Transferencia internacional de datos sanitarios

International transfer of health data

María Ascensión Martín Huertas

Profesora Contratada Doctora de la Universidad de Sevilla. España.

Resumen: Los datos genéticos, como las muestras que los contienen, si están identificados o son identificables (codificados o disociados de forma reversible) se consideran datos de carácter personal que por afectar a la salud del individuo tienen, además, la categoría de sensibles. Esta última nota impone que haya que garantizarles un Nivel de Seguridad Alto por lo que han de cumplir todos los requisitos que legalmente se establecen, entre otras cuestiones, cuando son objeto de una Transferencia Internacional. La finalidad perseguida por la regulación sobre Transferencias Internacional de Datos (TID) es evitar la vulneración del derecho a la protección de datos una vez transferidos a terceros países. En el presente análisis se estudia dicha cuestión tal y como se contempla en el ordenamiento jurídico español. En su mecánica de actuación se parte de un principio general: la transferencia de datos personales de un Estado a un tercer país sólo podrá efectuarse cuando éste garantice un nivel de protección adecuado; o bien, cuando preste las garantías adecuadas que aseguren la protección de los datos personales. Fuera de estas hipótesis el resto de transferencias requieren la autorización del Director de la Agencia Española de Protección de Datos. Finalmente, hay que tener en cuenta que se ha elaborado una propuesta de Reglamento por parte del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos que va a suponer, cuando entre en vigor, una adaptación de toda esta normativa a la era digital y, por ello, implicará, sin lugar a dudas, una mayor operatividad de las TID.

Palabras-claves: Datos sanitarios; transferencia internacional; niveles de protección; Ordenamiento jurídico español.

Abstract: *The genetic data, as well as samples containing them, when they are identified or identifiable (coded or dissociated reversibly) are considered personal data that for affecting the individual's health are also considered as a sensitive category. The latter characteristic imposes that they have to be ensured with a High Security Level for what they have to fulfil all the requirements legally established, among other cases, when they are subject to an International Transfer. The objective pursued by the regulation of the International Data Transference (IDT) is to prevent the violation of the right to data protection once transferred to third countries. In the present analysis we study how this issue is contemplated in the Spanish legal system. In its mechanical performance we start from a general principle: the transfer of personal data from one State to a third country can only take place when an adequate level of protection is provided; or, when the appropriate safeguards are offered to ensure the protection of*

personal data. Outside these scenarios the rest of transfers require the approval of the Director of the Spanish Agency for Data Protection (so-called «Agencia Española de Protección de Datos»). Finally, we must bear in mind that it has been developed a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to processing of personal data and on the free movement of such data, which will suppose, when in force, an adaptation of all this legislation to the digital age and, therefore, mean an indubitable greater operability of the IDT.

Key-words: *Health information; International transfer; levels of protection; Spanish legal system.*

Introducción[1]

Al poner en conexión el derecho a la investigación con el derecho a la salud, es necesario partir del reconocimiento de la vida humana como bien primario que está en la base de cualquier otro bien. No se puede perder de vista, en este contexto, que tanto el derecho a la salud como el derecho a la investigación son dos derechos fundamentales reconocidos como tales tanto en la Constitución española (arts. 43 y 44.2, respectivamente) (España, BOE, 1978, p. 29313-29424), como en diversos instrumentos internacionales (por ejemplo, en el Convenio sobre Derechos Humanos y Biomedicina del Consejo de Europa, de 4 de abril de 1997[2]; Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (España, BOE, 1985, p. 36000-36004).

En la actualidad se ofrece como punto de reflexión bioética el de los derechos de la persona contrapuestos a los derechos de los investigadores, esto es, el problema de la investigación científica debe ser armonizado con los derechos de los individuos en la salvaguarda de su integridad. Se impone como ineludible la tarea de individualizar los principios que deben presidir la rectitud del comportamiento de los investigadores en la utilización del material biológico. Se trata de principios bien conocidos en la bioética que buscan, sobre todo, la obligación de evaluar los riesgos/beneficios que debe preceder cada participación en el protocolo de investigación y el privilegio dado en línea de máxima del anonimato bajo diversas

[1] El presente texto se enmarca en el Proyecto de Investigación PRY 149/11, del Centro de Estudios Andaluces, sobre la regulación de los Biobancos en Andalucía, bajo la dirección de la Doctora Cecilia Gómez-Salvago Sánchez.

[2] Este Convenio fue aprobado y suscrito por representantes de 20 países, miembros del Consejo de Europa, en una reunión celebrada en Oviedo, España, siendo ratificado por dicho país el 23-julio-1999 (España, *BOE*, 1999 (b), p. 36825- 36830). El Convenio relaciona la bioética con la defensa y pomoción de los derechos humanos, especialmente en el ámbito de la biomedicina.

formas de las muestras y de los datos para un evidente refuerzo de la tutela de la *privacy*, a menos que la tutela del material biológico o de los datos asociados en forma no anónima (esto es, identificada o codificada) no responda al interés del sujeto o sea aprobada por el mismo.

No obstante, la investigación presenta una indudable dimensión social. De ahí que, en el debido respeto a los derechos individuales y el respeto a la vida privada pueda ser instrumento de una nueva forma de solidaridad entre los grupos y entre las generaciones basada en compartir voluntariamente la información y los hallazgos obtenidos. De este modo, los beneficios no se deben limitar a los individuos que participan en la investigación, sino que deben ser compartidos con todos. En este sentido, sería necesario evitar que laboratorios privados sean financiados con contratos de exclusividad que favoreciendo una lógica competitiva, tiendan a perjudicar la investigación pública y la cooperación solidaria internacional. Se debe obviar, en particular, el llamado "colonialismo científico", concretamente, el de países en vías de desarrollo: de un lado, mediante un uso indiscriminado de material genético proveniente de países considerados óptimos recursos para muestras biológicas dada la presencia de familias numerosas de fuerte consanguinidad; de otro, a través de la no comunicación y aplicación de los beneficios resultantes de la investigación misma a tales países. De este modo, las eventuales entidades comerciales que recabasen ganancias de las investigaciones genéticas en dichos países deberían usar parte de las ganancias en potenciar las infraestructuras sanitarias o en la adquisición de vacunas farmacéuticas o tratamientos a nivel local, nacional o internacional, en vista de la finalidad que se pretende conseguir.

En el caso concreto de España, el legislador español ha potenciado claramente la libertad de investigación con la Ley 14/2007, de 3 de julio, de Investigación Biomédica (en adelante LIB) (España. BOE, 2007, p. 28826-28848). Sin embargo, la Ley no agota toda la investigación biomédica, sino determinados tipos que interesa potenciar porque a nivel jurídico y social constituyen un problema. Se establece por tanto, como línea de principio la libertad de investigación, pero con los debidos controles que se actúan a través de los llamados Comités de Bioética.

Resulta necesario, en definitiva, evaluar hasta qué punto la investigación científica puede suponer un riesgo para la salud del ser humano individualmente considerado, en atención a la defensa del interés general. Las soluciones que se den en este ámbito deben llegar a un encuentro entre los intereses de los particulares (afirmados en cualquier caso prevalentes en el art. 2 del Convenio sobre Derechos

Humanos y Biomedicina del Consejo de Europa de 1997)[3] y los intereses para el progreso social y la ciencia en la futura aplicación biomédica. De todos modos, ningún daño ni discriminación de la persona puede ser consentido en este contexto, ya que el debido respeto a la libertad y dignidad del hombre constituyen un mínimo ético irrenunciable.

En el ámbito europeo, el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea[4] consagra el derecho a la protección de datos personales como un derecho con carácter autónomo, distinto del derecho a la tutela de la vida privada. Además, la Constitución contempla la necesidad de crear una autoridad independiente sólo para la protección de datos personales, lo que enfatiza dicho carácter. El artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE), introducido por el Tratado de Lisboa[5], establece el principio según el cual toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. Además, con el artículo 16, apartado 2, del TFUE, el Tratado de Lisboa introdujo una base jurídica específica para la adopción de normas relativas a la protección de datos de carácter personal por parte de las instituciones, órganos y organismos, y por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y de normas relativas a la libre circulación de estos

---

[3] Artículo 2. "Primacía del ser humano.
El interés y el bienestar del ser humano deberán prevalecer sobre el interés exclusivo de la sociedad o de la ciencia".

[4] Hecha en Niza el 7 de diciembre de 2000 (*DO* 83, de 30 de marzo de 2010). Entrada en vigor el 1 de diciembre de 2009. Versión consolidada publicada en el *DO* C 326, de 26 de octubre de 2012.
Artículo 8. Protección de datos de carácter personal
"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la
persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene
derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[5] Hechos en Lisboa el 13 de diciembre de 2007 (España, *BOE*, 2009). Entrada en vigor el 1 de diciembre de 2009. Versión consolidada publicada en el *DO* C, 326, de 26 de octubre de 2012.
Artículo 16
"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.
Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea".

datos. Por su parte, el art. 8 de la Directiva europea 95/46[6], prevé una regulación específica para los datos sensibles, dentro de los que se incluyen claramente los datos de salud.

En palabras de Rodotá (2003, p. 17),

> el hecho de que nuestra vida se esté transformando sin duda en un canje continuo de informaciones, y de que vivimos en un flujo continuo de datos, ha atribuido a la protección de datos una importancia creciente, desplazándola hacia el centro del sistema político-institucional, y atribuyéndola una importancia creciente y autónoma.

En este "mundo feliz de datos" necesitamos un robusto conjunto de reglas sobre su protección que estén hechas a prueba de futuro y se adapten a la era digital. El gran protagonismo que en los últimos años han experimentado las cuestiones relativas a la intimidad y a la protección de datos ha venido propiciado porque la tecnología ha ido avanzando a un ritmo exponencial, aportando grandes cambios a la forma en que se utilizan los datos personales.

En particular, los datos afectantes a la salud se consideran que tienen la categoría de sensibles[7]. Esta última nota impone que haya que garantizarles un nivel de seguridad alto por lo que han de cumplir todos los requisitos que legalmente se establecen, entre otras cuestiones, cuando son objeto de una transferencia internacional (como por ejemplo, en el marco de la creación de redes de información sanitaria que facilitan proyectos de investigación llevados a cabo por entidades situadas en distintos países[8]).

---

[6] Directiva 95/46/CE del Parlamento europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (*DOCE* L, 281, de 23 de noviembre de 1995).

[7] Art. 7.3 LOPD: “Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente”. (España. *BOE*, 1999 (a)).

[8] Documento de Trabajo del Grupo de Trabajo del art. 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los Historiales Médicos Electrónico (HME), de 15 de febrero de 2007 (00323/07/ES WP 131). Este Grupo de trabajo se creó en virtud del artículo 29 de la Directiva 95/46. Se trata de un órgano consultivo independiente que interviene en materia de protección de las personas en lo que respecta al tratamiento de datos personales. Sus funciones se hallan enunciadas en el artículo 30 de dicha Directiva, así como en el artículo 15, apartado 3, de la Directiva 2002/58/CE. Está integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del Espacio Económico Europeo acuden a las reuniones del GT 29 en condición de observadores. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997. Disponible en: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm. Consulta 12 oct. 2013.

La transferencia internacional de datos (en adelante TID) es, por tanto, una cuestión que reviste gran importancia en el ámbito de la salud (por ejemplo, cuando se trata de ensayos clínicos que se desarrollan en varios países), pero que no ha sido merecedora de mucha atención doctrinal y jurisprudencial, a pesar de su innegable complejidad jurídica y relieve práctico. Centrándonos en la regulación de esta institución en el ordenamiento jurídico español, su normación se contiene, básicamente, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) (España. BOE, 1999 (a), p.43088-43099) y en su Reglamento de desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre (en adelante, RLOPD) (España. BOE, 2008, p. 4103-4136), que adaptan la legislación española a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

En dicha regulación y para el estudio de la cuestión que nos ocupa, hay que partir de la base de que en el conjunto de dicha normativa, no se establece un régimen específico dedicado a las TID en el campo de la salud, sino únicamente referencias puntuales que se verán a lo largo del desarrollo de este trabajo.

1 Elementos personales que intervienen en la TID

Hay que comenzar el estudio de esta materia precisando los términos subjetivos que pueden estar implicados en las transferencias. Para ello, señalaremos las diferentes definiciones contenidas en los diversos textos legales.

Responsable del fichero:

LIB: “El responsable del fichero atenderá las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación u oposición formuladas por los sujetos fuente, de conformidad con lo dispuesto en la normativa vigente sobre protección de datos de carácter personal” (art. 66.3).

LOPD: “Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento” (art. 3.d).

RLOPD: “Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente” (art. 5.1.q).

Elementos personales conforme a la normativa comunitaria

Dentro del ámbito propiamente dicho de las TID los dos actores que la materializan, conforme a la normativa acuñada en la nomenclatura comunitaria, son el exportador de datos y el importador:

- Exportador de datos personales: persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente reglamento, una transferencia de datos de carácter personal a un país tercero (art. 5.1.j RLOPD). En principio, es un responsable del tratamiento, pero no necesariamente, ya que en el RLOPD el exportador se desvincula del responsable lo que supone una mejora técnica (Álvarez Rigaudías, 2010, p. 1803).

- Importador de datos personales: persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un país tercero, ya sea responsable del tratamiento, encargada del tratamiento o tercero (art. 5.1. ñ RLOPD). Importador, en definitiva, es el responsable que acepta recibir del exportador datos personales para su posterior tratamiento, o el encargado del tratamiento que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de éste, conforme a las instrucciones que aquél le entrega.

También se les puede definir como: 'Transmitente' la persona física o jurídica, pública o privada, responsable del fichero o tratamiento de los datos de carácter personal que son objeto de transferencia internacional, y 'Destinatario', la persona física o jurídica, pública o privada, situada fuera del territorio español que recibe los datos transferidos.

2 Concepto y clases de transferencia internacional de datos

2.1 Concepto

TID es una forma de tratamiento[9] que supone una transmisión de los mismos fuera del territorio de la Unión Europea (en adelante, UE) y del Espacio Económico Europeo (integrado por los siguientes países: Islandia, Liechtenstein y Noruega), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español (art. 5.1.s RLOPD)[10]. Es necesario que concurra también su carácter

[9] Tratamientos de datos personales: LOPD (art. 3.c): "Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". RLOPD (art. 5.1, letra t): "Cualquier operación o procedimiento técnico sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización y cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

[10] La referencia que en la definición se realiza a la cesión y al acceso a los datos por cuenta de terceros, podría causar problemas de interpretación, pues llevaría a entender el concepto de transferencia en un sentido especialmente amplio. El Tribunal de Justicia de la UE, en una

internacional derivado de la circunstancia de que el destinatario de los datos esté establecido fuera de España y no del dato de que se dirija a un responsable o encargado[11]. Con ello se quiere destacar el hecho de que nos estamos refiriendo a salida física de los datos y no a la salida jurídica de los mismos. Es decir, que se entiende que hay transferencia internacional cuando los datos salen de la UE o del Espacio Económico Europeo (salida física) aunque continúe siendo de aplicación la legislación nacional (salida jurídica). Este sería el caso, como se acaba de referenciar, de que el destinatario de los datos en el extranjero fuera un simple encargado del tratamiento. En esta hipótesis, pese a la transferencia de los datos al extranjero, continuará siendo de aplicación la legislación española que es la que rige el tratamiento de los datos puesto que el responsable de dicho tratamiento está en España. Pero no por ello dejará de existir una transferencia internacional. No podemos identificar el carácter internacional de la transferencia con la pérdida de competencia de la ley española.

En definitiva, existirá una transferencia internacional tanto si el destinatario de los datos en el extranjero tiene la consideración de cesionario como si tiene la consideración de simple encargado del tratamiento de los mismos.

Desde un punto de vista técnico-jurídico habrá que entender como TID aquella que se da cuando exista un transporte de datos entre sistemas informáticos por cualquier medio de transmisión, difusión o cualquier otra forma de puesta a disposición de los datos siempre y cuando el país de origen y de destino sean países distintos. Es por tanto indiferente el canal de transmisión: soporte papel o digital (memoria) o medios electrónicos Intranet o por Internet.

Este enfoque es adecuado en la medida en que el fin perseguido por la regulación sobre transferencias de datos es evitar la vulneración del derecho a la protección de los mismos una vez transferidos a terceros países y el riesgo de dicha vulneración existe independientemente del medio por el cual los datos son transferidos al margen de que ciertos canales presenten riesgos más acusados, como puede ser la transferencia por Internet.

---

esclarecedora sentencia (STJUE, de 6 de noviembre de 2003, *Bodi Lindqvist*, asunto C-101/01, FJ 68), ha afirmado que la publicación de datos vía Internet, en una simple página Web, a un destinatario indefinido, no constituye una operación en tal sentido, ya que en las TID, el receptor es un sujeto determinado. (Aberasturi Gorriño, 2011, p. 335).

[11] La definición proporcionada por el RLOPD, difiere notablemente de la establecida por la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos. Sin embargo, en la actualidad no existe incompatibilidad ya que dicha norma ha sido anulada, en algunos de sus preceptos por dos sentencias (S de la Audiencia Nacional de 15 de marzo 2002 y S del Tribunal Supremo de 25 de septiembre de 2006) y tácitamente derogada por el RLOPD, en virtud de su Disposición Derogatoria Única, en todo lo que se le oponga.

2.2 Clases

De los diferentes criterios a los que se pueden someter las TID, el que toma como base el diferente ámbito geográfico en el que dichas transferencias pueden operar constituye, sin lugar a dudas, el que presenta mayores consecuencias jurídicas. Puesto que dicho criterio se va a desarrollar ampliamente en el apartado posterior, nos fijaremos ahora en otro tipo diseñado en la legislación sobre protección de datos.

Así, el art. 2.1 LOPD distingue dos tipos de TID:

- las realizadas desde un establecimiento del responsable del tratamiento situado en territorio español, es decir que el exportador de datos sea una entidad establecida en España. Son supuestos en los que un responsable establecido en España transmite los datos a un responsable establecido en el extranjero (aquel con capacidad para decidir sobre la finalidad y el uso de los datos).

- las realizadas por un responsable del tratamiento que no se encuentre establecido dentro de un territorio de la UE[12], pero utilice en el tratamiento medios situados en territorio español. En este caso, el responsable de datos personales que se recogen en España, será la entidad que utilice los medios de tratamiento en dicho país y por tanto deberá cumplir con la normativa de TID, teniendo en cuenta que en este caso existe una TID por el mero hecho de que el responsable del fichero esté situado fuera de la UE. Además, el responsable del fichero situado fuera de la UE al que se aplique la normativa de protección de datos española, de conformidad con lo establecido en el art. 5 LOPD, deberá designar un representante en España, ante el que los individuos cuyos datos se traten puedan ejercitar sus derechos de acceso, rectificación, cancelación y oposición.

3 Mecánica de actuación de las transferencia internacionales de datos

A la hora de examinar el funcionamiento de los flujos internacionales de datos es cuando se manifiesta toda la complejidad de estas operaciones, ya que es preciso distinguir diferentes situaciones en función del marco geográfico en el que la transferencia puede hacerse efectiva.

3.1 Transferencias a países de la Unión Europea y del Espacio Económico Europeo

[12] Hay que entender que la delimitación geográfica se extiende también a los países que componen el Espacio Económico Europeo.

El objetivo que se trata de evitar en las TID es que datos recogidos y tratados en un Estado sean utilizados en otro Estado sin las debidas garantías. El criterio generalmente utilizado es el de la reciprocidad: la transferencia de datos personales de un Estado a un tercer país sólo podrá efectuarse cuando éste garantice un nivel de protección adecuado; o bien, cuando preste las garantías idóneas que aseguren la protección de los datos personales.

Como hemos apuntado en el concepto de TID, en la actualidad solo se entienden por tal las que se realizan a países terceros, es decir, la comunicación de datos que se opera desde España a un país que no sea uno de los Estados miembros de la Unión Europea o del denominado Espacio Económico Europeo (Islandia, Liechtenstein y Noruega), ya que el espacio interior de dichos países se encuentra liberalizado[13]. Ello responde a que en estas hipótesis no existe para el titular de los datos riesgo alguno, ya que la Directiva 95/46/CE ha armonizado los niveles de protección de los Estados miembros, haciéndolos extensivos a los países del EEE, aunque de hecho no lo tengan[14].

De este modo, en las TID que tengan lugar desde España a los países mencionados, no se exige recabar la autorización del Director de la Agencia Española de Protección de Datos (en adelante AEPD), al igual que sucede con los países de los que nos ocupamos a continuación.

3.2 Transferencias a terceros países que no requieren autorización del Director de la Agencia Española de Protección de Datos

Muy diferente es la regulación que se establece cuando la TID tiene lugar fuera del ámbito territorial indicado. El principio general para estas hipótesis es que no se pueden realizar TID temporales ni definitivas, salvo que el país de destino proporcione un nivel de protección equiparable al que presenta el sistema español o se trate de supuestos legalmente excepcionados de la autorización del Director. En su defecto, además de haberse observado lo dispuesto en la LOPD, se ha de obtener autorización previa del Director de la AEPD, que sólo podrá otorgarla si se obtienen garantías adecuadas (art. 33.1 LOPD). No obstante, existen determinados supuestos de

[13] El RLOPD, a diferencia de lo establecido en la LOPD, incluye, además de los Estados miembros de la UE, como establece aquélla, a los países del EEE.

[14] En el proceso de adopción de la Decisión, para evaluar el nivel de protección del tercer Estado, la Comisión cuenta con la ayuda de los dictámenes que emite el Grupo del artículo 29 de la Directiva europea (art. 30.1.b), con el apoyo de un Comité (art. 31). A dicho Grupo le corresponde también comprobar la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieran afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales, informando de ello a la Comisión (art. 30.2 Directiva 95/46/CE).

transferencias que, a pesar de no efectuarse dentro del ámbito territorial indicado, no requieren de la susodicha autorización.

3.2.1 Países que presentan un nivel de protección equiparable

La determinación de cuándo un Estado ofrece un nivel de protección adecuado puede ser evaluada por la Agencia Española de Protección de Datos (AEPD), a través de una resolución administrativa, que deberá ser publicada en el Boletín Oficial del Estado (art. 67 RLOPD) o por la Comisión Europea (art. 34.k) LOPD y 68 RLOPD), sin que hasta el momento la primera Institución haya ofrecido pronunciamiento alguno al respecto. En dicha determinación habrá que tener en cuenta diferentes aspectos[15].

Distinta ha sido la actuación de la Comisión Europea que ha procedido a señalar el elenco de países (las llamadas "listas blancas") que, por el momento, sí gozan del nivel de protección exigido y que por orden cronológico de adopción de las Decisiones son: Suiza (Decisión de la Comisión 2000/518/ CE, de 26 de julio de 2000), las entidades que en EE.UU respetan los denominados Principios de Puerto Seguro (compromisos Safe Harbor)[16], Canadá[17], Argentina (Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003), Guernsey (Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003), la Isla de Man (Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004), Jersey (Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008), Islas Feroe (Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010), Andorra (Decisión 2010/625/UE, de la Comisión, de 19 de octubre de 2010), Israel (Decisión 2011/61/UE, de la Comisión, de 31 de enero de 2011) y República Oriental del Uruguay (Decisión 2012/484/UE, de la Comisión, de 21 de agosto de 2012). En última instancia, cabe citar Nueva Zelanda como país que, a pesar de no contar

[15] Concretamente: 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, 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 (arts. 33.2 LOPD y 67.1 RLOPD).

[16] Dichos principios constituyen, básicamente, criterios que garantizan que las entidades que los asumen mantienen un nivel adecuado de protección de los datos de carácter personal y se recogen en la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000 (DOUE L-215, de 25 de agosto de 2000). La relación de las entidades "Harborites" disponible se encuentra en la Web del Departamento de Comercio de EE.UU: https://www.export.gov/safehrbr/list.aspx. (Barceló y Pérez Asinari, 2009, p. 141-166).

[17] Con respecto a este país, se establecen matices sobre la posibilidad de transmitir datos a importadores que se encuentren allí, dependiendo de si se trata de sujetos sometidos a la *Personal Informatio and Electronic Documents Act* o no (Decisión 2002/02/CE, de 20 de diciembre de 2001; *DO* L-02, de 4 de enero de 2002).

expresamente con la valoración positiva de la Comisión, sí ha obtenido aprobación del grupo de Trabajo del artículo 29 de la Directiva[18].

Cuando son los propios Estados miembros los que determinan bajo qué condiciones un país ostenta un nivel adecuado de protección de datos, ante la diferente valoración que puedan establecer respecto de un mismo país, la Directiva recoge un sistema de información a la Comisión: por un lado, se impone a todos los Estados miembros que informen a la Comisión y a los demás Estados sobre la consideración del régimen de protección de un país como adecuado con el fin de que, ante la eventualidad de posibles divergencias, se puedan adoptar las medidas oportunas (art. 26.3 Directiva 95/46/CE). Además, se establece un sistema por el que la Comisión pueda comprobar la situación del citado derecho en un país determinado y obrar en consecuencia para que los Estados miembros eviten, en su caso, transferencias a dicho país (art. 25.3.4.5.6 Directiva 95/46/CE).

3.2.2 Excepciones legalmente establecidas

El art. 34 LOPD y 66.2 RLOPD, así como el art. 26 de la Directiva 95/46/CE, contemplan la posibilidad de realizar TID a terceros países, sin necesidad de recabar la autorización previa del Director AEPD y con independencia de cuál sea el nivel que a la protección de datos de carácter personal se otorgue cuando:

- la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España;

- la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional;

- 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;

- se refiera a transferencias dinerarias conforme a su legislación específica;

- el afectado haya dado su consentimiento inequívoco a la transferencia prevista;

- 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;

[18] Dictamen 6/2010 Grupo de Trabajo del artículo 29, de 12 de octubre de 2010; Dictamen 11/2011 Grupo de Trabajo del artículo 29, de 4 de abril de 2011.

- 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;

- 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;

- la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

- la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

Estas excepciones son tan amplias que podrían llegar a desvirtuar la regla general. El apartado tercero contempla directamente las que tienen su ámbito de actuación dentro del sector sanitario como una de las hipótesis que quedan fuera del régimen general del protocolo de actuación de las TID. En cuanto a la precisión del ámbito concreto al que se extiende la mencionada excepción al representar una desviación que afecta a datos que gozan de una especial protección, *ex* art. 7.3 LOPD, parece que lo deseable es que sea objeto de una interpretación restrictiva y que sea aplicada únicamente cuando las otras modalidades de hacer TID no se puedan emplear (Aberasturi Gorriño, 2011, p. 354).

También merece la pena destacar, de los supuestos del elenco que acabamos de referenciar, el del consentimiento del afectado, por presentar un interés general. En efecto, el consentimiento se ha articulado como la pieza clave de la normativa de protección de datos española[19]. Generalmente, para obtener un consentimiento válido, es necesario que se informe a los afectados de los extremos establecidos en el art. 5 LOPD, indicando la entidad que actuará como importador de los datos, los países a los que se transfieran dichos datos y las finalidades de la transferencia. La manifestación de voluntad del interesado ha de ser, según el art. 6 LOPD, inequívoca (que no deje lugar a dudas), específica (que se produzca con carácter concreto), de forma libre (sin ningún tipo de coacción o cortapisas) e informada (que, en cierto modo se subsume en la característica anterior, aunque le añade la necesidad del deber de información, recogida en el art. precedente) (Fernández López, 2010, p. 457). Además, dicho consentimiento al recaer sobre uno de los denominados “datos sensibles”, es decir, datos especialmente protegidos, habrá de ser expreso y por escrito, en todo caso. De

[19] En este sentido, la Sentencia del Tribunal Constitucional 292/2000 ha definido el derecho a la protección de los datos personales como un auténtico derecho fundamental. De ahí que el principio del consentimiento se haya erigido en la columna vertebral para el tratamiento de datos.

cualquier modo, es importante enfatizar que un adecuado consentimiento informado por parte del sujeto logrará, sin ningún género de dudas, simplificar el arduo proceso de la TID.

3.3 Transferencias a terceros países que requieren autorización del Director de la Agencia Española de Protección de Datos

Fuera de los supuestos que se han contemplado en los apartados anteriores, el resto de TID requieren la autorización previa del Director de la AEPD, cuyo procedimiento se encuentra normado en los arts. 137-140 RLOPD, teniendo en cuenta que la facultad de otorgar la autorización no constituye una potestad completamente discrecional, ya que sólo se puede denegar en los casos establecidos en el art. 70.3 RLOPD[20]. En caso contrario, sólo podrá otorgarla si se obtienen garantías adecuadas (art. 33 LOPD, art. 66.1 RLOPD), aportando el exportador un contrato escrito celebrado con el importador en el que consten las 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 (art. 70.2 RLOPD).

A tal efecto, se articulan dos mecanismos que implican la existencia de dichas garantías para conseguir la preceptiva autorización: las Cláusulas Contractuales Tipo y las Normas Corporativas Vinculantes (Binding Corporate Rules - BCR). Ambos constituyen instrumentos privados que suplen la labor de regulación general del legislador (Sancho Villa, 2008, p. 443).

3.3.1 Cláusulas contractuales tipo

[20] "En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:
Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.
Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.
La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.
Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible".

Dichas cláusulas se erigen en un mecanismo especialmente apto para facilitar el acuerdo de garantía entre importador y exportador al que acabamos de referirnos y constituyen el instrumente más utilizado por las empresas que solicitan autorizaciones de TID. Su regulación se contiene en los arts. 33.1 LOPD y 70.2 RLOPD que las conciben como métodos para homologar el sistema de protección de datos en los países que no cuentan con un nivel de protección adecuado.

En efecto, el artículo últimamente citado, determina que el responsable del fichero o tratamiento puede aportar un contrato escrito celebrado entre el exportador y el importador. Dicho contrato ha de contener los datos que son objeto de la transferencia y se establecerán respecto a los mismos las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantizará el ejercicio de sus respectivos derechos.

Las partes pueden fijar libremente el contenido del contrato en el extremo relativo al ofrecimiento de las garantías necesarias. No obstante, la necesidad de que la AEPD determine si quedan o no suficientemente cubiertas dichas garantías, se puede obviar si las partes utilizan cláusulas contractuales modelo aprobadas por la Comisión europea (art. 70.2 RLOPD).

Existen dos tipos de cláusulas: de responsable a responsable (Decisión 2001/497/CE, de 15 de junio de 2001, modificada por la Decisión 2004/915/CE, de 27 de diciembre de 2004). Estos tipos de cláusulas, conocidos como Modelo I y Modelo II, respectivamente, se pueden utilizar, por tanto, para las transferencias entre responsables del tratamiento, el exportador establecido en España y el importador establecido en un Estado que no proporcione un nivel adecuado de protección. A ellas hay que añadir, a partir del 15 de mayo de 2010, las cláusulas de responsable a encargado establecido en países que no tengan el adecuado nivel de protección (Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, que incorpora la figura del subencargado).

Las TID basadas en tales cláusulas requieren la tramitación de un expediente de autorización del Director AEPD.

3.3.2 Normas corporativas vinculantes (*binding corporate rules* - BCR)

Dentro del apartado dedicado a las TID a países sin nivel de protección adecuado, el RLOPD, establece una regulación embrionaria de las transferencias realizadas en el seno de grupos multinacionales de empresas. Esta posibilidad se ha desarrollado en tiempos recientes cuando las empresas han empezado a establecer normas de carácter interno, de obligado cumplimiento para todas las empresas del grupo, que regulan determinados aspectos relacionados, generalmente, con la

seguridad de la información, código de conducta de empleados, etc. En palabras de Rubí Navarrete (2012), constituyen una "nueva herramienta que permite definir el marco de actuación aplicable a las TID intragrupo". Precisamente, su ámbito de actuación, determinará que en muchas ocasiones no puedan aplicarse a las transferencias de muestras biológicas, ya que están pensadas sólo para grupos de empresas.

El art. 70. 4 y el último apartado del art. 137 RLOPD determinan el régimen jurídico aplicable a dicho tipo de transferencias. El complemento a dicha regulación se encuentra en diferentes documentos elaborados por el Grupo del art. 29 de la Directiva 95/46/CE, atinentes al contenido de las normas corporativas vinculantes y al procedimiento previo, que se desarrolla entre los diversos Estados miembros implicados en su aprobación:

WP 155 - Preguntas más frecuentes sobre BCR.

WP 154 - Cuadro que establece la estructura de las BCR.

WP 153 - Cuadro que establece la relación de los elementos y principios que deben contener las BCR.

WP 108 - Modelo de solicitud de autorización de transferencia internacional basada en BCR en el ámbito del procedimiento coordinado.

WP 107 - Documento sobre la competencia de las Autoridades de Control europeas en el procedimiento coordinado de aprobación de las BCR.

WP- 74 - Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las BCR.

4 Actuaciones comunes que se deben llevar a cabo ante la Administración

En todos los caso de TID resulta esencial el cumplimiento de todas las garantías que las diferentes normas exigen que se efectúen rigurosamente. La entidad encargada de realizar dicha fiscalización es la AEPD que lo llevará a cabo en el momento de prestar la autorización, cuando sea preceptiva o, siempre, cuando la transferencia se inscriba en el Registro correspondiente (art. 36.2.b LOPD), previa la correspondiente notificación (art. 26.1 LOPD y 66 RLOPD). La obligación de notificación se impone por la Ley, en todo caso, tanto si se trata de ficheros públicos (art. 20.2 LOPD), como privados (art. 26.2 LOPD) y entre los extremos objeto de notificación (identidad del responsable del fichero, finalidad, tipo de datos, medidas de seguridad, cesiones previstas) destaca, particularmente, la precisión de las transferencias internacionales que se prevean realizar (art. 26.2 LOPD). La notificación se articulará siguiendo el procedimiento ordinario establecido en el Reglamento, sin que para estos casos se exijan requisitos específicos (arts. 130 y ss. RLOPD). Es

interesante destacar que si la necesidad o intención de transferir los datos surge con posterioridad a la creación del fichero el responsable debe solicitar una modificación del contenido del asiento en el Registro, para que conste la transferencia proyectada (art. 130 RLOPD).

5 Régimen de infracciones y sanciones

Como se ha puesto de manifiesto, en muchísimas ocasiones, y sin ser conscientes de ello por parte de la mayoría de los sujetos que intervienen en las TID, dicha operación supone y conlleva numerosas consecuencias legales, siendo seguramente las más relevantes las relativas a las elevadísimas sanciones que pueden originar (multas de 600 a 600.000 euros).

Sin embargo, dicho régimen ha sufrido últimamente una notable modificación en virtud de la disposición final quincuagésima sexta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible (España. BOE, 2011, p. 25033-25235). La reforma en cuestión afecta a los arts. 43 a 46 y 49 de la LOPD que se enmarcan en el Título VII, referido a las infracciones y sanciones.

La mencionada reforma ha sido acogida muy favorablemente ya que “permite suavizar sustancialmente el régimen sancionador hasta ahora previsto en la LOPD”, constituyendo “una vieja pretensión de algunos sectores, que veían en dicho régimen un elemento enormemente perturbador para los responsables de ficheros y tratamientos” (Piñar Mañas y Canales Gil, 2011, pp. 17-18), aunque continúa siendo un sistema considerablemente exigente (Ferré Tous, 2011, p. 84). Entre otras novedades que incorpora la presente legislación, cabe destacar la modificación de la tipificación de las infracciones que se reducen considerablemente: la comunicación o cesión de datos sin legitimación pasa a ser infracción grave (en lugar de muy grave), salvo que afecte a los datos especialmente protegidos (art. 7.2.3.5 LOPD) y la cesión de datos a un encargado sin cumplir las previsiones formales previstas en el art. 12 de la LOPD se considera infracción leve. Dentro del catálogo de infracciones graves figuran: no inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos cuando haya sido requerido para ello por el Director de la Agencia; tratar datos personales sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en la Ley y sus disposiciones de desarrollo; el impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

El otro gran bloque donde se ubican las modificaciones más importantes es en el art. 45 que recoge el régimen de graduación y fijación de la cuantía de la sanción. De este modo, se sube el suelo y se baja el techo de las infracciones leves, de tal

forma que si antes la mínima penalización de una infracción leve era de 600 euros, ahora es de 900, y si antes el tope eran 60.000 euros, ahora son 40.000. Este techo de 40.000 para las leves sitúa el suelo de las infracciones graves en 40.001 euros, manteniendo el máximo en 300.000 euros. Las muy graves siguen siendo sancionadas con multas de 300.001 a 600.000 euros. Dentro de este mismo artículo se introducen nuevos criterios a la hora de graduar la cuantía de las sanciones[21] y para su atenuación[22].

Finalmente, se crea un nuevo apartado (art. 45.6) que introduce la medida del apercibimiento. Se trata de una medida excepcional y limitada (sólo procede cuando concurran de forma significativa los criterios de atenuación) que permite avisar de la irregularidad y requerir la adopción de las medidas que sean oportunas. Se reserva para los casos en que los hechos sean constitutivos de infracciones leves o graves, y cuando el infractor no hubiese sido sancionado o apercibido con anterioridad. Si el apercibimiento no se cumple en el plazo establecido, provocará la apertura de un procedimiento sancionador por dicho incumplimiento.

En cuanto al régimen de infracciones y sanciones establecido para las infracciones que se cometan en ficheros de titularidad pública se contempla en los arts. 46 y 48 LOPD (art. 43.2). El artículo 46, que también se ha visto reformado por la Ley de Economía Sostenible, ha quedado configurado de la siguiente manera:

1. “Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo

[21] Art. 45.4: “La cuantía de las sanciones se graduará atendiendo a los siguientes criterios: El carácter continuado de la infracción. El volumen de los tratamientos efectuados. La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal. El volumen de negocio o actividad del infractor. Los beneficios obtenidos como consecuencia de la comisión de la infracción. El grado de intencionalidad. La reincidencia por comisión de infracciones de la misma naturaleza. La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas. La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor. Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora”.

[22] Art. 45.5: “El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos: Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo. Cuando la entidad infractora haya regularizado la situación irregular de forma diligente. Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción. Cuando el infractor haya reconocido espontáneamente su culpabilidad. Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente”.

serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

Los autores no han dejado de subrayar que este sistema de infracción sin sanción constituye una de las previsiones más llamativas de la LOPD que introduce una evidente discriminación entre ficheros de titularidad privada y pública a efectos de establecer las consecuencias represoras que de la comisión de las infracciones tipificadas en la Ley se pueden derivar (Fernández Salmerón y Valero Torrijos, 2010, páginas 2188-2194).

6 La suspensión de las transferencias internacionales de datos

En el marco punitivo es muy importante, además, tener en cuenta la facultad que el art. 37.1.f LOPD concede al Director de la AEPD para ordenar la cesación de los tratamientos y la cancelación de los ficheros cuando no se ajusten a las disposiciones legales. Desarrollando la disposición legal, el RLOPD hace referencia expresa a la posibilidad de acordar, previa audiencia del exportador, la suspensión temporal de la transferencia, si bien sólo está prevista en los supuestos de transferencias a países con nivel adecuado de protección si se dan una serie de circunstancias, fundamentalmente, cuando se haya constatado o haya indicios racionales de que el importador concreto que recibirá la información ha vulnerado los principios de protección de datos (art. 69 RLOPD), o cuando las transferencias obtienen autorización al amparo de un contrato suscrito entre importador y exportador, supuesto en el que la facultad de suspensión cuenta con un mayor campo de actuación, como se comprueba al examinar las circunstancias que han de concurrir para que se pueda acordar (art. 70.3 RLOPD).

La referida suspensión se tramita, en ambos casos, ateniéndose al procedimiento establecido en los arts. 141-144 RLOPD.

7 Perspectivas de futuro

Sin duda alguna, la Directiva europea sobre protección de datos está pidiendo a gritos una actualización que pueda hacer eficaz la alta protección que se pretende lograr[23]. La Comisión Europea ha detectado esta situación y ha propuesto, con fecha de 25 de enero de 2012[24], una gran reforma general del marco jurídico europeo de las normas de protección de datos personales que logre armonizar las divergencias que en los diferentes Estados miembros de la Unión Europea se han suscitado en cuanto a su ejecución y cumplimiento[25]. Como se ha puesto de manifiesto, la rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales. Se ha incrementado enormemente la magnitud del intercambio y la recogida de datos. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social y requiere que se facilite aún más la libre circulación de datos dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales[26]. En concreto, con respecto a la TID se considera que la complejidad de las normas en materia de transferencias internacionales de datos personales constituye un impedimento sustancial a su funcionamiento, ya que se necesita transferir con regularidad datos personales de la UE a otras partes del mundo.

---

[23] "Ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas (Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Bruselas, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), Considerando 6. (DAVARA RODRÍGUEZ, 2011).

[24] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las regiones COM (2012) 9 final. Para mayor información se puede consultar: http://ec.europa.eu/justice/data-protection/index_es.htm.

[25] La Comisión del PE de Libertades Civiles, Justicia y Asuntos de Interior tiene prevista la votación de los informes sobre el Reglamento de Protección de Datos (ponente: Jan Philipp Albrecht (Verdes / ALE, DE)) y de la Directiva (Ponente: Dimitrios Droutsas (S & D, GR)) para lunes, 21 de octubre 2013 a las 6.30 horas, en Estrasburgo. El comité adoptará un mandato para las negociaciones con el Consejo con el fin de tratar de llegar a un acuerdo sobre el paquete de protección de datos antes de las elecciones europeas de mayo de 2014.

[26] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Bruselas, 25.1.2012 COM (2012) 11 final 2012/0011 (COD), Considerando 5.

A diferencia de lo que sucede en la regulación actual que, como dijimos, no presenta ninguna disposición específica para el tratamiento de datos relativos a la salud, la Propuesta de Reforma de la que nos venimos ocupando explica: "el tratamiento de datos personales relativos a la salud, como categoría especial de datos que merece mayor protección, puede justificarse a menudo por motivos legítimos en beneficio de los ciudadanos y la sociedad en su conjunto, en particular cuando se trate de garantizar la continuidad de la asistencia sanitaria transfronteriza. Por tanto, el presente Reglamento debe establecer unas condiciones armonizadas para el tratamiento de los datos personales relativos a la salud, sujetas a garantías específicas y adecuadas a fin de proteger los derechos fundamentales y los datos personales de las personas físicas. Ello incluye el derecho de las personas físicas a acceder a sus datos personales relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información de este tipo como los diagnósticos, los resultados de exámenes, las evaluaciones de los facultativos y cualesquiera tratamientos o intervenciones practicadas" (Considerando 122)[27].

---

[27] Artículo 81: "Tratamiento de datos personales relativos a la salud
1. Dentro de los límites establecidos en el presente Reglamento y de conformidad con el artículo 9, apartado 2, letra h), el tratamiento de datos personales relativos a la salud deberá realizarse sobre la base del Derecho de la Unión o de los Estados miembros, que deberá establecer las disposiciones específicas adecuadas para salvaguardar los legítimos intereses del interesado, y deberá ser necesario:
a) a los fines de la medicina preventiva o la medicina del trabajo, el diagnóstico médico, la prestación de asistencia sanitaria o el tratamiento o la gestión de los servicios de asistencia sanitaria, siempre que tales datos sean tratados por un profesional sanitario sujeto a la obligación del secreto profesional o por otra persona también sujeta a una obligación de confidencialidad equivalente en virtud de la legislación del Estado miembro o de las normas establecidas por los organismos nacionales competentes; o
b) por razones de interés público en el ámbito de la salud pública, como la protección contra riesgos sanitarios transfronterizos graves, o para garantizar altos niveles de calidad y seguridad de los medicamentos o del material sanitario; o
c) por otras razones de interés público en ámbitos como la protección social, especialmente a fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad.
2. El tratamiento de datos personales relativos a la salud que sea necesario para los fines de la investigación histórica, estadística o científica, como el establecimiento de registros de pacientes con el fin de mejorar el diagnóstico, distinguir entre tipos de enfermedades similares y preparar estudios para terapias, estará supeditado al cumplimiento de las condiciones y garantías contempladas en el artículo 83.
3. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 87, a fin de especificar otras razones de interés público en el ámbito de la salud pública a que se refiere el apartado 1, letra b), así como los criterios y requisitos de las garantías del tratamiento de datos personales a los fines a que se hace referencia en el apartado 1".
Artículo 83: "Tratamiento para fines de investigación histórica, estadística o científica
1. Dentro de los límites del presente Reglamento, podrán tratarse los datos personales para fines de investigación histórica, estadística o científica sólo si:
a) dichos fines no pueden lograrse de otra forma mediante un tratamiento de datos que no permita o que ya no permita la identificación del interesado;

El Capítulo V está dedicado en exclusiva a las Transferencias Internacionales de Datos. Es ncesario comenzar denunciando que no se contiene ninguna definición de "transferencia de datos"[28]. Ante tal laguna la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo propone la siguiente: «transferencia»: "toda comunicación de datos personales, puestos de manera activa a disposición de un número limitado de partes identificadas, con el conocimiento o la intención del remitente de dar acceso al destinatario a los datos personales"[29].

Dicho capítulo presenta el siguiente contenido:

El artículo 40 establece, como principio general, que la observancia de las obligaciones que figuran en dicho capítulo es de obligado cumplimiento para toda transferencia de datos de carácter personal a terceros países u organizaciones internacionales, incluidas las transferencias ulteriores.

El artículo 41 fija los criterios, condiciones y procedimientos para la adopción de una decisión relativa a la adecuación del nivel de protección de datos por parte de la Comisión, basada en el artículo 25 de la Directiva 95/46/CE. Entre los criterios que deberán tenerse en cuenta para que la Comisión evalúe si existe o no un nivel adecuado de protección se incluyen expresamente el Estado de Derecho, el recurso jurisdiccional y la supervisión independiente. El artículo confirma ahora explícitamente la posibilidad de que la Comisión evalúe el nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país. Esta hipótesis constituye la regla general.

---

b) los datos que permitan la atribución de información a un interesado identificado o identificable se conservan por separado del resto de la información, en la medida en que dichos fines puedan lograrse de este modo.
2. Los organismos que llevan a cabo investigaciones históricas, estadísticas o científicas podrán publicar o hacer públicos por otra vía datos personales sólo si:
a) el interesado ha dado su consentimiento en las condiciones establecidas en el artículo 7;
b) la publicación de los datos personales es necesaria para presentar los resultados de una investigación o para facilitar una investigación, siempre que los intereses o los derechos o libertades fundamentales del interesado no prevalezcan sobre tales objetivos; o
c) el interesado ha hecho públicos los datos.
3. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 86, a fin de especificar los criterios y requisitos del tratamiento de los datos personales a los efectos mencionados en los apartados 1 y 2, así como las limitaciones necesarias a los derechos de información y de acceso por parte del interesado, y de detallar las condiciones y garantías de los derechos del interesado en tales circunstancias".

[28] Tal y como ha sido puesto de manifiesto en el Dictamen del Comité Económico y Social Europeo sobre la Propuesta de Reglamento. El Dictamen se puede consultar en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:229:0090:0097:ES:PDF .

[29] Enmienda 86 Propuesta de Reglamento Artículo 4 – punto 3 bis (nuevo). Justificación Es necesaria la definición de «transferencia» para distinguirla de la puesta a disposición (pública) de los datos. El texto se puede consultar en: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387es.pdf .

Por ello, para las transferencias a terceros países en relación con las cuales la Comisión no haya adoptado ninguna decisión de adecuación, el artículo 42 requiere que se aporten las garantías apropiadas, especialmente cláusulas tipo de protección de datos, normas corporativas vinculantes y cláusulas contractuales. La posibilidad de hacer uso de cláusulas tipo de protección de datos de la Comisión se basa en el artículo 26, apartado 4, de la Directiva 95/46/CE. Como novedad, estas cláusulas tipo de protección de datos también pueden ser adoptadas ahora por una autoridad de control y ser declaradas generalmente válidas por la Comisión. Las normas corporativas vinculantes se mencionan ahora específicamente en el texto jurídico. La opción de las cláusulas contractuales ofrece cierta flexibilidad al responsable o al encargado del tratamiento, aunque está sujeta a la autorización previa por parte de las autoridades de control.

El artículo 43 describe con mayor detalle las condiciones aplicables a las transferencias realizadas en el marco de normas corporativas vinculantes, sobre la base de las prácticas y requisitos actuales de las autoridades de control.

El artículo 44 define y aclara, detalladamente, las excepciones a una transferencia de datos sobre la base de las disposiciones en vigor del artículo 26 de la Directiva 95/46/CE. Ello se aplica en particular a las transferencias de datos requeridas y necesarias para la protección de intereses públicos importantes, por ejemplo en caso de transferencias internacionales de datos entre autoridades de competencia, administraciones fiscales o aduaneras, o entre servicios competentes en materia de seguridad social o de gestión de la pesca. Por otra parte, en determinadas circunstancias una transferencia de datos puede estar justificada por un interés legítimo del responsable o del encargado del tratamiento, aunque únicamente después de haber evaluado y documentado las circunstancias de dicha operación de transferencia[30].

[30] Artículo 44. “Excepciones
1. En ausencia de una decisión de adecuación de conformidad con lo dispuesto en el artículo 41 o de garantías apropiadas de conformidad con lo dispuesto en el artículo 42, solo podrá procederse a una transferencia o una serie de transferencias de datos personales a un tercer país o una organización internacional cuando:
a) el interesado haya dado su consentimiento a la transferencia propuesta, tras haber sido informado de los riesgos que entraña debido a la ausencia de una decisión de adecuación y de garantías apropiadas; o
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la implementación de medidas precontractuales adoptadas a solicitud del interesado; o
c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; o
d) la transferencia sea necesaria por motivos importantes de interés público; o

Cierra el Capítulo el artículo 45 que establece explícitamente mecanismos de cooperación internacional para la protección de los datos de carácter personal entre la Comisión y las autoridades de control de terceros países, especialmente aquellas que se considera que ofrecen un nivel de protección adecuado, teniendo en cuenta la Recomendación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la cooperación transfronteriza en la ejecución de leyes que protegen la privacidad, de 12 de junio de 2007[31].

Referencias

---

e) la transferencia sea necesaria para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial; o
f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o
g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de un Estado miembro, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de un Estado miembro para la consulta; o
h) la transferencia sea necesaria para la satisfacción de los intereses legítimos del responsable o del encargado del tratamiento, que no puedan ser calificados de frecuentes ni de masivos, y el responsable o el encargado hayan evaluado todas las circunstancias que rodean la operación o la serie de operaciones de transferencia de datos y hayan ofrecido en su caso, sobre la base de dicha evaluación, garantías apropiadas con respecto a la protección de datos personales.
2. Una transferencia efectuada de conformidad con el apartado 1, letra g), no implicará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Cuando la finalidad del registro sea la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o cuando ellas sean las destinatarias.
3. Cuando el tratamiento se efectúe de conformidad con el apartado 1, letra h), el responsable o el encargado del tratamiento prestarán especial atención a la naturaleza de los datos, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecerán, en su caso, garantías apropiadas con respecto a la protección de datos personales.
4. Las letras b), c) y h) del apartado 1 no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.
5. El interés público contemplado en el apartado 1, letra d), deberá ser reconocido por el Derecho de la Unión o del Estado miembro a que esté sujeto el responsable del tratamiento.
6. El responsable o el encargado del tratamiento documentarán, en la documentación contemplada en el artículo 28, la evaluación y las garantías apropiadas ofrecidas contempladas en el apartado 1, letra h), e informarán de la transferencia a la autoridad de control.
7. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar los «motivos importantes de interés público» a tenor de lo dispuesto en el apartado 1, letra d), así como los criterios y requisitos aplicables a las garantías apropiadas contempladas en el apartado 1, letra h)".

[31] El último *iter* en este proceso lo constituye la adopción por parte de la Comisión del PE de Libertades Civiles, Justicia y Asuntos de Interior de la votación de los informes sobre el Reglamento de Protección de Datos (ponente: Jan Philipp Albrecht (Verdes / ALE, DE)) y de la Directiva (Ponente: Dimitrios Droutsas (S & D, GR)) que tuvo lugar el 21 de octubre 2013 en Estrasburgo. El comité adoptará un mandato para las negociaciones con el Consejo con el fin de tratar de llegar a un acuerdo sobre el paquete de protección de datos antes de las elecciones europeas de mayo de 2014, fecha límite para su aprobación.

ABERASTURI GORRIÑO, Unai. Movimiento internacional de Datos. Especial referencia a la transferencia internacional de datos sanitarios. *Revista de Administración Pública* (Madrid), (186): 329-369, 2011. ISSN 0034-7639.

ÁLVAREZ RIGAUDÍAS, Cecilia. Comentario a los artículos 34 y 35. Las Transferencias Internacionales de Datos. En: TRONCOSO REIGADA, Antonio (Director). *Comentario a la Ley Orgánica de Protección de Datos*. Cizur Menor (España): Civitas-Thomson, 2010, 2292 p. ISBN: 978-84-470-3423-9.

BARCELÓ, Rosa; PÉREZ ASINARI, María Verónica. Transferencia internacional de datos personales. En MARTÍNEZ MARTÍNEZ, Ricard, *protección de datos*. *Comentarios al Reglamento de Desarrollo de la LOPD*, Valencia: Tirant lo Blanch, 2009, 293 p. ISBN 978-84-9876- 356-0.

DAVARA RODRÍGUEZ, Miguel Ángel. Modificaciones en la Directiva Europea sobre Protección de Datos. *El Consultor de los Ayuntamientos y de los Juzgados,* La Ley-Actualidad, (13): 1669-1676, 2011. ISSN 0210-2161.

ESPAÑA. *Boletín Oficial del Estado* (BOE)*;* núm. 55, de 5 de marzo de 2011, páginas 25033-25235.

ESPAÑA. *Boletín Oficial del Estado* (BOE); núm. 286, de 27 de noviembre de 2009.

ESPAÑA. *Boletín Oficial del Estado* (BOE); núm. 17, de 19 de enero de 2008, páginas 4103-4136.

ESPAÑA. *Boletín Oficial del Estado* (BOE): núm. 159, de 4 de julio de 2007, páginas 28826-28848.

ESPAÑA. *Boletín Oficial del Estado* (BOE); núm. 298, de 14 de diciembre de 1999, páginas 43088-43099. (a)

ESPAÑA. *Boletín Oficial del Estado* (BOE); núm. 251, de 20 de octubre de 1999, páginas 36825- 36830. (b)

ESPAÑA. *Boletín Oficial del Estado* (BOE); núm. 274, de 15 de noviembre de 1985, páginas 36000-36004.

ESPAÑA. *Boletín Oficial del Estado* (BOE); núm. 311, de 29 de diciembre de 1978, páginas 29313-29424.

FERNÁNDEZ LÓPEZ, Juan Manuel. Comentario al artículo 6. Principio de consentimiento. En TRONCOSO REIGADA, Antonio (Director). *Comentario a la Ley Orgánica de Protección de Datos*. Cizur Menor (España): Civitas-Thomson, 2010, 2292 p. ISBN: 978-84-470-3423-9.

FERNÁNDEZ SALMERÓN, Manuel; VALERO TORRIJOS, Julián. Comentario al artículo 46. Las infracciones de las Administraciones Públicas. En TRONCOSO REIGADA, Antonio (Director). *Comentario a la Ley Orgánica de Protección de Datos*. Cizur Menor (España): Civitas-Thomson, 2010, 2292 p. ISBN: 978-84-470-3423-9.

FERRÉ TOUS, Santiago. Date breach notification, procedimiento sancionador y derecho a no confesarse culpable. *Revista Aranzadi de Derecho y Nuevas tecnologías*, Aranzadi (26): 69-85, 2011. ISSN 1696-0351.

PIÑAR MAÑAS, José Luis; CANALES GIL, Álvaro. *Legislación de Protección de Datos*. (2. ed.) Madrid: Lustel, 2011, 409 p. ISBN 978-84-9890-148-1.

RODOTÀ, Stefano. Democracia y protección de datos. *Cuadernos de Derecho Público*, INAP (19-20): 17-26, 2003. ISSN 1138-2848.

RUBÍ NAVARRETE, Jesús. Protección de Datos y gestión de fichero, Conferencia pronunciada dentro de las Jornadas sobre el *Impacto del nuevo Real Decreto de Biobancos. Cuestiones prácticas*. En: Auditorio del Instituto de Salud Carlos III (2012, febrero, Madrid). Disponible en www.institutoroche.es/Jornadas.

SANCHO VILLA, Diana. Protección de datos personales y transferencia internacional: cuestiones de ley aplicable. *Revista Jurídica de Castilla y León*, Junta de Castilla y León, (16): 401-445, 2008. ISSN 1696-6759.

Recebido para publicação em 18 de dezembro de 2012
Versão final em 7 de novembro de 2013