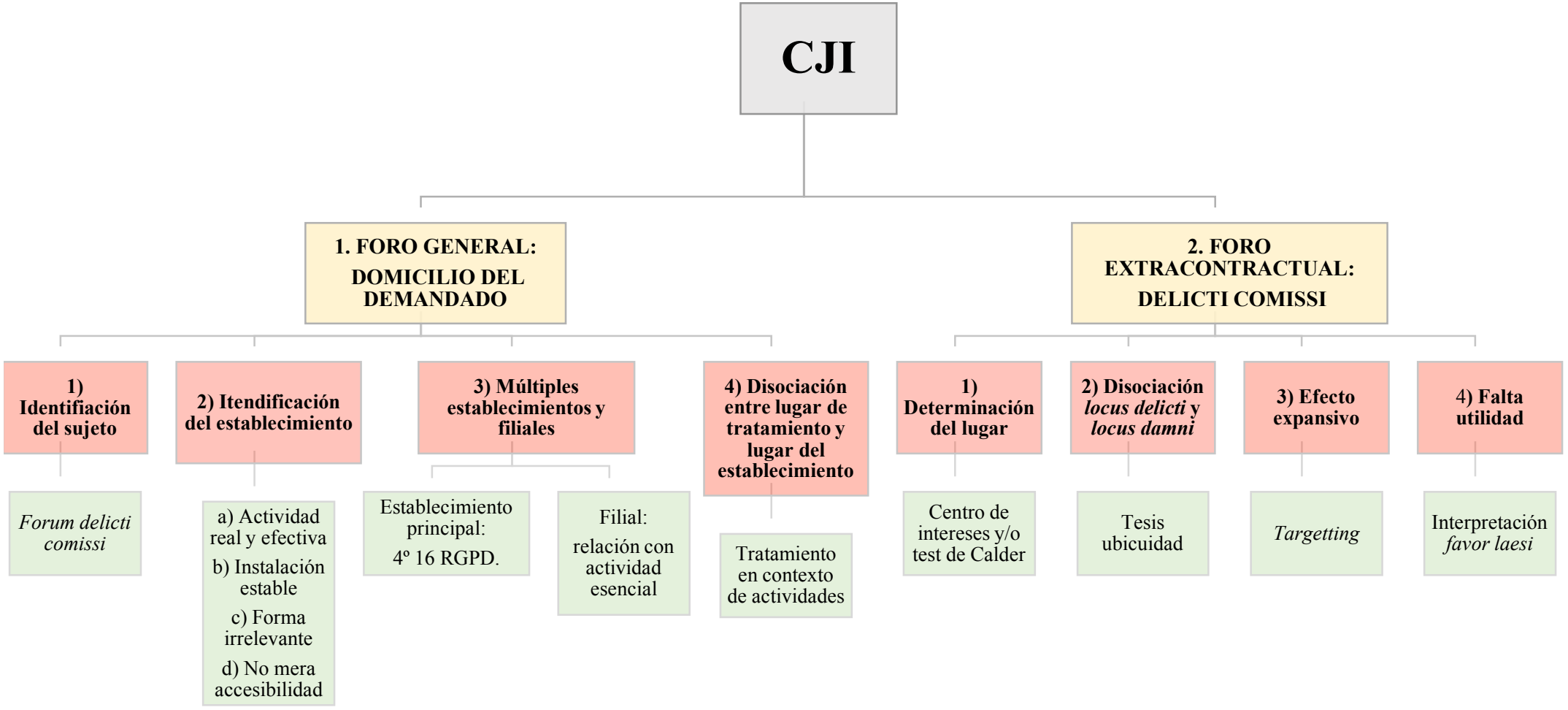
ANEXOS

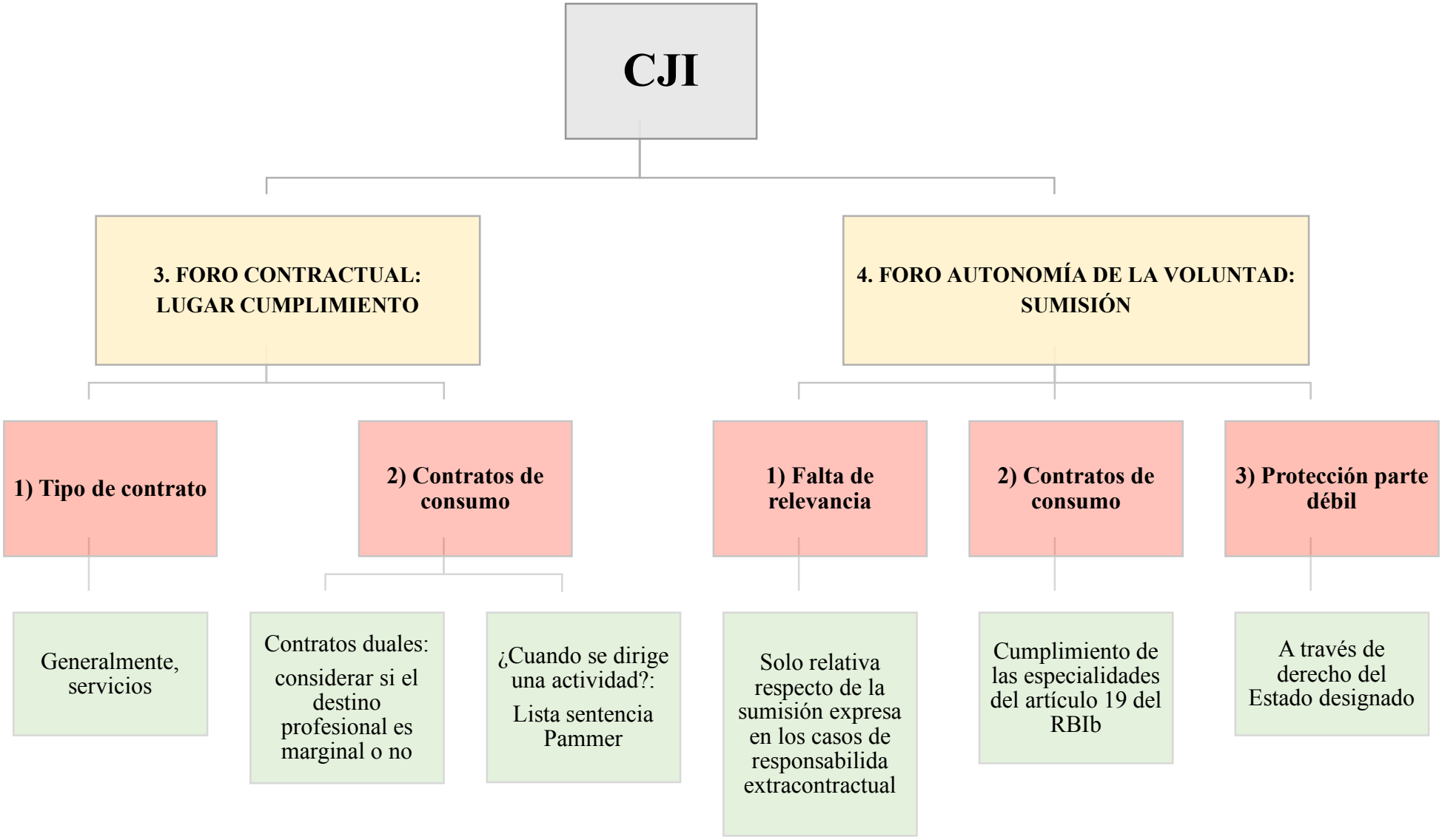
Anexo 1



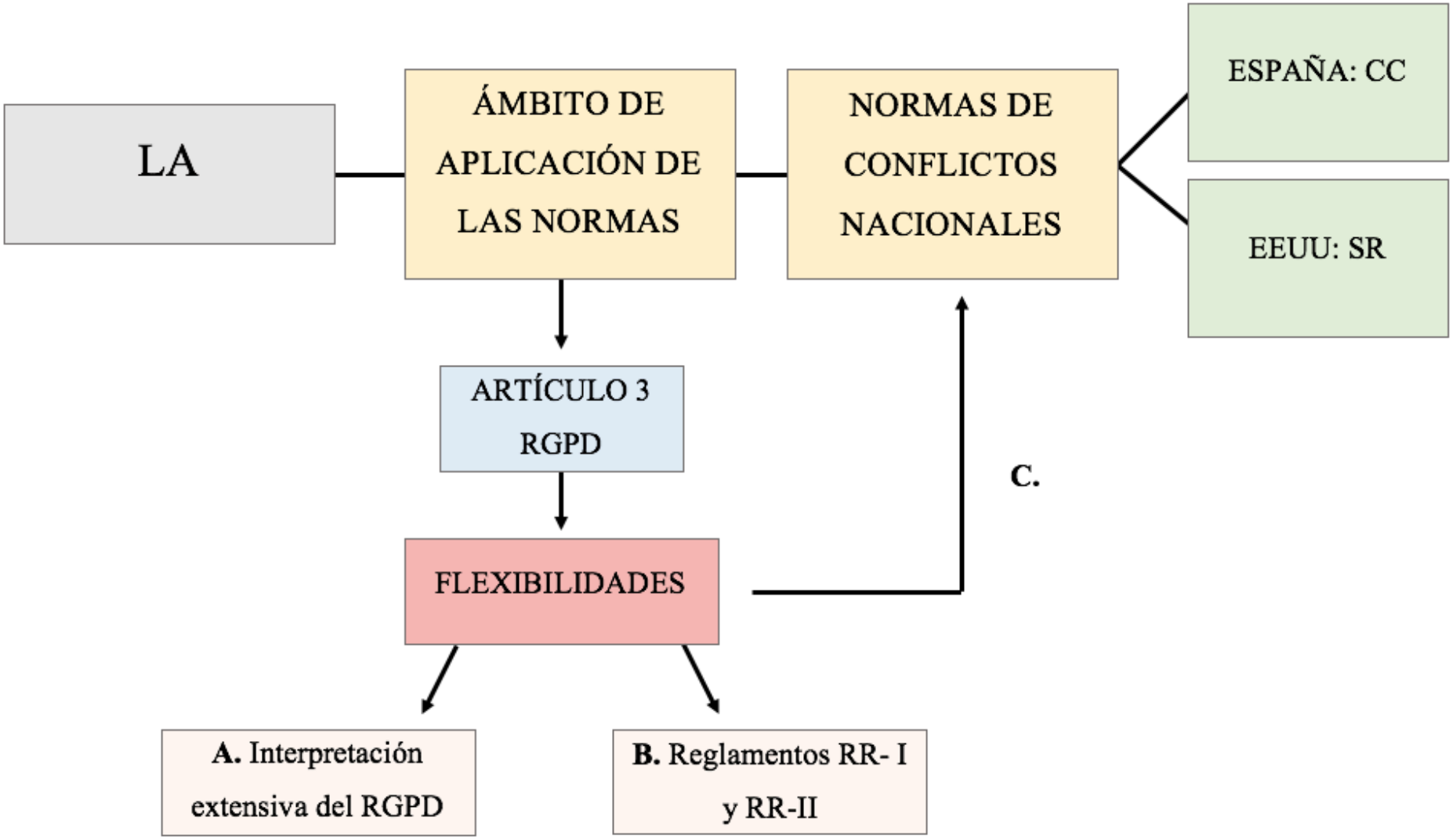
Anexo 2

COLOR: FOROS
COLOR: PROBLEMAS
COLOR: SOLUCIONES




CJI
3. FORO CONTRACTUAL: LUGAR CUMPLIMIENTO
4. FORO AUTONOMÍA DE LA VOLUNTAD: SUMISIÓN
1) Tipo de contrato
2) Contratos de consumo
1) Falta de relevancia
2) Contratos de consumo
3) Protección parte débil
Generalmente, servicios
Contratos duales: considerar si el destino profesional es marginal o no
¿Cuando se dirige una actividad?: Lista sentencia Pammer
Solo relativa respecto de la sumisión expresa en los casos de responsabilida extracontractual
Cumplimiento de las especialidades del artículo 19 del RBIb
A través de derecho del Estado designado

Anexo 3


LA
ÁMBITO DE APLICACIÓN DE LAS NORMAS
NORMAS DE CONFLICTOS NACIONALES
ESPAÑA: CC
EEUU: SR
ARTÍCULO 3 RGPD
FLEXIBILIDADES
C.
A. Interpretación extensiva del RGPD
B. Reglamentos RR- I y RR-II