FACULTAD DE DERECHO

Protección de datos: una perspectiva histórica desde el Derecho Internacional Privado

Sofía Ruiz de la Viuda

5ºE5

Área de Derecho Internacional Privado

Tutor: Salomé Adroher Biosca

Madrid

Junio de 2019

Resumen:

El uso de las tecnologías de la información se aplica en nuestros días en un gran número de industrias, sectores y servicios, habiéndose implantado de lleno en el tejido social. El Derecho, como disciplina que busca entender y ordenar esta realidad social, debe por tanto incorporar estos nuevos servicios y presentar soluciones ante los posibles problemas que su uso pueda plantear. Recientemente, y con la aprobación y entrada en vigor de un nuevo Reglamento 679/2016, General de Protección de Datos, tanto el legislador europeo como el español se centran en este área en pos de conseguir una mejor seguridad de base para la información personal que se comparte desde europa, a un creciente mercado internacional. Este trabajo lidia con la regulación que enmarcan las transferencias de datos personales a través de internet en materia de Derecho Internacional Privado y busca analizar la evolución de las normas en materia de ley aplicable y autoridad competente en las situaciones de conflicto internacional privado que se deriven de estas transferencias.

Abstract:

The use of information technologies is now applied in a large number of industries, sectors and services, having been fully implanted in the social fabric. Law, as a discipline that seeks to understand and order this social reality, must therefore incorporate these new services and present solutions to the possible problems that their use may pose. Recently, and with the approval and entry into force of a new General Data Protection Regulation 679/2016, both European and Spanish legislators are focusing on this area in order to achieve better basic security for personal information shared from Europe to a growing international market. This work deals with the regulation that frames the transfers of personal data through the Internet in the area of Private International Law and seeks to analyze the evolution of the rules in the area of applicable law and competent authority in situations of private international conflict arising from these transfers.

I. Introducción

La creciente importancia de los servicios digitales en esta nueva etapa de la sociedad de la información es una realidad social que el Derecho tiene aún que entender y ordenar desde muchas de sus áreas. Una discusión recurrente entre estudiosos juristas y en general profesionales del Derecho versa sobre la velocidad en la que deben avanzar las diversas disciplinas de la ciencia jurídica para adaptarse a las realidades cambiantes que se dan en la sociedad. En este caso, la urgencia que se siente por parte de tanto juristas como ciudadanos por regular ciertos aspectos de estas tecnologías digitales es proporcional a la velocidad con la que estas se han implantado en la fibra social. La rapidez que ha caracterizado la incorporación de estas tecnologías, tales como las redes sociales, el internet de las cosas o demás servicios computación en la nube, en diversas áreas de nuestras vidas, acompañada por la novedad y la especialidad técnica que acarrean estos servicios y fenómenos, explican en parte la complejidad en la regulación de ciertos temas como el que se trata en este trabajo, la dimensión internacional de la protección de datos.

Junto a la rapidez, se encuentra la dimensión global de todos los servicios que se ofrecen y por supuesto de la información que se difunde. De esta forma, nos encontramos con que las fronteras desdibujadas que en muchas áreas ha traído la globalización, en internet están todavía más difusas, y la naturaleza digital e inmaterial de los datos hacen que en este caso sea especialmente difícil determinar cuáles serán las autoridades y órganos competentes y el derecho aplicable. Ahí radica la importancia del Derecho Internacional Privado como disciplina ordenadora de la competencia de las jurisdicciones y autoridades y de las normas aplicables en casos de conflict. En estos casos los actores son privados, como son la mayoría de las empresas que ceden sus servidores para albergar servicios de correo electrónico, de comercio por internet, de almacenamiento en la nube, o de utilización de redes sociales. Los límites territoriales son básicamente irrelevantes para las transferencias de información digital, pero no lo son para los ordenamientos jurídicos, ni por supuesto para las actividades de las empresas tecnológicas, cuyos órganos directivos están establecidos en un país determinado pero que pueden, por otra parte, abrir sedes de operaciones específicas en Estados con regímenes tributarios ventajosos (Charlín, 2015).

A través del estudio de legislación y jurisprudencia tanto nacional como europea y con especial importancia a las cuestiones relevantes al Derecho Internacional Privado, este trabajo tratará de pre-

sentar los cambios por los que ha pasado la protección de datos de los ciudadanos que pasen por sistemas de tratamiento y almacenamiento masivos. El estudio desde la importancia del Derecho Internacional Privado en esta materia no es casual, ya que la mayoría de los actores que llevan a cabo este tratamiento de datos no son empresas nacionales de la UE, esta es una materia comunitarizada, sino de terceros estados no miembros (Fortuño, 2017). Estudiaremos, con el objetivo de llegar a un mejor entendimiento de la regulación legal actual, el marco de regulación anterior al comienzo del despliegue de efectos del Reglamento 679/2016, General de Protección de Datos, en 2018 y las normas que se establecen en éste para la actualidad.

II. Principios de protección de datos en la legislación española: desde la LORTAD hasta la LOPD

II.I Movimiento internacional de datos

Los legisladores pretenden que el Derecho regule las nuevas situaciones para dotarlas un marco jurídico apropiado, y a este objetivo obedeció nuevo Reglamento 679/2016, General de Protección de Datos. Este Reglamento actualiza los elementos del marco de regulación europea en materia de protección de datos tras la publicación de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Esta desactualización ha producido de hecho, una desprotección de los ciudadanos, que ha durado mientras las autoridades europeas, con la competencia sobre esta materia, buscaban la mejor manera de regular un sector que aunque pueda parecer lejano a los ciudadanos, depende directamente de su navegación por internet y la utilización de los servicios. En los más de veinte años que separan la Directiva de 1995 del Reglamento de 2016, los usos antes limitados de la tecnología de la información se han re-inventado en nuevos servicios, presentes ahora tanto en el sector público y en el privado, pero también en nuevos modelos de negocio que se basan justamente en este tratamiento y análisis de datos, que se pueden comprar y vender fácilmente en mercados dedicados en exclusivo a ello (El País, 2018).

Tanto la Comisión Europea a través de diversas comunicaciones como el Tribunal de Justicia de la Unión Europea (TJUE) a través diferentes sentencias se hacen eco de la preocupación creciente de ciudadanos europeos de diversos Estados Miembros que advierten que la innovación en su sector tecnológico es amenazado por unos competidores que no respetan sus reglas (de Miguel, 2015). Si bien dentro de la Unión Europea existe total la libertad de movimiento de datos informáticos, como veremos esto es porque todos los Estados Miembros pueden garantizar un mismo nivel de protección mientras que otros actores no comunitarios no han podido demostrar las mismas precauciones. En esta sección del trabajo presentaremos el marco de regulación anterior al nuevo Reglamento 679/2016, ilustrando las diferentes posturas de las autoridades nacionales y europeas respecto al tratamiento y análisis de datos por parte de actores de terceros estados, poniendo especial atención en las reglas que determinen la competencia judicial internacional en estos casos.

La Directiva de 1995 ya tuvo en cuenta las tendencias que han marcado la entrada de siglo, como la importancia que del tratamiento tanto manual y automatizado de datos personales gracias a medios informáticos. Sin embargo en el momento de su redacción no pudo ponderarse la importancia que estas nuevas técnicas iban a tener en nuestros días a nivel económico y social.
De igual manera, la ley española anterior, la Ley 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), ofrecía unas protecciones adaptadas a los riesgos de su tiempo, que se demostraron insuficientes frente una sociedad cada vez más digitalizada. De hecho, en su primer artículo, esta ley señala como objetivo: "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos." En ese momento, las compras por internet no eran tan corrientes, y los datos personales se guardaban ficheros electrónicos de negocios convencionales, necesarios para el objetivo final de la facturación de servicios (Llaneza, 2019). Sin embargo, los datos son ahora objetos de comercio internacional y los desafíos de la protección jurídica actual son precisamente los estos derechos a la intimidad, al honor y al olvido, con respecto a una creciente mercantilización de su información.

En cuanto al movimiento internacional de información personal, en su artículo 32 la LORTAD establecía la prohibición a las transferencias de datos personales para aquellos países: "que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas".
La importancia de este artículo reside en la palabra "equiparable". Posteriormente, el criterio de protección mínima se modifica, y en pos de garantizar movimientos internacionales de información personal a países no miembros de la UE, estas serán permitidas, a partir de la aplicación de la Directiva 95/46/CE, a aquellos Estados que "garanticen un nivel de protección adecuado". Así, es en el Capítulo IV, de esta Directiva 95/46/CE, sobre "Transferencias de Datos Personales a Terceros", donde encontramos la regulación, dentro del marco legal sobre protección de datos, sobre las transferencias internacionales de éstos. Este capítulo establece los principios a respetar en estas transferencias. En particular, el art. 25 resuelve sobre la clasificación de terceros estados según los niveles de seguridad que materialmente desplieguen y a partir de ésta dispone la prohibición o el permiso para proseguir con las transferencias de datos a estos Estados. Este artículo define por lo tanto diversas circunstancias en las que encuadrar las capacidades y normas en materia de protección de

datos de Estados no miembros de la UE, para así poder determinar a cuáles de éstos se permitirán transferencias de datos. Ad-supra hemos mencionado que se podrá autorizar la disposición de los datos personales de ciudadanos de la UE por parte de actores en estados no miembros que garanticen "un nivel de protección adecuado". La adecuación de estos niveles deberá determinarse, según los criterios establecidos en el art. 25.2:

> "*atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países."*

Para mantener esta protección activa, este artículo también incluye la imposición de cooperación entre los responsables en la Comisión y las autoridades de los Estados miembros, que deberán comunicarse e informarse de forma recíproca en el pos de limitar posibles desigualdades en las garantías de seguridad de terceros estados. Aparte de dar estas directrices, el artículo 25 remite también, en su sexto apartado, al art. 31 de la Directiva, que se ocupa del proceso de ejecución comunitaria de las medidas que busquen probar que un tercer estado no protege adecuadamente los datos transferidos. De estas clasificaciones derivan tres situaciones bien diferenciadas; la primera es la transferencia de datos entre dos estados dentro de los bordes de la Unión, entre los que existe libertad de movimiento de datos, mientras que las otras dos son transferencias extra-comunitarias. Los otros dos supuestos restantes lidian, por lo tanto, con los movimientos internacionales de datos fuera de la UE, diferenciando aquellos estados que, como se ha señalado anteriormente, cumplen con las garantías para ofrecer un "nivel de protección adecuado", de aquellos que no las cumplen. De esta forma, se establece una primera categoría de estados receptores de información personal compuesta por aquellos que despliegan mejores medidas de seguridad, aunque estas no tengan que ser directamente "equiparables" a las de los Estados Miembros, como se requería antes. Este cambio, se hace en este momento para facilitar y liberalizar estas transmisiones internacionales hacia países con una "protección sectorial" suficiente, como se consideraba por ejemplo a los Estados Unidos (Carrascosa, 2003). En cuanto al tercer supuesto de movimientos internacionales de datos de ciudadanos de la Unión Europea, este trata la situación de aquellos terceros estados que no puedan asegurar una "protección adecuada" según los estándares de la Unión.

Cuando los datos son recogidos para su tratamiento por actores establecidos en terceros países con una protección insuficiente son prohibidas por la Directiva 95/46/CE. Sin embargo, se establecen en su art. 26 una serie de excepciones que deberán tenerse en cuenta. Estas posibilitarían por tanto las transferencias de datos en casos en los que: 1) se cuente con el consentimiento informado e inequívoco del interesado; 2) la transferencia constituya un elemento necesario para la celebración, ejecución o las medidas pre-contractuales de un contrato celebrado o por celebrar entre el interesado y el responsable del tratamiento; 3) sea necesaria esta transmisión de información para la salvaguarda ya sea del interés público como del interés personal vital del interesado o para el ejercicio de derechos en un procedimiento judicial; 4) finalmente, en los casos en los que estos datos sean facilitados desde un registro público, abierto a ser consultado por el público (ya sea en general o o limitado a interesados).

Estas excepciones abren realmente la puerta a que se justifiquen un gran número de transacciones hacia estados sin la protección mínima adecuada (de Miguel, 2015), además de no acompañarse de unas normas básicas que regulen el consentimiento en sí o las situaciones en las que pueda considerarse el interés público en peligro.

II.II Competencia y ley aplicable al tratamiento de datos personales

La regulación de la Directiva de 1995 se traspuso dentro de nuestro ordenamiento jurídico con la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal. En particular, el contenido de los artículos 25 y 26, sobre los principios y las excepciones aplicables al movimiento internacional de datos, se recoge en los arts. 33 y 34 de la LOPD. En cuanto al ámbito de aplicación de esta ley, su artículo 2 señala lo siguiente:

Artículo 2. LOPD:

1. (...)

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito. (...)

El tratamiento es llevado a cabo por un responsable, que la LOPD define en el artículo siguiente como "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". En este momento, nos encontramos con que, aparte de los datos personales que se almacenan en registros administrativos, ya sea de hospitales, ayuntamientos o servidores del gobierno estatal, el resto de datos sobre sí mismos que las personas comparten en internet suelen ser recogidos por grandes empresas, muchas con la sede en Estados Unidos (de Miguel, 2011), que aún contando con oficinas en un gran número de estados europeos, utilizan y tratan esta información normalmente fuera de la UE. El ámbito de aplicación de esta ley se establece, según el artículo citado ad-supra, para los supuestos recogidos, sin embargo, como vemos, la determinación de la Ley aplicable deberá primero considerar las características especiales de cada movimiento internacional de datos, y sobre todo los diferentes niveles de protección que ofrecen los terceros estados donde estén sitos los responsables del tratamiento de esta información o donde este tratamiento se realice.

En lo que se refiere a los criterios determinantes de la ley a aplicar para transferencias internacionales de datos, se ha estudiado ya la existencia de libertad de circulación internacional de datos personales entre Estados miembros de la Unión Europea. De hecho, esta libertad de circulación viene asegurada por una legislación armonizada para todos los países de la Unión, a través de la transposición de la Directiva 95/46, que establece una protección mínima homogeneizada para los datos de todos sus ciudadanos dentro del territorio de la UE.
Esta regulación supone la existencia de un Derecho comunitario, que define la norma de conflicto, determinando la Ley aplicable al tratamiento automatizado de datos personales en situaciones internacionales. Esta norma de conflicto viene establecida en el art. 4 Directiva 95/46:

"*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."

Una vez determinado el Derecho aplicable a todos los conflictos que se deriven entre particulares en relación con el análisis y el tratamiento de datos digitales, gracias a la regulación de bases de la Directiva 95/46, era necesaria la determinación de los mecanismos encargados de resolver los conflictos que suscitasen estos movimientos internacionales de datos.

Como hemos visto, la LOPD establece una serie de supuestos a los que se aplica. Dentro de estos supuestos nos encontramos con situaciones muy diferenciadas y de hecho también diferentes criterios para determinar la Ley aplicable, dependiendo de si los Estados en los que las empresas responsables del tratamiento de datos tienen establecida su sede sean o no miembros de la Unión Europea. En el artículo citado ad-supra, nos encontramos tanto con el criterio de la "Ley de la sede de la empresa" (Carrascosa, 2003) como con el criterio histórico del Derecho Internacional Privado "*Lex loci delicti commissi"*. Este principio, el "*Lex loci delicti commissi",* determina que la Ley aplicable a un delito sea la ley del lugar donde éste se haya cometido.

Adaptándose a casos de movimiento internacional de datos, este criterio conduciría a la aplicación de la Ley del territorio donde el análisis y tratamiento de los datos se lleve a cabo (Eslava, 2002). Sin embargo, las particulares características de los intercambios internacionales de datos, como la inmaterialidad, difuminan las fronteras estatales preexistentes y en muchos casos hacen difícil la determinación del lugar en el que el tratamiento en sí se está desarrollando, al recogerse la información en un país, almacenarse en otro y tratarse en un tercero en un gran número de ocasiones. No obstante, esta no es una norma general, pudiéndose dar casos en los que una misma empresa ha podido subcontratar el almacenamiento de los datos en servidores de terceros países, casos en los que se haya podido subcontratar el mismo trabajo de tratamiento de los datos o casos de venta de estos a otras empresas, que realizarán también actividades de tratamiento. Es justamente a causa de esta especialidad que presentan las transacciones de datos, que se establecen criterios diferentes en los casos de transferencias dentro de la Unión Europea, dentro de la cual opera un Derecho global comunitario sobre movimiento y tratamiento internacional de datos, y fuera de ésta.

Si el ámbito de aplicación de la LOPD viene regulado en su artículo 2, la Directiva 95/46 desarrolla de una forma más amplia en su artículo 4, también citado arriba, las situaciones que pueden darse en transmisiones internacionales de datos. De esta forma, mientras que la LOPD es escueta en la regulación de transferencias de datos personales entre empresas establecidas en Estados miembros de la Unión Europea, la Directiva clarifica el criterio distinto al de *lex loci delicti commissi,* que será aplicable a empresas sitas en Estados miembros de la Unión. Este criterio se establece en el primer apartado de su artículo 4, según el cual, la primera de las situaciones a las que debía aplicarse el contenido de la Directiva 95/46 era cuando el tratamiento de datos fuese:

> "(*...) 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 (...)"*

Conforme a lo recogido en este artículo, en casos de conflictos sobre el tratamiento de datos de ciudadanos europeos por empresas establecidas en la Unión Europea, éstos habrán de adecuarse a la ley estatal del territorio en el que esté establecido el responsable, la entidad que realiza el tratamiento. Como se ha señalado, de acuerdo al principio de previsibilidad o proximidad de la Ley aplicable,

la Directiva emplea el criterio de la "ubicación del fichero" para determinar la Ley aplicable (Carrascosa, 2003). Por lo tanto, los conflictos dentro de la UE sobre protección de datos no se regularían por la más difícilmente determinable Ley del lugar donde se realiza el tratamiento de los datos sino por la Ley del país europeo donde se encuentra la sede de la empresa, en cuyo establecimiento se presupone que se ubican los archivos, y por tanto donde se localizan y se almacenan los ficheros de datos personales, que han de guardarse físicamente en discos duros. Esto se plasma en el apartado primero del articulo 2 de la LOPD, de forma menos desarrollada, que establece que esta ley regirá cuando el tratamiento "sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable". Por lo tanto, aunque el criterio de *lex loci delicti commissi* también venga cristalizado en este artículo, entre Estados miembros de la Unión Europea el contenido de la Directiva se ha interpretado de forma a que pase a ser el criterio de la "Ley de la sede de la empresa", de acuerdo con el principio de eficiencia.

De hecho, la determinación de la ley aplicable según el Estado en el que el responsable del tratamiento de datos esté establecido, la aplicación del criterio de la "Ley de la sede de la empresa", tiene su base no únicamente en el principio de previsibilidad de la Ley aplicable, sino que también operan los principios de la "única Ley" y de la "Ley de la empresa" (Carrascosa, 2003). La determinación de la Ley aplicable puede así efectuarse de una forma más directa y las partes pueden de igual manera contar con menos dificultad a la hora de saber el ordenamiento jurídico y la Ley a la que están sujetas estas situaciones. Esta unificación de la norma de conflicto para todos los Estados miembros de la Unión Europea es posible gracias a los estándares de protección que estos países tienen que cumplir con la transposición de la Directiva y esto no es únicamente positivo para los ciudadanos, que gozan de una mayor seguridad jurídica, sino también para las propias empresas que realizan estas actividades, ya que la Ley a la que estarán sujetas será para ellas una Ley conocida, al ser la del Estado en el que están establecidas y realizan sus operaciones. Además, al someter el conjunto de las actividades de tratamiento de datos de la empresa responsable a un mismo ordenamiento jurídico, independientemente del número de Estados miembros en el que desarrollen sus operaciones y recojan datos, esto significa que el responsable del tratamiento de los datos está obligado bajo una "Ley única" que de esta forma le será más fácil conocer y acatar.

Como se acaba de señalar, la norma de conflicto atiende a dos criterios diferenciados para determinar la ley aplicable en situaciones de transferencias internacionales, sin embargo, si bien en casos en los que el responsable del tratamiento está establecido en un Estado miembro de la Unión Europea

se atiende a la Ley estatal del lugar del establecimiento de la empresa (Carrrascosa, 2003). De esta forma, una empresa sita en Alemania, que recopile datos personales de ciudadanos españoles, italianos y franceses, deberá atender dentro de la realización de sus actividades, a la Ley alemana. Esto no se limitará tampoco únicamente al respeto del contenido de la Ley alemana de protección de datos, sino que estará de igual forma sujeta a las obligaciones administrativas previstas para las empresas sitas en Alemania. Esto es consecuencia como ya sabemos, de que el criterio de "Ley de la sede de la empresa" es el applicable; sin embargo, este criterio opera únicamente en aquellos conflictos en los que la empresa que tome parte en el conflicto esté establecida en la Unión Europea. También se ha señalado anteriormente que un gran número de las empresas responsables del tratamiento de datos a nivel mundial no son europeas sino estadounidenses, por lo que este criterio no les sería aplicable. Dada la cantidad de información sensible que estas empresas manejan sobre ciudadanos europeos es de vital importancia que sus actividades puedan regularse bajo unos mínimos de protección y unas directrices para un adecuado tratamiento.

Así, las empresas internacionales, que operan y tienen su sede en terceros estados no miembros de la Unión Europea, no deberán atender a este criterio sino, de nuevo, a la regla tradicional *Lex loci delicti commissi*, que establece que sea la Ley del lugar donde se ha cometido el delito o el ilícito la que debe ser aplicada. Así, en los casos en los que el tratamiento que se dé a los datos sea inadecuado, será la Ley del Estado en el que se ha realizado este tratamiento erróneo la aplicable. Este criterio, como se ha mencionado anteriormente, da lugar a problemas en su aplicación, al romper con los principios que hacían preferible la determinación de la Ley aplicable según el establecimiento del responsable de tratamiento (Carrascosa, 2003). Por lo tanto, en lo que respecta a las transacciones de datos personales con empresas sitas en estados no europeos, no les serán de aplicación los principios que rigen el criterio de la Ley de la sede de la empresa, por lo que no se podrá considerar que se esté aplicando un Derecho global y será necesario acudir a los ordenamientos jurídicos internos para encontrar la norma de conflicto correcta. Además, tampoco es aplicable el principio de la Ley única, al deber atender a una multitud de sistemas jurídicos según los estados en los que los responsables realicen el tratamiento y por lo tanto, tampoco será empleada la "Ley de la empresa", ya que deberá atenderse siempre al Derecho circunstancial del lugar del tratamiento.

Los problemas que puede crear una desprotección de los ciudadanos y usuarios de ciertas plataformas frente a los responsables de su información personal han sido analizados ad-supra; sin embargo, parece que en aquellos casos en los que este responsable, que decide sobre "la finalidad, con-

tenido y uso del tratamiento", esté establecido en Estados fuera de la Unión, esta desprotección aún sin ser inevitable, es más difícil de solucionar. Mientras tanto, las empresas más grandes dentro de este sector digital, y aquellas cuyo modelo de negocio se asienta sobre esta captación, recopilación y almacenamiento de datos para su uso en nuevas tecnologías de inteligencia artificial, están establecidas en su inmensa mayoría en EEUU, empresas como Facebook o Alphabet (matriz de Google), por lo que la norma aplicable a sus actividades será la determinada dentro del ordenamiento jurídico plurilegislativo estadounidense. Aunque, como se ha explicado anteriormente, EEUU es un Estado que, se consideraba, otorga una privacidad suficiente para los datos personales que se transmitan a servidores bajo su jurisdicción, dada la importancia de este sector dentro de la economía digital, el texto regulador abre la posibilidad de extender la protección garantizada en la Directiva a aquellos casos en los que, aún estando establecida la empresa que realiza el tratamiento en un tercer Estado, los medios necesarios para el tratamiento de datos personales se consideren situados dentro de las fronteras de la Unión. Esta norma se recoge en la LOPD en su art. 2.1.c), citado ad-supra, y será de aplicación siempre y cuando estos "medios" a los que se refiere no tengan únicamente vocación de instrumento que facilita el tránsito de la información. No obstante, la dificultad de aplicación de esta norma de conflicto deriva de la indefinición del término "medios" y de la utilización de conceptos diferentes para referirse a la empleo de éstos en la Directiva, que dice "recurrir", y en la LOPD, que se refiere a "utilizar" medios situados dentro de la UE. De esta forma, la captación de datos que se efectúe a través de mecanismos de almacenamiento de ficheros en los ordenadores de los usuarios situados dentro de la Unión Europea, como por ejemplo el empleo de *cookies,* se consideraría como una actividad realizada dentro de la Unión y por lo tanto, una actividad a la que le es de aplicación el contenido de la Directiva. No obstante, esta aplicación se ha criticado como una "extralimitación de los poderes de la Unión Europea" al traducirse materialmente en una competencia sobre un gran número de entidades domiciliadas por todo el mundo que, aún recopilando datos dentro de Estados miembros de la Unión, pueden de igual manera no desarrollar ninguna parte de su actividad principal en el territorio europeo (de Miguel, 2011).

Hasta aquí se han analizado los criterios y normas sobre ley aplicable y los límites del ámbito espacial en los que operan las reglas reguladoras del régimen de protección de datos. Sin embargo es necesario analizar también la ley aplicable en materia de la responsabilidad civil extracontractual en casos de incumplimiento de las normas contenidas en este régimen de protección.

El art. 23.1 de la Directiva 95/46/CEE, transpuesto en el artículo 19 de la LOPD, establece un derecho de indemnización para aquellos damnificados por el uso incorrecto de su información digital. El

criterio a seguir para resolver sobre la legislación a aplicar en estos casos de responsabilidad se basa en la ubicación del lugar en el que se ha sufrido el daño o donde se ha ocasionado la lesión de los bienes o derechos del afectado, por lo que se suele concretar en la residencia habitual del perjudicado. Por tanto, si hubiesen sido los derechos de un ciudadano español los lesionados, y estando el Estado español obligado por el Reglamento (CE) n864/2007 de 11 de julio de 2007 sobre la Ley aplicable a las Obligaciones Extracontractuales (Reglamento Roma II), este sería el primer texto regulador de la indemnización por incumplimiento del deber de protección de datos, si bien en su art. 1.2.g) se establecen como una excepción a la aplicación del Reglamento aquellos casos en los que las obligaciones extracontractuales "se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación." Es así como en lugar de atender al contenido de este Reglamento, pasamos a la norma de conflicto contenida en el artículo 10.9 CC, según el cual se establece, como ya se ha mencionado arriba, que las "obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven." Así es como, en los casos en los que sea de aplicación la LOPD, dentro del ámbito de aplicación que determina su art. 2.1, y se dé un quebrantamiento del régimen regulador de la protección de datos que ésta contiene, los ciudadanos españoles podrán actuar para reclamar su derecho de indemnización, según lo previsto en el art. 10.9 CC, en base a la ley del lugar donde se hubiese producido este quebrantamiento.

III. Modernidad en la legislación de protección de datos

Tras esta visión general de la legislación previa al actual marco regulador administrativo de las transacciones con datos en lo que respecta especialmente a la dimensión internacional de estos movimientos de información personal, en esta segunda mitad del estudio de la evolución de la protección de datos analizamos los cambios que han resultado en la publicación del último Reglamento sobre este tema, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales 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). Las tecnologías digitales de la información han sufrido, desde la publicación del texto que este Reglamento deroga, cambios fundamentales y solo han crecido en importancia y en implantación social, por lo tanto, antes de la publicación en 2016 de este Reglamento, las autoridades europeas también llevaron a cabo, a través de decisiones, comunicaciones y sentencias del Tribunal de Justicia de la Unión, ciertos cambios en la aplicación de la Directiva 95/46, en pos de garantizar una mayor seguridad a sus ciudadanos. En este apartado se analizará de esta forma, las novedades introducidas poco a poco por las autoridades que dieron forma al actual marco regulador de las transacciones y protección internacional de datos personales.

III.I. Complicaciones en las relaciones entre EEUU y la UE en materia de protección de datos: sentencias Schrems y Weltimmo (2015)

En el primer apartado de este trabajo, sobre movimientos internacionales de datos, ya se expuso la existencia de la libertad de movimiento de datos dentro de la UE, que constituye una primera situación de transferencias permitidas y libres de información digital dentro del espacio europeo. Esta libertad de movimiento de datos puede darse entre Estados de la UE al contar todos con una base mínima homogénea de protección que viene recogida en el contenido de la Directiva 95/46 como también se ha analizado previamente. Sin embargo, aparte de esta situación de libertad de movimiento europea, esta misma Directiva establecía en su artículo 25, con respecto al permiso para las transferencias de datos personales fuera de la Unión Europea, dos situaciones diferenciadas dependientes de los niveles de protección que garanticen los estados en los que estén establecidos los responsables de tratamiento de datos. Por consiguiente, se podrá diferenciar según los niveles de protección que aseguren los terceros estados en sus ordenamientos jurídicos, un primer grupo al que las transferencias de datos de ciudadanos de la UE les serán permitidas, por otorgar un “nivel de

protección adecuada", mientras que aquellos estados en los que los niveles de seguridad no llegan a cumplir unos requisitos mínimos no podrán recopilar, recoger, transferir ni almacenar información dentro del territorio europeo.

En cuanto a qué países pueden considerarse en el primer o segundo grupo, se ha mencionado anteriormente que Estados Unidos, sede del establecimiento de un gran número de las empresas de tecnología digital con mayor número de usuarios, se ha considerado parte del primer grupo, como un Estado que garantiza niveles óptimos de protección. Esto se demuestra con la publicación de la Decisión de la Comisión 2000/520 de 26 de julio, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Esta Decisión, que data de cinco años después de la publicación de la Directiva, establece el marco de protección de la privacidad en las transferencias de datos entre la UE y EEUU basado en el método del principio de puerto seguro, tras largas negociaciones entre las autoridades de la Unión y de Estados Unidos para encontrar un punto óptimo entre el contenido de la regulación estadounidense y las garantías brindadas en la UE (Börding, 2018). Este régimen se compone de una serie de medidas de protección a las que las empresas deben auto-subscribirse y comprometerse en su cumplimiento, pudiendo evitar así la exigencia de una previa autorización por parte de las Agencias nacionales de protección de datos, en este caso la Agencia Española de Protección de Datos, al dar a entender la subscripción a este régimen que estas empresas proporcionan un nivel de seguridad adecuado para los datos personales de los ciudadanos de la UE. Se instaura así la base jurídica para articular las transferencias de datos personales recopilados en la UE por parte de empresas establecidas en EEUU que se hayan adherido a los principios de puerto seguro. Un tiempo más tarde, sin embargo, y también ligado a la creciente importancia de las empresas de servicios digitales estadounidenses, la confianza tanto de las autoridades como de los ciudadanos europeos en los mecanismos de protección de datos de EEUU se ve alterada a la luz de las revelaciones que hace Edward Snowden en junio de 2013 (Elola, 2015) sobre los programas de supervisión y vigilancia llevados a cabo por el gobierno estadounidense en colaboración con grandes empresas tecnológicas.

Seguidamente, en noviembre de 2013, las autoridades europeas publican la Comunicación de la Comisión al Parlamento Europeo y al Consejo, con el objeto de "Restablecer la confianza en los flujos de datos entre la UE y EE.UU." COM(2013) 846 final. Esta comunicación refleja las preocupaciones de las autoridades europeas en cuanto a la protección de la que disfrutan los datos person-

ales de los ciudadanos de la Unión bajo el ordenamiento estadounidense y, aún concediendo la importancia debida a las relaciones entre la UE y EEUU, al que se refiere como un "socio estratégico", admite la debilitación de la confianza tanto por parte de los dirigentes y parlamentarios en la UE, como por los Estados miembros y los ciudadanos, en lo que respecta a las garantías ofrecidas por las empresas tecnológicas sitas en ese país dentro de las transferencias transatlánticas de datos personales. Como se ha mencionado anteriormente, estos problemas de desprotección no afectan únicamente a los ciudadanos particulares sino que constituyen una ventaja competitiva para las empresas estadounidenses que, aún habiéndose adherido a los principios del régimen de puerto seguro, al ser este método de carácter voluntario, no pueden garantizar que se estén cumpliendo las normas básicas para una protección adecuada de la información personal de sus usuarios europeos. En cuanto a los programas de vigilancia por parte del gobierno de EEUU, la Comisión advierte de que las transferencias de datos sujetos a la legislación europea que se hayan facilitado a las autoridades estadounidenses constituirán una infracción a la normativa europea, en los casos en los que no se haya cumplido con los requisitos previos para su autorización, como por ejemplo la evidente proporcionalidad de estas medidas para asegurar la salvaguarda del interés y la seguridad nacional del país (Boehm, 2015). En lo referente a las soluciones que propone esta Comunicación europea, contamos las siguientes: reformar el marco de protección de datos de la UE, reforzar la seguridad del régimen de puerto seguro, fortalecer las garantías de protección de datos en el marco de cooperación entre los servicios coercitivos de los dos Estados, la necesidad de responder a las preocupaciones europeas por parte de las autoridades estadounidenses y por último fomentar a nivel global la adopción de normas internacionales de protección de la privacidad.

Queda claro con el contenido de la citada Comunicación, la desconfianza de la UE en cuanto al régimen de puerto seguro, y este malestar se ve confirmado con la decisión del Tribunal de Justicia de la Unión Europea en la Sentencia Schrems, del 6 de octubre de 2015[1], que declara directamente la invalidez de la Decisión 2000/520 sobre los principios de este régimen de protección. Subrayando de nuevo los problemas ya manifestados en la Comunicación de la Comisión de 2013, esta sentencia declara, la falta de eficacia de los controles establecidos hasta entonces, en especial del modelo de puerto seguro (Brkan, 2015). La decisión del Tribunal se basa en dos argumentos principales. El primero es la falta de fiabilidad del mecanismo de autocertificación de las empresas, ya que aún

[1] Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015, Maximillian Schrems contra Data Protection Commissioner

estando adheridas a los principios de protección, estos no son de cumplimiento obligatorio. En segundo lugar, el Tribunal considera que al no quedar sometidas a estos principios las propias autoridades del estado, no se establecen las suficientes garantías procesales sobre el procedimiento a seguir para asegurar la protección de la información privada de ciudadanos europeos. En la sentencia, llegan a destacar que aquella normativa que no prevea "posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le concierne o para obtener su rectificación o supresión no respeta el contenido esencial del derecho a la tutela judicial efectiva (…)". Además, los magistrados entienden que, aún existiendo una excepción en el régimen de protección de datos cuando se vean en peligro materias específicas y concretas, como el interés público o la seguridad nacional, estos no se pueden argumentar en los casos de recogida indiscriminada de las comunicaciones de ciudadanos europeos sin una motivación suficiente.

Esta sentencia no hace más que señalar los principales problemas que se derivaban de las diferencias entre los modelos de protección de datos de la UE y EEUU (Boehm, 2015). Como acabamos de ver, el marco regulador establecido para las transferencias trasatlánticas de datos se demuestra insuficiente a raíz de las revelaciones sobre los programas de vigilancia del gobierno estadounidense. Es por ello que desde la publicación de esta resolución judicial, las autoridades europeas redirigieron sus esfuerzos hacia nuevas conversaciones y negociaciones con el gobierno del país americano para llegar de nuevo a un acuerdo que instaure un mecanismo protector adecuado. Asimismo, a falta de un camino claro por el que enjuiciar situaciones lesivas para particulares en cuanto a estas transferencias de datos a EEUU, la cuestión clave para que los ciudadanos europeos afectados puedan reclamar en caso de daños, es la localización geográfica en la que se lleve a cabo el tratamiento de la información. Esto es determinante en tanto en cuanto, como se ha estudiado en el apartado sobre aplicación de la Directiva 95/46 y de la LOPD, esto vendrá a decidir sobre la competencia de los tribunales europeos o extranjeros. Sin embargo, dentro de las transferencias de datos de particulares europeos a empresas establecidas en el territorio de un Estado miembro de la UE, también encontraremos conflictos de normas en situaciones en las que esta empresa lleve a cabo sus actividades en otros Estados europeos, fuera del que esté establecida.

La siguiente sentencia a analizar, también de octubre de 2015, es la sentencia *Weltimmo*[2], que vino a dar respuesta a estas situaciones en las que no cabe duda de que una empresa está establecida en el

---

[2] Sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de 2015, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság

territorio de un Estado miembro, ya que el interrogante se plantea sobre si se puede considerar que tiene establecimientos en más de uno. Como se viene estudiando, en aquellos casos en los que se pueda probar que las actividades de tratamiento las está desarrollando un responsable establecido dentro de la Unión Europea, estas actividades quedan sometidas a los principios de la legislación europea de protección de datos. Además, el establecimiento del responsable también determinará la ley nacional que le será de aplicación a estas actividades, según las propias normas de conflicto de la normativa estatal. Dada la importancia del establecimiento del responsable para solucionar los conflictos de normas, por tanto, es necesario que existan unos requisitos y características que permitan identificar específicamente al Estado miembro del establecimiento.

Como se ha resaltado anteriormente, la creciente importancia de las transferencias internacionales de datos ha venido de la mano de un mundo cada vez más globalizado y, aunque la legislación europea presente un marco unitario para todos los países de la Unión, la Directiva dejaba sin plantear todavía algunas cuestiones procesales como la que se discute a continuación. En este caso, residentes en Hungría presentan reclamaciones ante la autoridad de protección de datos húngara relativas a una empresa inmobiliaria con domicilio social en Eslovaquia. Al llevar a cabo actividades como anunciante de edificios sitos en territorio húngaro y tener usuarios húngaros, se plantea la cuestión de si la ley húngara es de aplicación considerándose a la empresa únicamente establecida en Eslovaquia. Aparte de pronunciarse negativamente en este respecto, la sentencia busca fijar unas características que definan las situaciones en las que el responsable del tratamiento esté establecido en más de un único Estado miembro y también los requisitos para considerar que el tratamiento se ha hecho fuera del marco de actividades que se dan en el Estado del domicilio social del responsable.

En cuanto a la problemática que plantea delimitar las actividades que denotan un establecimiento del que habla el art. 4.1.a) de la Directiva, los magistrados del TJUE se remiten al contenido del considerando 19 de este mismo texto. Este considerando define lo siguiente sobre un establecimiento dentro del territorio de un Estado miembro, que este:

> *"implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por*

> *medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades".*

Partiendo así del contenido de una Directiva veinte años anterior a la sentencia, el Tribunal decide aplicar una definición amplia para la noción de establecimiento en materia de protección de datos en contraposición a una concepción formal y acotada (de Miguel, 2015). Así, se instaura que a la hora de estimar al responsable del tratamiento de datos como establecido en uno u otro Estado miembro, no habrá de juzgarse únicamente dependiendo del Estado en el que tenga su domicilio social, sino que se estimará establecido en aquellos Estados en los que desarrolle un ejercicio efectivo y real de su actividad desde un asentamiento estable. En cuanto a qué se considera un asentamiento o instalación estable, el apartado 30 de la sentencia *Weltimmo* recuerda que el objetivo de la Directiva 95/46 es la garantía de una protección suficiente, y con este objetivo en mente establece lo siguiente:

> *"la presencia de un único representante puede bastar, en determinadas circunstancias, para constituir una instalación estable si actúa con un grado de estabilidad suficiente a través de los medios necesarios para la prestación de los servicios concretos de los que se trate en el Estado miembro en cuestión."*

Por lo tanto, esta sentencia no instaura únicamente un concepto amplio de "establecimiento" sino que también indica que la "instalación estable" del responsable puede contarse desde la presencia de un único individuo, siempre y cuando cumplan unos requisitos en el desarrollo de sus actividades. Esto quiere decir que deberá tenerse en cuenta la ya mencionada "estabilidad" de esta instalación en el Estado miembro en cuestión y la efectividad de las actividades de tratamiento. Sobre este punto, la sentencia también indica, en su apartado 32, que la mera gestión del sitio de internet que esté dirigido a hacer negocios en un tercer estado por parte del responsable supone ya una muestra de una actividad efectiva y real dirigida dentro de otro país de la UE. En definitiva, en cuanto a la cuestión planteada por la autoridad de protección de datos de Hungría sobre la posibilidad de que la sociedad del responsable esté establecida en más de un Estado, a parte de donde tenga instaurado el domicilio social, la respuesta del Tribunal es positiva, y esto supone el cumplimiento obligado de las legislaciones de protección de datos no solo del Estado donde tenga su domicilio social sino de todos en los que se le pueda considerar establecido. Además, el establecimiento en

otro Estado también determina la posibilidad de sanciones por las autoridades encargadas de protección de datos de los territorios en los que esté asentado.

En relación con estos conflictos de competencia entre las autoridades de control, la sentencia incluye la respuesta del Tribunal a una consulta en cuanto a la aplicación del art. 28 de la Directiva 95/46, en particular de sus apartados 1, 3 y 6. El art. 28 es el primero de los tres articulo del capitulo VI de la Directiva, titulado "Autoridad de Control y Grupo de Protección de Datos de las Personas en lo que Respecta al Tratamiento de Datos Personales". Este articulo trata sobre la figura de la autoridad de control, sus funciones, competencias y poderes, y en cuanto a estos, la autoridad de protección de datos húngara plantea en la séptima cuestión prejudicial una clarificación sobre la relación entre la ley aplicable y la autoridad nacional competente. En concreto, esta autoridad equivalente a nuestra Agencia Española de Protección de Datos, se pregunta si en el caso de no considerarse a la empresa eslovaca como establecida en Hungría, al verse afectados los intereses de ciudadanos húngaros, la autoridad de este país será competente para conocer y actuar sobre las actividades de la inmobiliaria extranjera (de Miguel, 2015). En busca de respuestas, el Tribunal acude a los artículos dedicados a las autoridades de control de la Directiva, en particular el art. 28 cuya clarificación se había planteado en las cuestiones prejudiciales. En el primer apartado de este artículo, se crea la figura de la autoridad de control, estableciéndose que cada Estado miembro contará con al menos un organismo público que lleve el seguimiento y el cumplimiento del contenido de la Directiva. Este apartado también faculta a esta autoridad de control el ejercicio de las funciones que le sean atribuidas, lo que conecta con el apartado 3 del mismo articulo, en el que se le conceden a la autoridad publica poderes de investigación e intervención, a parte de la capacidad procesal necesaria para imponer sanciones en caso de incumplimiento de disposiciones nacionales o de dar a conocer las infracciones que se produzcan a la autoridad judicial. En cuanto a las restricciones a los poderes de esta autoridad de control, el art. 28.6 dice lo siguiente:

> *"Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro."*

En cuanto a la interpretación que hace el Tribunal del contenido de la Directiva, los magistrados defienden que el art. 28 defiende una concepción restringida al ámbito territorial de las competencias de las autoridades estatales de protección de datos. De esta forma, el Tribunal declara que el organismo de control de Hungría no tendría poder de control sobre las actividades de un responsable establecido fuera de su territorio estatal, sin embargo, sí seria competente para ejercer las facultades otorgadas en el art. 28.3, dentro del territorio de su propio Estado. Por lo tanto, y habiendo fallado los magistrados del TJUE positivamente sobre el establecimiento de la empresa Weltimmo dentro de Hungría, la Agencia de Protección de Datos de este país puede ejercer las funciones antes mencionada, pero carecería de competencia para ejercer cualesquiera de sus funciones que no sean de investigación, si se hubiese dictado a esa empresa como establecida únicamente en Eslovaquia. Así lo establece el apartado 57 de la sentencia, según la cual las autoridades de control, a la hora de conocer una denuncia, podrán desarrollar sus funciones de investigación independientemente del Derecho que le sea de aplicación a la situación, pero que "si llega a la conclusión de que es aplicable el Derecho de otro Estado miembro, no puede imponer sanciones fuera del territorio de su propio Estado miembro." (ap. 57, sentencia Weltimmo).

Esta limitación del área de competencia de las autoridades de control a los territorios de su propio Estado se basa fundamentalmente en la salvaguarda de la libertad de circulación de datos personales dentro de la Unión Europea, y en la defensa de los derechos vinculados a la privacidad, intimidad y honor que se recogen tanto en la Directiva como en los textos fundacionales de la UE. Esta libertad de circulación funciona para facilitar la tutela judicial efectiva en casos en los que un responsable de tratamiento de datos personales establecido en un Estado miembro de la Unión, vulnerase las protecciones mínimas de ciudadanos de otro Estado miembro, en el que lleve a cabo parte de sus actividades de tratamiento de datos pero en el que no esté instalado. Para evitar esta indefensión, el Tribunal adopta una propuesta hecha por el Abogado General que establece una correlación entre ley aplicable y autoridad nacional competente para la aplicación jurídica de la legislación de protección de datos. Por una parte, esto limita la capacidad de actuación de las autoridades de control de un Estado miembro con relación a las situaciones a las que les sean de aplicación la legislación de otro Estado de la Unión, dentro de las cuales no tendrán competencia. Sin embargo, sí que asegura el conocimiento de todas las actividades de tratamiento de información personal que se lleven a cabo dentro del territorio Estatal sobre el que cada autoridad de control tenga competencia.

Así, podemos ver como como el criterio determinante para la elección de ley aplicable es el establecimiento del responsable del tratamiento dentro del territorio de un Estado miembro, y como la autoridad competente viene ligada también al criterio de responsabilidad que establezca la legislación del Estado miembro donde esté establecido el responsable. Independientemente de si los afectados son o no ciudadanos de este Estado, las actividades de los responsables de los datos personales serán sancionadas por las autoridades del Estado donde estén establecidos.

III.II: El Reglamento 679, General de Protección de Datos (2016).

Recogiendo de los problemas estudiados en apartados anteriores, queda clara la necesidad de una actualización de la legislación europea en materia de la protección de datos personales compartidos por los ciudadanos en soportes digitales. La regulación de la responsabilidad y de las facultades que tienen las autoridades de control estatales sobre las diferentes situaciones que pueden plantearse en los intercambios internacionales de datos debe adaptarse paulatinamente a los cambios materiales que se dan en la sociedad, y esta necesidad es la que intenta cubrir el nuevo Reglamento (UE) 2016/679, general de protección de datos. Este reglamento, como se explicará a continuación, cumple un rol específico de unificación de la legislación europea de protección de datos, sustituyendo las leyes nacionales.

III.II.1. Ámbito territorial y determinación de la Ley aplicable

Mientras que la norma de conflicto que determinaba la Ley aplicable en materia de protección de datos en la antigua Directiva la recogía su art. 4 bajo el título “Derecho nacional aplicable”, en el nuevo Reglamento de 2016, la nueva norma que funciona para concretar el ámbito espacial es el art. 3 del RPD, que se refiere al “Ámbito territorial”. Diferencias en el título aparte, los dos articulos cumplen esta misma función de determinación del ámbito territorial de aplicación, al funcionar el antiguo art. 4 como una norma común y unificada para todos los países europeos. El Reglamento incluye también un artículo, el artículo 2, dedicado al “Ámbito material” de aplicación que determina qué tipos de datos personales están sujetos a esta regulación, y cuáles quedarán excluidos, como los datos necesarios para las diligencias relativas a infracciones penales, o los datos generados dentro del desarrollo de actividades domesticas o específicamente personales.

Como se ha señalado en la introducción al contexto del Reglamento, este ha sido planteado desde el legislador europeo como la base de un marco unificado, anteriormente armonizado, en el que el contenido del RPD sea el que sustituya las normas especificas de protección de datos de cada Estado miembro de la UE. La existencia de un único régimen sustituto para todas las legislaciones nacionales en aquellas materias que no habían sido armonizadas supone mayor facilidad a la hora de asegurar la tutela efectiva de las personas que puedan sufrir daños en cuanto a la licitud del tratamiento de sus datos. De esta forma, todas las autoridades públicas de control gozarán de las mismas funciones y poderes, si bien siguen existiendo problemas para determinar entre las autoridades nacionales de diferentes Estados miembros en situaciones ligadas a más de uno de ellos. Para ello, la antigua directiva como se ha visto a lo largo de este trabajo, establecía unos criterios de conexión de las actividades de los responsables del tratamiento de datos a las jurisdicciones de uno o más Estados miembros de la UE, y la aplicación de la legislación de este Estado vendría a determinar la competencia de su autoridad de control. Sin embargo, estos criterios estudiados anteriormente, como el criterio de la ubicación del fichero, de la sede de la empresa o el criterio *Lex loci delicti commissi,* no están presentes en el nuevo RPD, sino que estos conflictos en cuanto a la aplicación de la legislación son sustituidos por normas de competencia específicas para el ámbito administrativo.

Aún no recurriendo a algunos de los antiguos criterios sobre determinación del ámbito de aplicación de la legislativa que se daban en la antigua Directiva, sí encontramos semejanzas entre la nueva resolución del conflicto de normas que da el RPD. Así, ambos artículos presentan tres situaciones diferenciadas a las que les será de aplicación la regulación de protección de datos, siendo la primera los tratamientos, a los que les era de igual forma aplicada antes la directiva, efectuados dentro de las actividades de un responsable (o encargado) establecido en la UE y la segunda los tratamientos de datos por parte de responsables no establecidos en Estados miembros de la UE pero a los que les es de aplicación su legislación nacional por criterios del Derecho Internacional Público (como embajadas o misiones consulares).

Sin embargo, la regulación para la determinación de la aplicabilidad del nuevo RPD varía con respecto a la recogida en el art. 4.1.c) de la Directiva. En este apartado se señalaba que le sería de aplicación la regulación europea en materia de protección de datos a aquellos responsables de tratamiento que, aún sin estar establecidos en el territorio de algún Estado miembro, recurriese: “para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de

dicho Estado miembro, (…)". Tras establecerse este punto de conexión en la Directiva, este aspecto fue especialmente criticado al considerarse el concepto de "recurrir a medios" como demasiado amplio y poco específico, ya que se utilizaba por ejemplo el caso de las *cookies*, cuya utilización es generalizada entre los servicios de páginas web, para ilustrar lo excesiva que resultaba esta medida. Esto se reflejaba en cuanto al marco jurídico español, en el art. 2 LOPD, y tenía el objetivo de ampliar la protección de la Directiva a aquellas transferencias de datos fuera de la UE que en principio no quedarían sujetas a este texto. Parte de las criticas se dirigían hacia la consideración de que la Unión extralimitaba sus poderes de control a un gran número de empresas y organizaciones cuyas actividades se dirigen a niveles globales y no concretamente a los Estados miembros. Es por esto que se deja de recurrir al criterio de la presencia de medios de tratamiento en el art. 3.2 RPD, estableciéndose, en contraste, un ámbito material en relación con los datos que sean manejados por responsables no establecidos en la Unión, de forma que las actividades de estas empresas, organizaciones o instituciones quedarán sujetas a la legislación de protección de datos europea cuando las actividades que realicen tengan como motivo el control del comportamiento de los receptores dentro de la Unión o la oferta de bienes o servicios a interesados en el territorio de la UE (Javed, 2017). Por tanto, se puede observar como, a fin de modernizar y mejorar los procesos de determinación de ley aplicable o de facilitar una mayor unificación del marco regulador europeo, ciertos criterios por lo tanto ya no serán aplicables, mientras que otros necesitarán mayor concreción. En el caso del primer criterio que se ha mencionado anteriormente, sobre la sujeción de las actividades de tratamiento realizadas por un responsable o encargado establecido en la Unión, ha de revisar si el punto de conexión, el establecimiento del responsable, responde al mismo concepto antes estudiado. En primer lugar, queda clara una diferencia respecto a la norma contenida en la Directiva y la del RPD, ya que en el art. 4.1.a) de la Directiva se refiere al "responsable" del tratamiento mientras que en el RPD se introduce también la figura del encargado, por lo que se habla de "actividades de un estable cimiento del responsable o del encargado en la Unión" (art. 3.1 RPD). Además de añadir esta nueva figura, que el art. 4 RPD define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento", el Reglamento no aporta cambios mayores al concepto de "establecimiento", pero sí incluye que a estos datos les será de aplicación la legislación europea en materia de protección de datos "independientemente de que el tratamiento tenga lugar en la Unión o no." Además de esto, no se mencionan las situaciones en las que al desarrollar un mismo responsable actividades en diversos Estados miembros, este quede obligado bajo cada una de las legislaciones nacionales de los Estados en los que esté establecido, ya que éstas están ahora unificadas.

Para aquellos casos en los que los responsables del tratamiento de datos no estén establecidos en la Unión, como se ha visto anteriormente, es necesario dar una solución a posibles problemas de desprotección de los ciudadanos con respecto a sus derechos y garantías en casos de transferencia de sus datos personales a terceros Estados. Con respecto a los responsables no establecidos en el territorio de la UE, como hemos visto antes, el articulo 3.2 RPD establece el siguiente ámbito material:

> "*El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:*
> *a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o*
> *b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión."*

En este apartado se puede ver como el legislador busca conducir la aplicación de esta norma hacia aquellas organizaciones responsables del tratamiento que dirijan sus actividades específicamente a la Unión. El énfasis en cubrir las actividades, tanto las comerciales como las gratuitas) que desarrollan los responsables facilita el sometimiento bajo esta legislación de actividades de tratamiento llevadas a cabo por quienes no estén establecidos en el territorio de la Unión.

III.II.2. Límites en la competencia de las autoridades de control administrativo

Ya estudiados los principios y criterios y las normas de conflicto que operan en la determinación de la ley aplicable, se ha de completar con un examen de las normas que especifican la autoridad pública competente para conocer y decidir sobre reclamaciones o consultas de las personas interesadas dentro de su Estado. En cuanto a las protestas de interesados en defensa de sus derechos en relación con la protección de datos, han de diferenciarse aquellos que se tratan por la vía administrativa o por la vía judicial. Los interesados podrán por una parte ejercitar las acciones que correspondan a una demanda judicial, o podrán presentar una reclamación ante las autoridades de control de su Estado miembro (Brkan, 2015). Estas dos posibilidades ya se recogían en el texto de la Directiva 95/46, sin embargo, en cuanto a las competencias de las autoridades de control, su ámbito de actividades quedaba completamente al contenido del art. 4 sobre derecho aplicable. Siendo así como, en la Directiva, las normas sobre legislación nacional aplicable determinan de igual manera a

las autoridades de control en materia de protección de datos, de uno o varios Estados miembros, competentes para la supervisión de esas actividades. Esta determinación común se rompe en el Reglamento, ya que el art. 3 RPD no cumple esa doble función, y trata únicamente del ámbito territorial de aplicación de la directiva, sin establecer los mismos criterios para la delimitación de las actividades le cada autoridad competente.

Aunque esta norma de conflicto no ayude en la determinación de la competencia de cada autoridad de control, el art. 55 RPD excluye de su competencia el control de las actividades de tratamiento que desarrollen los tribunales dentro del ejercicio de sus funciones pero incluye, en sus dos primeros apartados las siguientes normas:

> *"1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.*
> *2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. (...)"*

Así, es posible constatar el criterio de territorialidad que se incluye en este art. 55, confiriendo competencia a las autoridades de control de cada Estado miembro sobre el territorio de éste, y sobre las actividades de autoridades u organismos públicos y privados sometidos a las reglas de licitud del tratamiento de datos personales contenida en el art. 6 RPD. En cuanto a la naturaleza de las actividades que se encuentran bajo el alcance territorial de las autoridades de control de cada Estado, estas abarcarían, a parte de aquellos tratamientos desarrollados dentro de la actividad de un responsable establecido en su Estado y los que realicen las autoridades de este Estado, también "los que afecten a interesados en su territorio, así como los realizados por quienes no están establecidos en la Unión cuando sus destinatarios son interesados residentes en su territorio (…)" (de Miguel, 2017, pp 12). Dado que bajo esta delimitación de competencias, aquellos responsables que estando establecidos en uno o más de un Estado miembro puedan quedar bajo la supervisión de diversas autoridades estatales de control, el RPD primero establece la categoría de "autoridad de control principal" en su artículo 56, e introduce de igual manera un modelo llamado de "ventanilla única" que facilite la elección entre autoridades de control en situaciones con interesados de dos o más Estados miembros.

En primer lugar, la autoridad de control principal es definida así: "la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento", y será la responsable de controlar los tratamientos transfronterizos que realicen estos responsables o encargados. Aún así, todas las autoridades de control estarán facultadas para conocer las reclamaciones o infracciones en materia de protección de datos de contra establecimientos en su Estado o intereses que conciernan a personas en su Estado sin ser la autoridad de control principal, a quien deberán comunicar estas actividades inmediatamente. La autoridad de control principal decidirá sobre si tratará ella misma el caso o no, basándose en los principios de cooperación entre la autoridad de control principal y las demás autoridades de control interesadas recogidos en el artículo 60 RPD. En cuanto a la definición de autoridad de control principal, la encontramos en el art. 4.16 y presenta dos supuestos, el primero siendo "en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión (…)" y el segundo:

> *"en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento".*

Dentro de los mecanismos de determinación de la competencia se encuentra el ya mencionado modelo de la "ventanilla única". A partir de la implementación de esta "ventanilla única" se abre la posibilidad de que los interesados puedan poner una reclamación ante cualquier autoridad de control dentro de la UE ya que ésta cooperará con la autoridad de control principal de cada caso para resolver la determinación de la competencia. Esto requiere desde el primer momento la identificación de la autoridad principal de control que se ha recogido al más arriba y que concretan el contenido de los considerandos. Este modelo aplica a las situaciones de "tratamiento transfronterizo" que cumplan las siguientes características: que se realice el tratamiento dentro de las actividades de el encargado o responsable establecido en más de un Estado de la Unión o que, teniendo este ente un único establecimiento en la Unión, sus actividades puedan afectar a personas en diferentes Estados miembros. Este modelo resolvería por tanto los problemas de competencia en cuanto a los tratamientos de datos que se efectúen por responsables y encargados establecidos en la UE, ya que

el establecimiento en cualquier país de la Unión asegura la cooperación entre la diversas autoridades de control según los principios del art. 60 RPD, pero no resultaría útil en situaciones en las que este organismo que realiza el tratamiento no esté establecido en territorio de la Unión.

Como excepciones a los criterios que sujetan a la autoridad principal y los principios de cooperación entre autoridades de control que recoge el art. 60 RPD, se encuentran las situaciones en las que una autoridad de control tenga capacidad para tratar una posible infracción o una reclamación en materia de protección de datos a un establecimiento de únicamente dentro de su Estado o en el caso de que afecte solo de forma sustancial a interesados en su Estado. El proceso de decisión, negociación y búsqueda de consenso entre las diferentes autoridades de control viene recogido, a parte de en el art. 60, en los artículos 61 y 62 sobre "Asistencia mutua" y "Operaciones conjuntas de las autoridades de control" y en las siguiente secciones de este capítulo del Reglamento, llamadas "Sección 2: Coherencia" y "Sección 3: Comité europeo de protección de datos" ambas relativas al trabajo de este Comité Europeo de Protección de Datos, que sustituye al antiguo Grupo de Trabajo de Protección de Datos

Por tanto y como se ha visto, del mismo modo que cada autoridad de control tiene la competencia para conocer reclamaciones e infracciones en materia de protección de datos en una gama amplia de situaciones, también los interesados pueden ejercer sus derechos en esta materia ante el organismo de protección de cualquier Estado miembro. Este derecho se establece en el artículo 77 RPD, y aunque concede la posibilidad de reclamar ante cualquier autoridad de control, admitiendo que tiene mayor relación aquel Estado de "en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción". Sin embargo, la tutela de los derechos de los interesados no se limitan a una reclamación inicial sino que para asegurarse hay que incluir la efectividad de las acciones contra la decisión de la propia autoridad de control. Para la defensa del Derecho a la tutela judicial efectiva contra las autoridades de control, recogido en el art. 78 RPD, es importante una vez más la determinación de la autoridad de control principal de cada situación, ya que en el caso de que haya sido ésta finalmente la que ha dictado la resolución del procedimiento administrativo previo, ante ésta y bajo su jurisdicción habrá que presentar la y como respuesta a la decisión que emita la autoridad de control competente, resulta necesario conocer la jurisdicción competente para presentar reclamaciones. Esto se debe principalmente a que, como se establece en el art. 78.3, las acciones contra una decisión de la autoridad de control deberán presentarse ante los tribunales del Estado de esta autoridad. Esto funciona como una extensión del orden contencioso-administrativo a los tribunales.

III.III. Tutela judicial civil en materia de protección de datos: supuestos y ley aplicable.

Aunque se haya analizado en el epígrafe anterior la vocación internacional y el ámbito de aplicación del Reglamento General de Protección de Datos, las normas de conflicto y mecanismos de determinación de la ley aplicable y competencia vistas hasta ahora se limitaban a las acciones ante autoridades administrativas en lugar de acciones judiciales. En contraposición, las decisiones de las autoridades de control únicamente pueden declarar la infracción o la existencia de daños en el tratamiento de los datos personales, pero no sirven para obtener la indemnización o reparación de estos daños. Esta doble vertiente en cuanto a la tutela de los intereses del interesado se refleja en el marco de la antigua Directiva en la jurisprudencia del Tribunal Supremo de nuestro país relativa al derecho al olvido, dentro de la cual las salas de lo Civil en la STS de 5 de abril de 2016 y la sala de lo Contencioso Administrativo en las STS de 14 de marzo de 2016. En estas dos sentencias se dan criterios contradictorios a la hora de definir al responsable del tratamiento, para determinar si le corresponde a la filial establecida dentro de un Estado miembro o a la empresa matriz situada en EEUU (Alphabet), la responsabilidad y el pago de las indemnizaciones o daños (de Miguel, 2017).

Para esto, el RPD establece una protección al derecho de la tutela judicial efectiva contra un responsable o encargado del tratamiento, en su art. 79. En primer lugar, en su primer apartado, el art. 79 establece las situaciones en las que se podrá aplicar estos criterios que aplican a las acciones civiles ante los tribunales, sin afectar esto a los recursos administrativos o extrajudiciales que también se contemplan en este reglamento, por lo que " todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales." Seguidamente, en su art. 79.2, se le atribuye a aquellos interesados que puedan encontrar una ilicitud en el trato de sus datos personales la posibilidad de presentar acciones ante el responsable o el encargado del tratamiento en los tribunales de cualquier Estado en el que estén establecidos o "ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual". Ya que bajo el marco de este art. 79, mayoritariamente se presentarán acciones civiles, hay que comprobar si es de aplicación el Reglamento (UE) No 1215/2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, también conocido como el Reglamento Bruselas I Bis. Ya que la protección de datos no está incluida en las excepciones a la aplicación del Reglamento en su

art. 1.2, y el ámbito de aplicación de este Reglamento como bien ilustra su nombre comprende acciones civiles y mercantiles, quedarán fuera de aplicación aquellos conflictos que afecten en materia de protección de datos a las actividades desarrolladas por una autoridad de control. Sin embargo, les será de aplicación a los supuestos en los que, al darse una vulneración en la protección conferida por el RPD, se interprete conforme al RBIbis que estos daños y perjuicios sufridos son elegibles para llevar acciones de responsabilidad extracontractual (Lundstedt, 2018). En caso de que exista un contrato, por ejemplo el de adhesión a unas condiciones o una determinada política de tratamiento de datos, o en aquellos casos en los que una parte ejercite una acción de responsabilidad civil basada en el incumplimiento de los deberes de protección obligatorios recogidos en el RPD (de Miguel, 2017), deberá entenderse bajo los criterios de competencias especiales que recoge el RBIbis en su art. 7.

En cuanto a cómo se articulan las relaciones entre las normas de conflicto del RPD y el RBIbis, es necesario conocer las relaciones de este último con el resto de instrumentos de determinación de jurisdicción y competencias. Esto viene regulado en el art. 67 RBIbis que establece que no calificará ni decidirá sobre materias especificas en cuanto a la "competencia judicial, el reconocimiento o la ejecución de las resoluciones contenidas en los actos de la Unión o en las legislaciones nacionales armonizadas en ejecución de dichos actos." Este marco para el funcionamiento de las relaciones entre fueros también viene recogido en los considerandos 145 y 147 del Reglamento, que establece lo siguiente sobre las normas de competencia judicial específicas del RPD:

> "*(...) en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.o 1215/2012 del Parlamento Europeo y del Consejo (1) deben entenderse sin perjuicio de la aplicación de dichas normas específicas."*

Por lo tanto y al ser la protección de datos una materia particular con sus propias reglas de competencia judicial, la aplicación del RBIbis quedará supeditada a los criterios contenido en el RPD, que establece por su parte fueros adicionales a los que contempla el Reglamento Bruselas I, como el fuero de residencia habitual contenido en el art. 79.2 RPD. Por lo tanto, la relevancia de la aplicación del RBIbis en la tutela judicial en materia de protección de datos se materializa en la ampliación de fueros ante los cuales será posible presentar estas acciones civiles. Así, el profesor Pedro

de Miguel (2017) establece la siguiente lista de fueros disponibles por la aplicación del RBIbis: por una parte se da la prórroga de la jurisdicción, también se facilita el fuero general del domicilio del demandado, los fueros basados en una relación de conexión o el fuero especial en materia extracontractual. Además, en tanto en cuanto se considera que, aún sin existir una relación contractual entre las dos partes, el incumplimiento por parte del responsable o del encargado de la normativa del RPD puede considerarse como una vulneración de los derechos garantizados en esta norma o un incumplimiento de las condiciones básicas para el tratamiento de datos personales, también serán de aplicación las normas de protección de los consumidores contenidas en los arts. 6.1 y 17-19 y las correspondientes de la Ley Orgánica del Poder Judicial (art. 22 quinquies *d)*), y el fuero del domicilio del consumidor para presentar acciones contractuales.

Ya que podemos ver como en materia de competencia para garantizar una tutela judicial efectiva se da un conflicto de normas, es necesario delimitar la Ley aplicable a los aspectos de la responsabilidad civil que se deriven de infracciones al contenido del RPD, cuando éste no los regule directamente. El estudio del ámbito territorial de aplicación contenido en el art. 3 RPD previamente realizado se refiere a las decisiones relativas a determinar la licitud del desarrollo del tratamiento de los datos. Por lo tanto, pueden darse situaciones en las que, aún tratándose de contratos internacionales regidos por la ley de un tercer Estado no miembro de la UE, como se ha visto anteriormente, estos contratos queden sujetos a la aplicación imperativa de la normativa europea de protección de datos. Estos supuestos vienen recogidos en las normas del Reglamento (CE) No 593/2008, conocido como el Reglamento Roma I sobre la ley aplicable a las obligaciones contractuales, que incluye en su art. 9.2 una norma sobre la naturaleza imperativa de ciertas leyes especificas, como el Reglamento de Protección de Datos, conocidas como Leyes de policía. Sin embargo, la imperatividad de la norma no asegura su aplicación sobre la totalidad de los aspectos que se derivan de la responsabilidad civil que pueda emerger de un tratamiento ilícito .

Quedando clara la aplicación del RPD como ley de policía, esta será por lo tanto de aplicación por encima de cualquier otra norma que regule conflictos en relaciones contractuales, como el RRI, dentro de su ámbito territorial de aplicación (Lundstedt, 2018). Mientras que el RPD concede en su art. 82 el Derecho a indemnización y responsabilidad para los interesados afectados, y establece por tanto la obligación de aquel responsable o encargado de indemnizar los daños y perjuicios en casos de tratamientos ilícitos, este artículo no consigue unificar las normas de delimitación y determinación del Derecho aplicable a estas indemnizaciones en casos en los que intervengan actores de

diferentes Estados. Esto presenta un problema especialmente en la delimitación de las situaciones de conexión autónoma al art. 3 RPD, o la sujeción de la Ley aplicable a obligaciones extracontractuales, ya que en materia de protección de datos no es de aplicación el Reglamento (CE) 864/2007, o Reglamento Roma II sobre ley aplicable a las obligaciones extracontractuales, que en incluye aquellas "obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular la difamación", entre las excepciones a su aplicación en su art. 1.2.*g)*. Podemos ver así como, sin serle de aplicación este reglamento a las situaciones de responsabilidad extracontractual en materia de protección del datos, la norma de conflicto a aplicar en estos casos de infracción deberá ser la norma de la legislación nacional de cada Estado. En este caso, por tanto, será de aplicación las normas de derecho internacional privado contenidas en nuestro Código Civil, en concreto el art. 10.9 CC que establece que: "Las obligaciones no contractuales se regirán por la ley del lugar donde hubiere ocurrido el hecho de que deriven." La remisión a las normas de conflicto nacionales para decidir sobre estas obligaciones no contractuales resulta en diferencias muy pronunciadas en las soluciones que da cada Estado a esta determinación de Ley aplicable, a falta de mejor una unificación en materia de tutela judicial efectiva para las acciones civiles en materia de protección de datos.

IV. Conclusión

A lo largo de este trabajo se ha realizado un análisis a las cuestiones relevantes de Derecho Internacional Privado de la regulación europea y española en materia de Protección de Datos. Como se ha podido constatar, esta regulación ha sufrido grandes cambios entre la publicación de la Directiva en 1995 y la aplicación del Reglamento 2016/679 General de Protección de Datos en mayo de 2018. En principio podemos constatar como este nuevo RPD tiene una vocación unificadora que sustituye las legislaciones nacionales de cada Estado miembro, mientras que el marco anterior se organizaba en torno a la armonización de la Directiva. Esto denota la importancia que la regulación de esta materia tiene para la Unión, no únicamente debida a las preocupaciones de los europeos sino también a los indicios de competencia desleal que resultaban claros con respecto a la difícil aplicación de la Directiva a terceros Estados.

Estos cambios se han hecho esperar y la actualización de las normas ha sido gratamente recibida tanto por parte de los particulares, como por las empresas de servicios de la información y los propios gobiernos estatales, al cobrar cada vez mayor importancia las nuevas tecnologías de redes sociales, comercio por internet o la computación en la nube en el entorno económico y social actual. Esto es evidente al ver como dentro de las 10 empresas más importantes de 2017, encontramos que cinco de ellas, Apple, Alphabet, Microsoft, Amazon y Facebook (BBC, 2017)[3] de ellas se dedican a negocios directamente ligados al sector de las comunicaciones o a los servicios de información digital. Además, la velocidad con la que se desarrollan y cambian en sus usos y su diseño estas nuevas tecnologías, requieren un estudio y trabajo continuo tremendamente especializado, que ha de hacerse desde el Derecho para garantizar la protección de los derechos de las personas. Este estudio y trabajo que ha de realizarse es especialmente necesario en la disciplina del Derecho Internacional Privado, al tratarse muchos de los responsables o encargados del tratamiento de datos personales de gente situada en el territorio europeo de empresas multinacionales, muchas veces extranjeras a la Unión, y por lo tanto darse numerosas situaciones de conflicto internacional entre particulares. La naturaleza inmaterial de los datos personales y los canales por los que estos circulan parece poner obstáculos a la hora de determinar ya sea la ley aplicable a las controversias o la competencia de los tribunales de determinado Estado miembro, sin embargo, acompañando al texto del Reglamento deberían implementarse iniciativas de divulgación e información a los ciudadanos en cuanto a las

[3] Las 10 empresas más valiosas del mundo (y cuáles son las 5 que lideran en América Latina), 14 de diciembre de 2017, BBC.com

garantías de las que disponen para proteger su información personal y el funcionamiento de estas nuevas tecnologías.

Las situaciones a las que es aplicable el nuevo Reglamento 2016/679 General de Protección de Datos son diversas y los criterios para determinarlas sujetas a esta normativa son amplios. Esta flexibilidad resulta necesaria en un entorno social en el que cada vez se da nuevos usos a estas tecnologías, ya que ha de tenerse en cuenta la seguridad jurídica y la protección de los intereses de los interesados. Los derechos que pueden verse infringidos son en un primer momento los derechos a la privacidad, intimidad y honor, o hasta el "derecho al olvido" sobre el que tratan varias sentencias tanto de nuestro Tribunal Supremo como del Tribunal de Justicia de la Unión Europea. Sin embargo, los usos proyectados de las nuevas tecnologías se recogen también en el Reglamento, que establece su aplicación para aquellas situaciones en las que las actividades de tratamiento de datos personales se relacionen con "el control de su comportamiento, en la medida en que este tenga lugar en la Unión".

BIBLIOGRAFÍA:

- BBC. (2017) Las 10 empresas más valiosas del mundo (y cuáles son las 5 que lideran en América Latina) https://www.bbc.com/mundo/noticias-42327754
- Boehm, F. (2015) A comparison between US and EU data protection legislation
- for law enforcement purposes. Policy Department, European Parliament. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf
- Börding A. (2018) Safe Harbor: The Decision of the European Court of Justice. In: Hoeren T., Kolany-Raiser B. (eds) Big Data in Context. SpringerBriefs in Law. Springer, Cham
- Brkan, M. (2015). Data protection and European private international law: observing a bull in a China shop: International Data Privacy Law, 5(4), 257–278
- Carrascosa González, J. (2003) Globalización y Derecho internacional privado. Ed. Liberlibro.
- Charlín Menéndez, F. (2015) La competitividad fiscal: El caso irlandés.
- COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO. COM(2013) 846. "Restablecer la confianza en los flujos de datos entre la UE y EE.UU." https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52013DC0846
- de Miguel Asensio, P.A. (2011) Derecho Privado de Internet. Pamplona, Ed. Thomson Reuters.
- de Miguel Asensio, P. A. (2015) Aspectos Internacionales de la Protección de Datos: las Sentencias Schrems y Weltimmo del Tribunal de Justicia. La Ley Unión Europea, (31), 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. (69/1), 75-108
- Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. C(2000) 2441. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32000D0520
- El País (2018). Mercado de datos y miedo digital. Editorial. https://elpais.com/economia/2018/05/24/actualidad/1527180839_511844.html
- Elola, J. (2015) El efecto Snowden. El País. Acceso en: https://elpais.com/tecnologia/2015/06/12/actualidad/1434129706_593265.html
- Eslava Rodríguez, M. (2002) El locus delicti commissi en los ilicitos contra la vida privada cometidos a través de Internet.

- Javed, U. (2017) The GDPR's Reach: Material and Territorial Scope Under Articles 2 and 3. Privacy in Focus, Wiley Rein.
- Llaneza, P. (2019). Datanomics. Barcelona. Ed. Planeta.
- Lundstedt, L. (2018). International Jurisdiction Over Cross-Border Private Enforcement Actions Under the GDPR.
- Moerel, L. (2011) The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?. International Data Privacy Law, 28-46

JURISPRUDENCIA CITADA

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de 2015, C−230/14. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság.
- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015, C-362/14. Maximillian Schrems contra Data Protection Commissioner.
- España, Tribunal Supremo, Sala de lo Civil, STS (Sala 1ª. Pleno) de 5 de abril de 2016. Num. 210/2016. Derecho al olvido digital.
- España, Tribunal Supremo Sala de lo Contencioso-Administrativo (Sección Sexta) de 14 de marzo de 2016 Num. 574/2016.

LEGISLACIÓN CITADA

- España. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. (LOPJ)
- España. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).
- España. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- 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.

- 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 (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 (UE) nº 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.
- Reglamento (UE) nº 6792016 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).