

LA TRANSFERENCIA INTERNACIONAL DE DATOS EN LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y EL DERECHO INTERNACIONAL PRIVADO.

• I. Planteamiento.	1
• II. Concepto de transferencia internacional de datos.	2
• III. Excepciones: régimen de autorización de las transferencias internacionales de datos.	4
• IV. Actividad de la Agencia Española de Protección de Datos en materia de transferencia internacional de datos.	6
• V. Aspectos de Derecho internacional privado relacionados con la transferencia internacional de datos.	10
• VI. Conclusiones finales.	15
• VII. Bibliografía consultada.	16

Alfonso Ortega Giménez

Profesor de Derecho internacional privado de la Universidad Cardenal Herrera-CEU en
Elche, Profesor Asociado de la Universidad Miguel Hernández de Elche, y Profesor
Colaborador del Proyecto UAIPIT.

I. Planteamiento. ➔

1. La transferencia internacional de datos personales de un Estado a otro es tema de especial atención en las Leyes de protección de datos ¹. Todos los principios y derechos recogidos en las mismas se ven seriamente amenazados si no se establece un control que marque unos límites de garantía y seguridad en la transmisión telemática o en la transferencia de los datos personales cruzando fronteras. Por ello, la regulación de los límites a la transferencia de datos se encuentra, a nuestro juicio, en el origen de las normas nacionales e internacionales reguladoras de la protección de datos. Precisamente, las normas internacionales que regulan la materia tienen por objeto establecer un núcleo básico de principios de protección de datos, que permita considerar uniforme el régimen aplicable en los Estados signatarios, permitiendo así el flujo de información hacia los mismos e impidiendo su transmisión a quienes no cumplan esos principios.

En este sentido, el objeto del presente estudio es el de analizar, desde la óptica del Derecho internacional privado, el fenómeno de la transferencia internacional de datos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) ², para lo cual partiendo del concepto de transferencia internacional de datos que establece la propia LOPD, analizaremos el régimen de autorización de las transferencias internacionales de datos, la actividad de la Agencia Española de Protección de Datos (en adelante, AEPD) en esta materia, y así poder centrarnos en la resolución de las principales cuestiones *iusprivatistas*:

a.

Competencia judicial internacional;

- b. Derecho aplicable; y,
- c. Reconocimiento y ejecución de decisiones extranjeras.

II. Concepto de transferencia internacional de datos. ➔

2. La transferencia internacional de datos de carácter personal es una de las actividades que regula con más cautela la LOPD con el objeto de prohibir las exportaciones de datos de carácter personal cuando se compruebe previamente que el lugar de destino no ofrece una protección semejante a la otorgada en la Unión Europea (en adelante, UE)³. En la medida en que el movimiento internacional de datos es libre entre los países de la UE, sólo existe una transferencia internacional de datos cuando el país de destino sea un tercer Estado, esto es, un Estado no miembro de la UE. No puede hacerse ninguna exportación de datos a países terceros, desde España, salvo que dichos países hayan sido declarados, como destinos seguros por el Ministerio de Justicia o se haya obtenido previamente una autorización de la AEPD.
3. Sin embargo, esa transmisión debe efectuarse de tal modo que los derechos de los particulares a quienes los datos se refieren y, en especial, su intimidad, queden plenamente garantizados. De ahí que la Exposición de Motivos de la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva 95/46/CE)⁴ recuerde, en su considerando 7, la necesidad de conciliar la protección de los derechos de los ciudadanos en los Estados Miembros, a fin de que las garantías que dicha protección establezca no puedan *“constituir un obstáculo para el ejercicio de una serie de actividades a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario”*. Por tanto, el régimen regulador de las transferencias internacionales de datos trata de conciliar la circulación de la información sobre las personas con los derechos de los afectados, logrando un equilibrio sumamente complejo, como complicado puede resultar, en ocasiones, el entendimiento de las normas que lo integran.
4. La norma primera de la Instrucción 1/2000, de 1 de diciembre, de la AEPD, relativa a las normas por las que se rigen los movimientos internacionales de datos⁵, define la transferencia internacional de datos como *“toda transmisión de los mismos fuera del territorio español”*. Tomando en consideración este concepto, debemos señalar que, tal y como indica la Memoria de la AEPD correspondiente a 1999⁶, el fundamento de las transferencias internacionales de datos, cuya inscripción ha sido solicitada en el Registro General de Protección de Datos (en adelante, RGPD), se encuentra en dos causas esenciales: a) Por una parte, en la necesidad de armonización y puesta en común de los sistemas de información de los grupos empresariales. Así sucede en los casos en que la gestión de personal, clientes y proveedores o actividad de un determinado grupo se centraliza en los sistemas de la sociedad matriz, con la finalidad de crear estrategias uniformes; y, b) Por otra parte, las transferencias pueden tener por objeto la prestación de un mejor servicio a los clientes del responsable del fichero. Así sucedería en el caso de prestación al cliente de servicios cuando éste se encuentre en un país distinto al de su residencia habitual.

5. A tenor de la Instrucción 1/2000, de 1 de diciembre de 2000, de la AEPD antes mencionada, se considera movimiento internacional de datos *“toda transmisión de los mismos fuera del territorio español”* y, en particular, *“se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero”*.

El régimen a que se someten los movimientos internacionales de datos de carácter personal queda reducido a los artículos 33 y 34 de la LOPD. En este sentido, en el artículo 33.1 de la LOPD, se establece que *“no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a 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”*.

6. La necesidad de conciliar los derechos de los ciudadanos con el movimiento internacional de datos obliga a que las normas reguladoras de la materia partan de un principio general de prohibición de la transferencia a terceros Estados que no garanticen un nivel de protección adecuado. Ello supone que, en principio, y sin perjuicio de la existencia de supuestos excepcionales, la transferencia queda vedada a empresas situadas en terceros Estados cuya regulación no reconozca el núcleo básico de principios de protección de datos al que nos referimos con anterioridad.
7. La primera cuestión a plantear será, en consecuencia, la de determinar cuándo un tercer Estado ofrece un nivel de protección *“adecuado”*, esto es, cuándo se considera que su regulación incorpora ese núcleo esencial de principios de protección de datos. La Directiva 95/46/CEE ofrece una solución a la cuestión en su artículo 25.2, que reproduce, en lo esencial, el artículo 33.2 de la LOPD, al señalar que *“el carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos de 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, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.”*. Este precepto se verá complementado por el artículo 25.4 de la Directiva 95/46/CEE, según el cual, siempre se considerará que ofrecen un nivel de protección adecuado aquellos terceros Estados respecto de los cuales la Comisión Europea haya declarado la existencia de esa adecuación, lo que también contempla el artículo 34 k) de la LOPD, cuando afirma que no será necesaria autorización del Director de la AEPD *“cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado”*.
8. En consecuencia, sólo serán, en principio, válidas las transferencias efectuadas a los Estados Miembros de la UE y a los Estados cuya adecuación haya sido declarada por la Comisión Europea. Hasta la fecha, sólo se considerarían adecuados los regímenes de los Estados integrantes del Espacio Económico Europeo (Islandia, Noruega y Liechtenstein) y los afectados por las Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE y 2000/520/CE, de 26 de julio (publicadas en el Diario Oficial de las Comunidades Europeas de 25 de agosto de 2000), que consideraron adecuado el nivel de protección de datos personales en Suiza, Hungría, así como de los EE.UU. y Canadá.

9. Finalmente, merece la pena señalar que, a tenor del artículo 12 de la LOPD, cuando la transferencia internacional de datos tenga su fundamento en la *“realización de un tratamiento de datos por cuenta del responsable del fichero”*, los términos en los que se desarrollará el servicio constarán por escrito.

III. Excepciones: régimen de autorización de las transferencias internacionales de datos. ➡

10. Las transferencias de datos no se permiten, con carácter general, *“a países que no proporcionen un nivel de protección equiparable”* al que ofrece la LOPD, salvo que el transmitente cumpla lo previsto en la LOPD y el Director de la AEPD autorice la transmisión *“si se obtienen las garantías adecuadas”*. En este sentido, el artículo 34 de la LOPD contempla, sin embargo, toda una serie de excepciones a la prohibición de la transferencia internacional de datos de carácter personal:
- a. *“ Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.*
 - b. *Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.*
 - c. *Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de Servicios sanitarios.*
 - d. *Cuando se refiera a transferencias dinerarias conforme a su legislación específica.*
 - e. *Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.*
 - f. *Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.*
 - g. *Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.*
 - h. *Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público.*

Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
 - i. *Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.*
 - j. *Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquella sea acorde con la finalidad del mismo.*

- k. *Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado”.*

Cuando el movimiento internacional de datos se realice bajo el amparo de alguno de los apartados a) a j) del artículo 34 de la LOPD, la AEPD podrá requerir al responsable del fichero, *“que aporte la documentación que justifique su alegación”*, en el caso de destinatarios situados en países que no pertenecen a la UE ni al Espacio Económico Europeo, respecto de los cuáles la Comisión Europea no haya declarado que existe un nivel adecuado de protección. Y, cuando la transferencia internacional de datos se base en el supuesto k) del artículo 34 de la LOPD, será el Director de la AEPD quién debe autorizarla. La autorización de la transferencia por la APD se otorgará cuando el *“responsable del fichero aporte un contrato escrito, celebrado entre el transmitente y el destinatario, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos”*.

11. El régimen general de prohibición de la transferencia a terceros Estados que no otorguen un nivel adecuado de protección es objeto de una larga serie de excepciones, contenidas como ya hemos visto en los artículos 33 y 34 de la LOPD, que traen su causa de lo establecido en los artículos 25 y 26 de la Directiva 95/46/CE. Por tanto, dichas excepciones responden a un doble criterio: a) Atienden a las circunstancias concurrentes en el caso concreto que motiva la transferencia (artículo 34 de la LOPD); b) Se fundan en la autorización singular del Director de la APD (artículo 33.1 *in fine* de la LOPD).

- A. En cuanto a las primeras, siguiendo la clasificación contenida en el artículo 26.1 de la Directiva 95/46/CEE, pueden fundarse en seis causas esenciales:

1. Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista, a tenor del artículo 34.e) de la LOPD.
2. Cuando la transferencia se encuentre directamente relacionada con la celebración de un contrato en que sea parte el afectado. En este supuesto cabe incluir dos de las excepciones enumeradas por la LOPD:
 - a. Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado, a tenor del artículo 34.f) de la LOPD; y,
 - b. Cuando se refiera a transferencias dinerarias conforme a su legislación específica, a tenor del artículo 34.d) de la LOPD.
3. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero, en virtud del artículo 34.g) de la LOPD.
4. Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento

médicos o la gestión de servicios sanitarios, en virtud del artículo 34.c) de la LOPD.

5. Cuando la transferencia se funde en un interés público. En este caso cabría hacer referencia a los siguientes supuestos:
 - a. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, según establece el artículo 34.i) de la LOPD;
 - b. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias, a tenor del artículo 34.h) de la LOPD;
 - c. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España, a tenor del artículo 34.a) de la LOPD; y,
 - d. Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional, a tenor del artículo 34.b) de la LOPD.
 6. Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo, según establece el artículo 34. j) de la LOPD.
- B. En caso de no concurrir uno de los supuestos singulares a los que acabamos de hacer referencia, la transferencia aún será posible, siempre y cuando la misma sea debidamente autorizada por el Director de la AEPD.

En este sentido, el artículo 33.1 de la Ley, tras establecer la regla general de prohibición a la que nos referimos en un momento anterior, añade que será posible la transferencia en los supuestos en que *“además de haberse observado lo dispuesto en ésta⁷, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas”*.

Es decir, en aquellos supuestos en que la transferencia no se funde en la existencia en el país de destino de un adecuado nivel de protección o quepa amparar la misma en un supuesto taxativamente enumerado en la Ley, aún será posible la transmisión de los datos si la remitente y la destinataria de los datos adoptan una serie de medidas que, a juicio del Director de la APD, suplan la inseguridad que pudiera existir en el lugar de destino de los datos.

IV. Actividad de la Agencia Española de Protección de Datos en materia de transferencia internacional de datos. ➡

12. De lo hasta ahora comentado, cabe deducir que las normas reguladoras de las

transferencias internacionales de datos establecen un sistema sumamente complicado de reglas generales y excepciones, basadas en el Derecho estatal o autónomo y en el derecho comunitario, que era necesario precisar. Por este motivo, y con la intención de dar cumplimiento a las decisiones de la Comisión Europea adoptadas en este ámbito, la AEPD adoptó, el 1 de diciembre de 2000, la mencionada Instrucción 1/2000 en la que, con una finalidad esencialmente orientativa, se establecen los criterios seguidos por la AEPD, de conformidad con la LOPD y las previsiones de la Directiva, en este ámbito.

13. Así, el apartado primero del Preámbulo de la Instrucción indica que *“la presente Instrucción tiene por objeto señalar los criterios orientativos seguidos por la Agencia de Protección de Datos en relación con aquellos tratamientos que supongan una transferencia internacional de datos, poniendo de manifiesto el procedimiento que, en uso de las competencias que la Ley le atribuye, se sigue por la Agencia en cada caso concreto”*. Por ello, concluye, *“no es finalidad de esta Instrucción efectuar innovación alguna dentro de la normativa reguladora de la protección de datos de carácter personal sino, simplemente, aclarar y facilitar a todos los interesados en un único texto, el procedimiento seguido por la Agencia para dar cumplimiento a las previsiones contenidas en la diversidad de normas que se refieren al movimiento internacional de datos”*.
14. La Instrucción se compone de 6 normas, divididas en dos secciones, referida, la primera, a los criterios aplicables a cualquier transferencia internacional de datos y, la segunda, a supuestos concretos de transferencia. A continuación, se expone, con la mayor claridad posible, el contenido de la Instrucción, atendiendo fundamentalmente a la estructura de la misma:

A. Ámbito de aplicación de la Instrucción.

Según se indica en la Norma primera, la Instrucción resultará de aplicación a cualquier supuesto de transferencia internacional de datos, esto es, a cualquier actividad que suponga la transmisión de datos de carácter personal *“fuera del territorio español”*.

A continuación, la citada Norma diferencia dos supuestos concretos de transferencia, al indicar que *“en particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero”*. Ello supone que, a efectos de la aplicación de las normas reguladoras de las transferencias internacionales de datos, carece de relevancia el hecho de que la entidad destinataria de los datos utilice los mismos en su propio beneficio o únicamente para realizar una actividad complementaria de la efectuada por la entidad española que transmite los datos, dado que las normas que regulan las transferencias tiene por objeto evitar los perjuicios que pueden derivarse de la salida de los datos a territorio de terceros Estados, siendo éstos similares en uno u otro caso. En consecuencia, las medidas que nuestra LOPD prevé serán igualmente aplicables a supuestos en que exista una venta de datos y aquellos otros en los que los datos simplemente se encuentren alojados en un servidor situado fuera de España.

B. Aplicación de los principios de protección de datos de la LOPD.

La Norma segunda de la Instrucción contiene un principio esencial que, como indica el apartado segundo de su Preámbulo, gobierna todo el régimen

regulador de transferencias internacionales. Según indica este principio, contenido en el artículo 25.1 de la Directiva 95/46/CEE, *“la transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento”*. Por ello, y con independencia del supuesto de transferencia ante el que nos encontremos, la recogida y tratamiento de los datos en España deberá respetar en su integridad los principios contenidos en la Ley, debiendo obtenerse el consentimiento del afectado salvo cuando la LOPD permita el tratamiento incontestado de los datos (artículo 6 de la LOPD), siendo el consentimiento expreso en los casos que prevé la Ley (artículo 7 de la LOPD) informando al interesado del tratamiento, su finalidad, destinatarios de los datos y posibilidad de ejercitar sus derechos (artículo 5 de la LOPD), ajustándose a los principios de calidad de datos y finalidad, sin que los datos puedan utilizarse para fines incompatibles con los que motivan su recogida (artículo 4 de la LOPD), imponiéndose al responsable del fichero los deberes de seguridad (artículo 9 de la LOPD) y secreto profesional (artículo 10 de la LOPD) y permitiendo a los interesados ejercitar sus derechos, en los términos que la LOPD establece.

C. Deberes formales del transmitente de los datos.

La Norma tercera de la Instrucción desarrolla el modo en que deberá darse cumplimiento a la obligación de notificar la transferencia internacional de datos al RGPD, integrado en la AEPD.

En cuanto al procedimiento para el cumplimiento de este deber, la Instrucción establece las siguientes reglas:

- La notificación de la transferencia se efectuará en los términos que se contengan en el modelo normalizado aprobado a tal efecto por el Director de la APD, con expresa indicación del país al que se pretende efectuar la transferencia y de los motivos que, en su caso, la habilitan, conforme a lo dispuesto en el artículo 34 de la citada LOPD, para no recabar la autorización expresa del Director de la AEPD.
- Recibida la notificación, la AEPD podrá requerir al responsable del fichero para que, en el plazo de diez días, aporte la documentación necesaria para completar la información relativa a la transferencia internacional contenida en aquélla, así como la identidad del receptor de la misma. En particular, podrá solicitar que se acredite la existencia de consentimiento o relación contractual que habilite la transferencia.
- Al requerirse la información a la que se refiere este apartado se indicará al responsable del fichero que, en caso de no ser aquélla aportada en el plazo de diez días, se le tendrá por desistido de su petición de inscripción o modificación, archivándose ésta.
- Si con la documentación aportada no se acreditara el cumplimiento de los requisitos contenidos en la LOPD, el Director de la AEPD, en ejercicio de las competencias que le atribuye dicha LOPD, denegará la inscripción o su modificación.

La denegación así producida surtirá un importante efecto, dado que la

inscripción del fichero en el RGPD es requisito previo y necesario para que el tratamiento de los datos de carácter personal pueda entenderse realizado de conformidad con lo establecido en la Ley. Por ello, la realización de una transferencia internacional no inscrita debidamente en el RGPD podría dar lugar a la imposición de una sanción en materia de protección de datos, siendo esta muy grave cuando los datos sean transferidos *“con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos”*.

D. Normas especiales atendiendo al país de destino de los datos.

En virtud de las Normas cuarta y quinta, podemos distinguir los siguientes supuestos:

1. *Transferencia a Estados Miembros de la Unión Europea o del Espacio Económico Europeo.*

La Ley no prevé especialidades respecto de estos países, excluidos de cualquier autorización del Director de la AEPD por su artículo 34.k) de la LOPD. Por este motivo, únicamente será necesario el cumplimiento de las disposiciones de la Ley en la recogida y tratamiento previos a la transferencia y la notificación de la misma al RGPD.

2. *Transferencia a países respecto de los que se haya declarado un nivel adecuado de protección.*

Como regla general rige un efecto similar al indicado en el epígrafe anterior. No obstante, la Instrucción, atendido lo establecido en las Decisiones de la Comisión Europea por las que se declara la adecuación de Suiza, Hungría y entidades de los EE.UU.⁸ y Canadá⁹, adheridas a los denominados “principios de Puerto Seguro”¹⁰, establece dos precisiones, una general y otra referida al último de los supuestos citados.

En cuanto a la previsión general, se prevé la posibilidad de que el Director de la AEPD pueda impedir una transferencia concreta o suspender una serie sucesiva de transferencias a estos países en caso de que la destinataria de los datos haya incumplido su Ley nacional o existan indicios de dicho incumplimiento y la autoridad del Estado destinatario no adopte medidas para impedirlo, causando un perjuicio a los afectados.

Por lo que respecta a la regla especial, se prevé que en las transferencias sujetas al denominado “puerto seguro” se acredite *“que el destinatario se encuentra entre las entidades que se han adherido a los principios, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión”*.

Ello se debe a la complejidad del régimen de “puerto seguro”, constituido por una serie de principios de autorregulación a los que las entidades de los EE.UU. podrán libremente adherirse. El único modo de comprobar la existencia de dicha adhesión, que impone el sometimiento a la decisión de un Organismo público de los Estados Unidos de América es que aquél certifique la efectividad de esa adhesión. Por ello, la transferencia será posible siempre que se aporte esa certificación.

3. *Transferencia a países que no ofrezcan un nivel adecuado de protección.*

Como ya se expuso, en este caso es posible la transferencia internacional de datos siempre que la misma o bien se encuentre amparada por una de las excepciones específicas que establece el artículo 34 de la LOPD, o bien haya sido objeto de una expresa autorización del Director de la AEPD.

E. Especialidades en caso de tratamiento por cuenta del transmitente.

Por último, la Norma sexta recoge las especialidades en caso de que el destinatario se limite a realizar una actividad por cuenta del transmitente de los datos, en términos similares a los establecidos en el artículo 12 de la LOPD.

En este caso, y sin perjuicio del cumplimiento de las previsiones que correspondan, atendiendo al país en que se ubique el destinatario, será necesaria la existencia de un contrato escrito que regule la prestación. Dicho contrato deberá indicar expresamente *“que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normas de protección de datos del Derecho español”*, debiendo además restituir o destruir los datos al término del contrato y no cederlos, ni siquiera para su conservación, a terceras personas.

Como especialidades, se prevé que los datos no podrán ser objeto de subcontratación por el destinatario de los mismos y que el contrato deberá hacer constar *“la responsabilidad directa de la transmitente como consecuencia de cualquier incumplimiento de la Ley en que incurriera el destinatario”*.

V. Aspectos de Derecho internacional privado relacionados con la transferencia internacional de datos. ➔

15. La internacionalización de las relaciones privadas hace necesario contemplar la responsabilidad civil extracontractual en materia de protección de datos de carácter personal desde una perspectiva *iusprivatista* en la medida en que son frecuentes los supuestos que se producen, no con ocasión de las denominadas “relaciones transfronterizas” sino con las que se producen en un ámbito más amplio. En este sentido, son tres las cuestiones que se plantean: primera, la Competencia judicial internacional; segunda, el Derecho aplicable al fondo del asunto; y, tercera, el Reconocimiento y ejecución de decisiones extranjeras en esta materia.

1. Competencia judicial internacional.

16. Para determinar la Competencia judicial internacional en materia de protección de datos de carácter personal, debemos acudir a los siguientes instrumentos normativos: el Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Bruselas, el 27 de septiembre de 1968 (en adelante, CB)¹¹, el Convenio relativo a la competencia judicial y a la ejecución de resoluciones

judiciales en materia civil y mercantil, hecho en Lugano, el 16 de septiembre de 1988 (en adelante, CL) ¹², el Reglamento (CE) nº 44/2001, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Reglamento “Bruselas I”- en adelante, RB-) ¹³ y, en su defecto, el artículo 22 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ) ¹⁴.

La estructura de los foros de competencia judicial internacional del Convenio de Bruselas de 1968, del Convenio de Lugano de 1988 y del Reglamento “Bruselas I”, se construye sobre tres niveles: a) El primer nivel está constituido por las competencias exclusivas previstas en el artículo 16 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988 (art. 22 del Reglamento “Bruselas I”). En determinadas materias, este precepto atribuye competencia única y exclusiva a los Tribunales de un Estado miembro, excluyendo absolutamente la posibilidad de que conozcan cualesquiera otros Tribunales. Si se trata de una de las materias previstas en el artículo 16, éste designará el único Tribunal del Estado competente posible.

Si no se trata de una de las materias previstas en el artículo 16 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988, es preciso recurrir al segundo escalón en el orden jerárquico: la sumisión expresa. La voluntad de las partes, con las condiciones y límites establecidos en los artículos 17, 12 y 15 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988 (13, 17 y 21 del Reglamento “Bruselas I”), atribuye competencia exclusiva a los Tribunales designados por las partes. No obstante, el acuerdo de sumisión a los Tribunales de un Estado miembro siempre puede ser modificado tácitamente, mediante la sumisión por ambas partes a otros Tribunales (art. 18 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988 y, 24 del Reglamento “Bruselas I”).

Finalmente, el tercer escalón jerárquico de las reglas de Competencia judicial opera en defecto de sumisión expresa o tácita por las partes y siempre que no se trate de una de las materias objeto de competencias exclusivas previstas en el artículo 16 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988 (art. 22 del Reglamento “Bruselas I”). En tales casos, serán competentes, indistintamente, los Tribunales del domicilio del demandado (art. 2 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988, así como, art. 2 del Reglamento “Bruselas I”) o los designados por los foros especiales de competencia previstos en los artículos 5 a 15 del Convenio Bruselas de 1968 y del Convenio de Lugano de 1988 (5 a 21 del Reglamento “Bruselas I”). Así, en lo que respecta a la responsabilidad civil extracontractual en materia de protección de datos de carácter personal, establece el artículo 5.3 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988 que, “Las personas domiciliadas en un Estado contratante podrán ser demandadas en otro Estado contratante... en materia delictual o cuasidelictual, ante el Tribunal del lugar donde se hubiere producido el hecho dañoso...”; en este sentido, el artículo 5.3 del Reglamento “Bruselas I”, permite la indeterminación del lugar de producción del hecho dañoso al señalar que “Las personas domiciliadas en un Estado miembro podrán ser demandadas en otro Estado miembro... en materia delictual o cuasidelictual, ante el Tribunal del lugar donde se hubiere producido o pudiese producirse el hecho dañoso...”.

17. Por tanto, en general, en materia de responsabilidad civil extracontractual y, en particular, en lo que a la responsabilidad civil extracontractual en materia de protección de datos de carácter personal respecta, en aplicación del CB, CL o RB, los criterios atributivos de competencia son los siguientes:

- a. El foro del domicilio del demandado, esto es, los Tribunales del país donde esté domiciliado el presunto vulnerador-demandado conocerá de todas las pretensiones que se deduzcan contra él, independientemente del país o países en los que se haya producido el hecho dañoso;
- b. El foro de la sumisión, expresa o tácita, que nos permite concentrar los litigios a los que las partes se refieran, bajo el conocimiento de los Tribunales de un solo país; y,
- c. El foro del lugar del hecho dañoso, que atribuye competencia a los Tribunales del “lugar donde se hubiere producido o pudiere producirse el hecho dañoso”¹⁵ del que nace la responsabilidad extracontractual, pudiendo considerarse como “país donde ocurre el hecho dañoso” tanto el país donde ocurre el hecho causal como el país donde se verifica el resultado lesivo, siendo el demandante el que decida ante qué Tribunales interponer la correspondiente demanda¹⁶.

18. Por último, debemos acudir a la LOPJ que, en su artículo 22, recoge las normas de competencia judicial internacional aplicables para que un órgano jurisdiccional español se declare competente, ante la imposibilidad de aplicación del Convenio de Bruselas, Convenio de Lugano o del Reglamento “Bruselas I”. La LOPJ recoge en su artículo 22.1º, en primer término, una serie de foros de competencia que presentan “carácter exclusivo” y que se inspiran y coinciden en buena medida con los previstos en el artículo 16 del Convenio de Bruselas de 1968 y del Convenio de Lugano de 1988.

El artículo 22.2º recoge dos foros generales que atribuyen competencia a los órganos jurisdiccionales cualquiera que sea la materia afectada: sumisión a los Juzgados o Tribunales españoles y domicilio del demandado en España. En este sentido, y en esta materia, en el artículo 22.3º se establece que “los Juzgados y Tribunales españoles serán competentes... en materia de obligaciones extracontractuales, cuando el hecho de que derivan haya ocurrido en territorio español o el autor del daño y la víctima tengan su residencia habitual común en España...”.

2. Derecho aplicable.

19. Siguiendo a CALVO CARAVACA y CARRASCOSA GONZÁLEZ,¹⁷ la determinación de la Ley aplicable en materia de responsabilidad civil extracontractual derivada del tratamiento automatizado de datos de carácter personal queda en manos de dos preceptos:

- a. El artículo 4 de la Directiva 95/46/CE, que señala como ley aplicable

la Ley del lugar donde esté ubicado el responsable del fichero; y,

- b. El artículo 2.1 de la LOPD, que, por el contrario, establece como ley aplicable la Ley del lugar donde se haya efectuado el tratamiento de los datos de carácter personal.

En resumen, sólo será de aplicación la LOPD, esto es la Ley española, cuando el tratamiento de los datos de carácter personal sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento, mientras que, cuando no sea así, será de aplicación la Ley del país de residencia del fichero, en virtud de la Directiva 95/46/CEE.

20. Es interesante reseñar, en este sentido, que el propio artículo 4 de la mencionada Directiva 95/46/CEE, concreta el criterio de la “ubicación del fichero” en dos supuestos concretos, en los que resulta especialmente difícil localizar el país de situación del fichero que trata los datos de carácter personal:

- a. Según el artículo 4.1.a) de la Directiva 95/46/CEE, si el responsable del fichero posee distintos establecimientos en diferentes Estados de la UE, el tratamiento de datos de carácter personal realizado “en el marco de las actividades de cada establecimiento se rige por la Ley del país donde radica cada establecimiento”; y,
- b. Según el artículo 4.1.b) de la Directiva 95/46/CEE, en el supuesto de que un responsable del tratamiento establecido en un lugar que no pertenece al territorio de un Estado miembro de la UE, pero en el que se aplica la Ley de un Estado miembro en virtud del Derecho internacional público, será de aplicación la Ley del país de establecimiento del responsable del fichero, con independencia del país donde esté situada la Embajada o Consulado correspondiente.

21. Si los datos de carácter personal fueran trasladados a terceros países para su tratamiento, los supuestos a contemplar serían los siguientes:

- a. Cuando se produce una transferencia de datos a terceros países que garantizan un “nivel de protección adecuado” del derecho a la intimidad frente a la informática, la transferencia está permitida y, por tanto, es de aplicación el artículo 10.9 del CC, que señala que el tratamiento de los datos de carácter personal se regirá por la Ley del país donde se lleve a cabo dicho tratamiento;
- b. Cuando se trata de una transferencia de datos a terceros países que no garantizan un “nivel de protección adecuado” del derecho a la intimidad frente a la informática, la transferencia está, en principio, prohibida y, la Ley aplicable a dicha responsabilidad será la Ley del país donde radica el establecimiento responsable de la cesión internacional de datos, pues el envío de datos de carácter personal a otro país constituye en sí mismo un tratamiento de datos de carácter personal, según señala el artículo 2.b) de la Directiva 95/46/CEE; y,
- c.

Cuando se produce un tratamiento de datos de carácter personal en un país de la UE pero realizado en el marco de actividades de un fichero situado fuera de la UE, la Ley aplicable será la Ley del Estado miembro de la UE donde se haya realizado el tratamiento de los datos de carácter personal.

22. No obstante, será el Convenio sobre la ley aplicable a las obligaciones contractuales de 1980 (en adelante, CR) ¹⁸ el que nos da la solución al respecto, cuando el tratamiento de datos de carácter personal sea como consecuencia de un contrato interpartes, al fijar como criterios de determinación de la ley aplicable los siguientes:

- a. En primer término, la Ley aplicable será la Ley elegida por las partes (artículo 3.1 del CR); y,
- b. En segundo término, en defecto de elección de la Ley estatal por los afectados, será de aplicación la Ley del país de residencia habitual del prestador característico (artículo 4.2 del CR), teniendo en cuenta, a estos efectos, que la situación física del servidor de *Internet* es irrelevante pues lo que interesa es la residencia del prestador característico y, que esta presunción del artículo 4.2 del CR debe decaer no sólo cuando es imposible identificar los elementos necesarios que permiten operar a las presunciones sino también cuando del conjunto de circunstancias del contrato resulta que éste presenta vínculos más estrechos con otro país (artículo 4.5 del CR).

3. Reconocimiento y ejecución de decisiones extranjeras.

23. En materia de Reconocimiento y ejecución de decisiones extranjeras podemos afirmar, de forma categórica, que no existen disposiciones normativas específicas en materia de protección de datos de carácter personal, por lo que deben de ser aplicados, de nuevo, los instrumentos convencionales internacionales, de carácter bilateral y multilateral, esto es, el CB, el CL y, el RB; y, en su defecto, las normas de régimen autónomo, esto es, los artículos 951 y ss. de la Ley de Enjuiciamiento Civil de 1881 ¹⁹

Quizás, el mayor problema en cuanto a la eficacia en España de las decisiones judiciales extranjeras relativas a los tratamientos de datos de carácter personal, y, en particular, cuando se producen en *Internet*, plantea especial atención en dos supuestos, acertadamente señalados por DE MIGUEL ASENSIO ²⁰ :

- por un lado, en lo referente al control de la competencia del órgano jurisdiccional emisor de la resolución judicial con el objeto de prevenir situaciones en las que se le haya atribuido la competencia a un órgano jurisdiccional escasamente vinculado con el litigio;
- y, por otro lado, en el plano contractual, en la posibilidad de denegar la eficacia en España de una decisión extranjera dictada vulnerando una cláusula atributiva de competencia válida incluida en el contrato, a favor de los órganos jurisdiccionales españoles, sobre todo en

materia de contratos de consumo, pues se debe garantizar que dicha decisión extranjera no se ha dictado vulnerando ninguno de los denominados “foros de protección” previstos en dichos instrumentos normativos.

VI. Conclusiones finales. ➔

24. Del estudio del régimen a que se someten los movimientos internacionales de datos de carácter personal podemos extraer dos conclusiones:
- a. Por un lado, en virtud de la LOPD, *“no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a 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”*. Además, no se permiten transferencias de datos *“a países que no proporcionen un nivel de protección equiparable”* al que ofrece la LOPD, salvo que el transmitente cumpla lo previsto en la LOPD y el Director de la AEPD autorice la transmisión *“si se obtienen las garantías adecuadas”*; y,
 - b. Por otro lado, señalar que ante los supuestos de transferencia internacional de datos hay que considerar diferentes variables:
 - a. La naturaleza de los datos que se van a transferir;
 - b. La finalidad del tratamiento que se efectuará en el extranjero;
 - c. La duración de dicho tratamiento;
 - d. El país origen de los datos;
 - e. El país de destino final de los mismos;
 - f. La legislación vigente en el país de destino en materia de protección de datos personales;
 - g. El contenido de los dictámenes emitidos por la Comisión de la UE respecto al nivel de protección que otorgan determinados países en materia de protección de datos personales;
 - h. Concretas normas profesionales, si fueran aplicables; y,
 - i. Las medidas de seguridad que estén en vigor en el país de destino de los datos.
25. Los posibles problemas de vulneración de datos personales en materia de

transferencia internacional de datos de carácter personal serán resueltos, cuando la situación revista carácter privado e internacional, aplicando las normas de Derecho internacional privado español relativas a la responsabilidad civil extracontractual:

- a. Respecto de la Competencia judicial internacional, debemos señalar que dependiendo del domicilio del demandado, serán de aplicación los Tribunales del lugar donde se ha producido o pudiere producirse el hecho dañoso, esto es, el “forum delicti commissi” (artículo 5.3 CB / CL, artículo 5.3 RB o Artículo 22.3.regla VIII LOPJ);
- b. En materia de determinación del Derecho aplicable, es de destacar que la Directiva 95/46/CE señala que la ley nacional es aplicable “cuando el procesamiento se efectúa en el marco de las actividades del responsable del procesamiento sobre el territorio del estado miembro” y, el responsable del procesamiento es aquella persona física que “sola o conjuntamente con otros, determina las finalidades y los medios de tratamiento de tipo personal”; y,
- c. Por último, con respecto al Reconocimiento y ejecución de cualquier decisión judicial extranjera en materia de protección de datos personales serán de aplicación, dependiendo del domicilio del demandado las normas de Derecho internacional privado español (artículos 25 y ss. CB / CL, artículos 32 y ss. RB y, artículos 951-958 LEC 1889).

VII. Bibliografía consultada. ➔

- CALVO CARAVACA, Alfonso Luis y CARRASCOSA GONZÁLEZ, Javier, Conflictos de leyes y conflictos de jurisdicción en Internet, Colex, Madrid, 2001.
- CARRASCOSA GONZÁLEZ, Javier, “Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado”, en Revista Española de Derecho Internacional, vol. XLIV, núm. 2, 1992.
- CARRASCOSA GONZÁLEZ, Javier, “Circulación internacional de datos personales informatizados y la Directiva 95/46/CE, en Actualidad Civil, núm. 23, 1997.
- DE MIGUEL ASENSIO, Pedro, Derecho privado de Internet, Civitas, 3ª edición, Madrid, 2002.
- DEL PESO NAVARRO, Emilio, Ley de Protección de Datos. La nueva LORTAD, Ediciones Díaz de Santos, Madrid, 2000.
- ESTEVE GONZÁLEZ, Lydia (Coord.) y otros, Derecho e Internet. Textos Jurídicos Básicos, Editorial Compás, Alicante, 2001.
- MAYOL GIL, Juan Antonio, MEDRÁN VIOQUE, Rafael y ORTEGA GIMÉNEZ, Alfonso, “Data Protection in Internet”, en REDi: Revista Electrónica de Derecho Informático, núm. 50, 2002.
- MAYOL GIL, Juan Antonio, MEDRÁN VIOQUE, Rafael, MIESKES, Manfred y ORTEGA GIMÉNEZ, Alfonso, “Comparative analysis between spanish and german

law concerning data protection in internet" en uaipit.com -Portal de la Universidad de Alicante sobre Propiedad Industrial e Intelectual y Sociedad de la Información- (http://www.uaipit.com/en/ITL/Data_Protection_Internet.pdf), 2003.

- ORTEGA GIMÉNEZ, Alfonso, "Censo promocional y consentimiento del afectado" en IURIS. Actualidad y Práctica del Derecho, Número 68, La Ley, Madrid, Enero 2003.
- ORTEGA GIMÉNEZ, Alfonso, "La protección de datos de carácter personal en Internet (con especial referencia a la transferencia internacional de datos)" en uaipit.com -Portal de la Universidad de Alicante sobre Propiedad Industrial e Intelectual y Sociedad de la Información-, 2003.
- ORTEGA GIMÉNEZ, A., "Transferencia de datos personales entre la Unión Europea y EEUU" en IURIS. Actualidad y Práctica del Derecho, Número 83, La Ley, Madrid, Mayo 2004.

1:

Vid. VV. AA., Guía práctica de la Ley Orgánica de Protección de datos, edición en cd-rom, Deloitte & Touche, 2002, pp. 46-62, y ORTEGA GIMÉNEZ, Alfonso, "La protección de datos de carácter personal en Internet (con especial referencia a la transferencia internacional de datos)" en uaipit.com -Portal de la Universidad de Alicante sobre Propiedad Industrial e Intelectual y Sociedad de la Información-, 2003.

➡

2:

Texto disponible en la Sección de Documentos (Legislación Nacional) de [UAIPIIT](#)

➡

3:

Consecuentemente, las Órdenes del Ministerio de Justicia de 2 de febrero de 1995 y de 31 de julio de 1998, realizan una "Lista blanca" de países respecto de los cuales se reconoce que otorgan una protección equivalente.

➡

4:

DOCE L nº 281, de 23/11/1995. Texto disponible en Sección de Documentos (Unión Europea) de [UAIPIIT](#)

➡

5:

Texto disponible en Sección de Documentos (Legislación Nacional) de [UAIPIIT](#)

➡

6:

Texto disponible en [AGPD](#)

➡

7:

Nos estamos refiriendo a la mencionada LOPD.

➡

8:

Mediante la Decisión de la Comisión Europea 2000/520/CE, de 26 de julio se autorizaba la transferencia de datos de carácter personal entre la UE y los EE.UU.

➡

9:

El 1 de enero de 2002, la Comisión Europea reconoció que Canadá tenía un régimen adecuado de protección con lo que autorizaba la transferencia de datos de carácter personal entre la UE y Canadá.

➡

10:

Vid. ORTEGA GIMÉNEZ, A., "Transferencia de datos personales entre la Unión Europea y EEUU" en IURIS. Actualidad y Práctica del Derecho, Número 83, La Ley, Madrid, Mayo 2004, pp. 66-68.

➡

11:

DOCE 1998 C 27/3. Texto disponible en la Sección de Documentos (Unión Europea) de [UAIPIT](#)

➡

12:

BOE núm. 243, de 10 de octubre de 1979. Texto disponible en la Sección de Documentos (Legislación Nacional) de [UAIPIT](#)

➡

13:

DOCE 2001 L 12/1. Texto disponible en la Sección de Documentos (Unión Europea) de www.uaipit.com.

➡

14:

BOE núm. 157, de 2 de julio de 1985. Texto disponible en la Sección de Documentos (Legislación Nacional) de [UAIPIT](#)

➡

15:

No obstante, en materia de responsabilidad civil extracontractual derivada del tratamiento automatizado de datos de carácter personal, debemos destacar que el hecho dañoso se produce en el país donde radica el fichero. Ahora bien, esto no tiene por qué ser siempre así, ya que, por ejemplo, si la actividad consiste en la recogida ilícita de datos en España para su ulterior almacenaje informático en un fichero sito en Lisboa, el lugar del daño es tanto España como Portugal. Y, en otras ocasiones, el daño puede ser consecuencia de la vulneración de un contrato interpartes, en cuyo caso no es el mencionado artículo 5.3 del RB aplicable sino el artículo 5.1 del RB, que concede competencia a los Tribunales del país en el que se incumplió la obligación contractual, por lo que, siguiendo con nuestro ejemplo, si según el contrato, los datos debían tratarse en Portugal y allí son objeto de tratamiento ilegal, los Tribunales lusos son competentes, sin perjuicio de la competencia de los Tribunales del país del domicilio del demandado (a tenor del artículo 2 del RB) o de los Tribunales pactados, expresa o tácitamente (artículos 23 ó 24 del RB).

➡

16:

Así, p. ej., ante un ilícito civil en Internet se podrían declarar competentes los Tribunales del país en que se ha procedido a introducir el contenido ilícito en Internet o, los del país desde el que se ha accedido al contenido ilícito vertido en Internet.

➡

17:

Vid. CALVO CARAVACA, Alfonso Luis y CARRASCOSA GONZÁLEZ, Javier, Conflictos de leyes y conflictos de jurisdicción en Internet, Colex, Madrid, 2001, pp. 58-83.

➡

18:

Texto disponible en la Sección de Documentos (Unión Europea) de [UAIPIT](#)

➡

19:

Texto disponible en la Sección de Documentos (Legislación Nacional) de UAIPIT



20:

Vid. DE MIGUEL ASENSIO, Pedro, Derecho privado de Internet, Civitas, 3ª edición, Madrid, 2002, pp. 495-496.

