REVISTA IBEROAMERICANA DE DERECHO INFORMÁTICO (SEGUNDA ÉPOCA).
FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.
ISSN 2530-4496 – AÑO 1, N° 1, 2016, PÁGS. 55-70

Transferencia internacional de datos personales desde España a países iberoamericanos.

International transfer of personal data from Spain to Ibero-american countries

MARTA GRANDE SANZ

RESUMEN

Las transferencias internacionales de datos personales deben cumplir ciertas garantías para evitar la infracción de los principios que rigen el derecho fundamental a la protección de datos personales.

Según la Directiva de Protección de Datos, la Comisión Europea resulta competente para decidir si un Estado cuenta con un adecuado nivel de protección de acuerdo con los estándares europeos y si, por tanto, resulta un destino seguro para los datos personales de los Estados miembros de la Unión Europea; entre ellos, España. Este reconocimiento permite realizar intercambios de datos personales con el país en cuestión sin necesidad de autorización (Argentina y Uruguay). Sin embargo, cuando la autorización del Director de la Agencia Española de Protección de Datos sea necesaria, el exportador debe aportar garantías suficientes mediante cláusulas contractuales tipo incluidas en el contrato que celebren el exportador y el importador de los datos o a través de reglas corporativas vinculantes.

En consecuencia, los países iberoamericanos deben emplear estos instrumentos si quieren favorecer los intercambios comerciales con España y el desarrollo de los servicios de la Sociedad de la Información e incrementar su atractivo como países destinatarios de transferencias de datos personales.

ABSTRACT

International transfers of personal data must be subject to some guarantees to prevent the infringement of the principles that govern the fundamental right to data protection.

The Data Protection Directive grants the European Commission competencies to decide that a country has established a legal frame for the protection of data in accordance with European standards and a secure destination for personal data originated in EU member countries and, therefore, in Spain. This recognition is equivalent to the full liberalization of the exchange of personal data between Spain and the country in question without authorisation (Argentina and Uruguay). Nevertheless, when the authorisation of the Director of the Spanish Agency of Data Protection was necessary, the exporter must be furnished sufficient guarantees based on standard contractual clauses in written contract concluded between the exporter and the data importer or Binding Corporate Rules.

Consequently, Ibero-American Countries should use such instruments in order to favour commercial exchanges and the development of the services available in the Information Society and increase their attractiveness as recipient countries of international transfers of personal data.

PALABRAS CLAVE

Dato personal, protección de datos personales, transferencia internacional de datos personales, nivel adecuado de protección, modelos de regulación de la protección de datos personales.

KEYWORDS

Personal data, data protection, international personal data transfer, adequate level of personal information protection, personal information protection regulation models.

I. INTRODUCCIÓN

El avance de las nuevas tecnologías y la sociedad de la información han provocado un desarrollo sin precedentes del tratamiento y del intercambio de datos personales lo que plantea, a su vez, nuevos retos en el ámbito de la protección de datos personales y, en particular, respecto a la transferencia in-

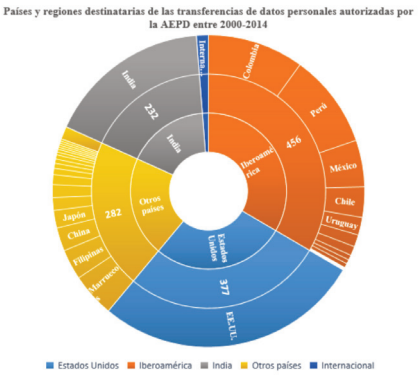
ternacional de datos personales a terceros países.

En los últimos quince años algunos países iberoamericanos tales como Argentina, Chile, Colombia, Costa Rica, México, Nicaragua, Perú y Uruguay han aprobado legislaciones nacionales sobre protección de datos personales[85]. En la mayoría de los casos, el derecho de las personas sobre la protección de sus datos se regula a través del denominado *habeas data*[86] y, por tanto, como garantía constitucional que impone ciertas obligaciones a las entidades que tratan la información y, en particular, las siguientes: la utilización de los datos para los fines para los que fueron recabados o la necesidad de garantizar su seguridad y controlar el acceso a los mismos por personas no autorizadas. En consecuencia, los ciudadanos tienen derecho a conocer la legalidad en la recopilación de sus datos y cuando se recaben ilegalmente podrán solicitar la correspondiente sanción a los responsables.

Cada vez son más los países que cuentan con normas específicas en materia de protección de datos y con medios legales y organizativos para proteger el derecho a la privacidad y al honor de los ciudadanos[87] bien mediante la elaboración de nuevas normas o a través de la actualización de las existentes (Honduras, Ecuador, Chile y México).

II. PAÍSES Y REGIONES DESTINATARIAS DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS AUTORIZADAS POR LA AEPD

Como indicamos en el punto anterior, los países iberoamericanos han realizado y siguen efectuando notables esfuerzos en materia de protección de datos personales. Sin embargo, un análisis de los datos recogidos en las Memorias anuales elaboradas por la Agencia Española de Protección de Datos (AEPD)[88] sobre el destino de las transferencias internacionales de datos personales efectuadas desde España pone de manifiesto que los países latinoamericanos deben incrementar sus esfuerzos si quieren mantener su posición como países receptores de las transferencias de datos internacionales (TID) realizadas desde España haciendo frente así al avance que, como destinatarias de este tipo de transferencias, están experimentando otras regiones.



[85] *LÓPEZ CABALLO, D.A., GONZALEZ-CALERO MANZANARES, F.R. (coords.), Protección de datos y habeas data: una visión desde Iberoamérica, AEPD, Madrid, 2015. Disponible en el sitio web: http://bit.ly/1JrfjKz (Fecha de consulta 15 de abril de 2016).*

[86] *En este sentido, la Constitución peruana de 1993, la Constitución Federal argentina de 1994, la Constitución de Honduras, la Carta Magna de 2008 de la República del Ecuador o la Constitución Política de Colombia.*

[87] *Cabe citar las siguientes: en Argentina, la Ley 25.326 de Protección de Datos de 2 de noviembre de 2000; en Colombia, la Ley Estatutaria 1851 que dicta disposiciones generales para la protección de datos personales; en Perú, la Ley 29733 de Protección de Datos Personales; en Uruguay, la Ley 18.331 de Protección de Datos Personales y Acción Habeas Data; o en la República Dominicana, la Ley Orgánica 172-13 de Protección de Datos de Carácter Personal.*

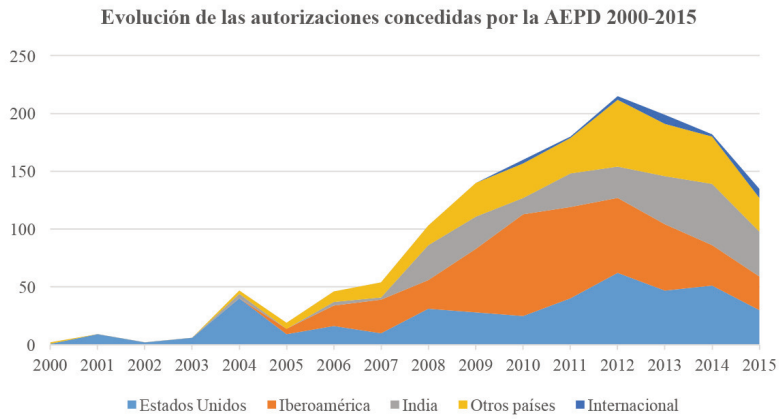
[88] *En particular, AEPD, Memoria de 2014, Agencia Estatal Boletín Oficial del Estado, Madrid, 2015 y Memoria de 2015, Agencia Estatal Boletín Oficial del Estado, Madrid, 2016. Disponibles en los sitios web http://bit.ly/1U51VPJ y http://bit.ly/293z8w3 (Fecha de consulta 22 de julio de 2016).*

Durante el período 2000-2015, el número de TID autorizadas por la AEPD se ha incrementado. Sus principales destinatarios son los países iberoamericanos (483 autorizaciones frente a las 456 del año anterior) seguidos por las 407 autorizaciones que acumula Estados Unidos (377 hasta 2014). Sin embargo, India alcanza ya la cifra de 271 (232 si tenemos en cuenta los datos de 2014) y cada vez son más los países que resultan destinatario de las TID efectuadas desde España.

EVOLUCIÓN DE LAS REGIONES RECEPTORAS DE LAS TRANSFERENCIAS DE DATOS AUTORIZADAS POR LA AEPD EN EL PERÍODO 2000-2015

REGIONES	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Estados Unidos	1	9	2	6	40	9	16	10	31	28	25	40	62	47	51	30
Iberoamérica	0	0	0	0	0	5	18	29	25	55	88	79	65	57	35	29
India	0	0	0	0	4	0	3	2	30	28	14	29	27	42	53	39
Otros países	1	0	0	0	3	5	9	13	17	29	30	31	58	45	41	29
Internacional	0	0	0	0	0	0	0	0	0	0	3	1	3	8	2	8
TOTAL	2	9	2	6	47	19	46	54	103	140	160	180	215	199	182	135

Si bien se ha reducido el número de las autorizaciones concedidas por la AEPD para TID destinadas a países iberoamericanos, han aumentado aquellas dirigidas a India; tendencia que se habrían mantenido también en los primeros meses de 2016 aunque aún no contamos para este periodo con datos definitivos de la AEPD.



En consecuencia, los países iberoamericanos deben aunar sus esfuerzos y aumentarlos si quieren resultar atractivos como países destinatarios de las TID que se efectúen tanto desde España como desde el resto de países de la Unión Europea. Solo así lograrán aumentar su cuota de mercado en lo que a transferencias de datos personales se refiere. Para lograrlo deberán aproximar su marco normativo al existente en España -y, por tanto, al de la Unión Europea- lo que exige conocer los requisitos, las condiciones y los procedimientos que deberán cumplir como receptores de TID.

III. MARCO NORMATIVO DE LAS TID QUE SE EFECTÚEN DESDE ESPAÑA A PAÍSES IBEROAMERICANOS

A continuación, se presentan los principales instrumentos normativos que resultarán de aplicación a las TID realizadas desde España a países iberoamericanos. Sin embargo, también merecen ser mencionados: la Declaración Universal de Derechos Humanos de las Naciones Unidas de 1948 como primer instrumento jurídico internacional que reconoce el derecho a la protección de la esfera privada de las personas frente a la intrusión de otros y, en especial, del Estado[89]; y el Convenio Europeo de Derechos Humanos de 1950[90] que reconoce el derecho a la protección de los datos personales, garantiza el derecho al respeto de la vida privada y familiar, el domicilio y la correspondencia y determina las condiciones necesarias para poder limitar este derecho (arts. 7 y 8).

El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio n.º 108)

El Convenio n.º 108 es el único instrumento internacional jurídicamente vinculante en materia de protección de datos personales entendiendo por "dato personal" «cualquier información relativa a una persona física identificada o identificable» (art. 2.1). El Convenio resulta de aplicación al tratamiento automatizado de los datos de carácter personal lo que incluye tanto operaciones lógicas aritméticas como su modificación, borrado, extracción o difusión siempre que se efectúen, total o parcialmente, con ayuda de procedimientos automatizados (arts. 1 y c) del Convenio n.º 108).

Los flujos transfronterizos de datos se definen como aquellas transmisiones realizadas por cualquier medio a través de las fronteras nacionales de datos de carácter personal que sean objeto de un tratamiento automatizado o cuando se reúnan con el propósito de someterlos a ese tratamiento. Aunque, con carácter general, el Convenio n.º 108 permite la libre circulación de los datos personales entre los Estados parte del mismo incorpora ciertas excepciones como, por ejemplo, cuando la transferencia se produzca a un país que no sea parte del Convenio y el flujo internacional entre Estados parte se realice con el propósito de vulnerar la legislación del Estado origen del flujo de datos.

Todos los Estados miembros de la Unión Europea (UE)[91] han ratificado el Convenio n.º 108. En 1999

---

[89] *Declaración Universal de Derechos Humanos de las Naciones Unidas de 10 de diciembre de 1948. Disponible en el sitio web: http://www.un.org/en/documents/udhr/ (Fecha de consulta 20 de abril de 2016). Entre otros muchos, son Estados miembros de las Naciones Unidas: Argentina (fecha de admisión 24-10-1945); Bolivia (14-11-1945); Brasil (24-10-1945); Chile (24-10-1945); Colombia (5-11-1945); Costa Rica (2-11-1945); Cuba (24-10-1945); Ecuador (21-12-1945); El Salvador (24-10-1945); Guatemala (24-11-1945); Honduras (17-12-1945); México (7-11-1945); Nicaragua (24-10-1945); Panamá (13-11-1945); Perú (31-10-1945); República Dominicana (24-10-1945); Uruguay (18-12-1945); Venezuela (15-11-1945); Alemania; Austria; Bélgica; Bulgaria; Chipre; Croacia; Dinamarca; Eslovaquia; Eslovenia; España; Estonia; Finlandia; Francia; Grecia; Hungría; Irlanda; Italia; Letonia; Lituania; Luxemburgo; Malta; Países Bajos; Polonia; Portugal; Reino Unido; República Checa; Rumanía y Suecia. Disponible en el sitio web: http://www.un.org/es/member-states/ (Fecha de consulta 20 de abril de 2016).*

[90] *Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales. Disponible en el sitio web: http://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/005 (Fecha de consulta 20 de abril de 2016).*

[91] *Actualmente forman parte de la UE veintiocho países: Alemania (miembro desde 1958); Austria (1995); Bélgica (1958); Bulgaria (2007); Chipre (2004); Croacia (2013); Dinamarca (1973); Eslovaquia (2004); Eslovenia (2004); España (1986); Estonia (2004); Finlandia (1995); Francia (1958); Grecia (1981); Hungría (2004); Irlanda (1973); Italia (1958); Letonia (2004); Lituania (2004); Luxemburgo (1958); Malta (2004); Países Bajos (1958); Polonia (2004); Portugal (1986); Reino Unido (1973); República Checa (2004); Rumanía (2007) y Suecia (1995). Disponible en el sitio web: http://bit.ly/1zomIVP (Fecha de consulta 20 de abril de 2016).*
Resulta obligado hacer una breve referencia al referéndum que tuvo lugar el pasado 23 de junio de 2016 sobre la permanencia de Reino Unido en la UE y que ha tenido como resultado el denominado "Brexit" (British Exit o "salida

se modificó para que la UE, en su conjunto, pudiera formar parte del mismo[92] y dos años después se adoptó un Protocolo Adicional para introducir disposiciones sobre los flujos transfronterizos de datos a los Estados no parte (terceros países) e incorporar la obligación de contar con autoridades nacionales de supervisión de la protección de los datos[93].

Además, el Convenio n.º 108 se encuentra abierto a la incorporación de países que no pertenecen al Consejo de Europa[94] destacando, en este sentido, la adhesión de Uruguay en agosto de 2013; si bien la Comisión Europea ya había declarado previamente su adecuado nivel de protección mediante Decisión 2012/484/UE.

La Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre, 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 el ámbito de la UE, la Directiva 95/46/CE constituye el principal instrumento legal en materia de

británica) al haber sido apoyada esta opción por el 51,9% de los votos. Si bien el cambio no será repentino se abre un período transitorio en el que, por primera vez, se llevará a cabo el procedimiento establecido en el art. 50 del Tratado de la UE que finalizará con un acuerdo de salida. Este acuerdo será sometido para su aprobación al Parlamento Europeo antes de que el Consejo -antiguo Consejo de Ministros de la UE- lo eleve a definitivo y entrará en vigor en la fecha que conste en el mismo o, en su defecto, a los dos años de la notificación de la retirada contados desde su notificación -no desde el referéndum- salvo que el Consejo Europeo de conformidad con Reino Unido decidan prorrogar el plazo. Algunos autores han estimado que este proceso puede durar entre cuatro y siete años. FREIXES, T., "El Brexit y sus implicaciones", Diario La Ley, n.º 8791, 27 de junio de 2016.

Con relación a la TID, la salida de Reino Unido de la UE hará que pase a considerarse un país externo a la UE. Por tanto, para realizar TID a Reino Unido será necesario que se garantice la existencia de un nivel de protección adecuado. La cuestión no carece de importancia porque además el proceso de salida se producirá en el período en el que el nuevo Reglamento de protección de datos personales que incrementa el nivel de protección recogido en la Directiva vigente. De este modo, las empresas establecidas en el mercado interior europeo se adaptarán al nuevo marco legal y establecerán estándares muy elevados de protección de datos mientras que Reino Unido difícilmente conseguirá una regulación más protectora lo que provocará que las empresas modifiquen sus estrategias internas sobre TID incluso cuando Reino Unido se adapte voluntariamente a los estándares europeos. MACHUCA, J.C., SARMIENTO, D., "Brexit: consecuencias jurídicas y empresariales del referéndum", Diario La Ley, n.º 8784, Sección Tribunal, 16 de junio de 2016, Ref. D-240.

La salida de Reino Unido de la Unión Europea hace que el futuro de las leyes de protección de datos sea más incierto. Las numerosas empresas multinacionales establecidas en Reino Unido pueden verse afectadas por la incertidumbre que la salida genera y, aunque habrá que esperar para ver cómo se desarrolla el proceso de salida de Reino Unido de la UE, cabe aventurar que las consecuencias serán de gran calado y que no se producirán solo en el ámbito jurídico. Pueden consultarse, entre otros: GONZÁLEZ, A., "Si hay Brexit hay transferencia internacional de datos a Reino Unido", 23 de junio de 2016. Disponible en el sitio web: http://bit.ly/2aB4HeB (Fecha de consulta 22 de julio de 2016); GIL GONZÁLEZ, E., "Brexit: transferencias internacionales de datos y comercio electrónico", 29 de junio de 2016, Blog Ecija. Disponible en el sitio web: http://bit.ly/2aB5kVq (Fecha de consulta 22 de julio de 2016); ROBINSON, D., "¿Cómo afecta el Brexit a la transferencia de datos?", Financial Times, 17 de julio de 2016. Disponible en el sitio web: http://bit.ly/2a5ZlbW (Fecha de consulta 22 de julio de 2016).

92 *Modificaciones del convenio para la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal (CETS nº 108) para permitir la adhesión de las Comunidades Europeas, adoptado por el Comité de Ministros, el 15 de junio en Estrasburgo. Disponible en el sitio web: http://bit.ly/1YXWoLu (Fecha de consulta 25 de abril de 2016).*

93 *Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos en lo que respecta a las autoridades de control y los flujos transnacionales de datos, CETS nº 181, 2001. Disponible en el sitio web: http://bit.ly/1SB6VMm (Fecha de consulta 23 de abril de 2016).*

94 *La solicitud de adhesión debe contener información relativa al marco jurídico de protección de datos y, en especial, sobre: la legislación (ley de protección de datos y normas sectoriales); la existencia de una autoridad de control, su composición, estatuto y actividades; y, eventualmente, información sobre la jurisprudencia. Disponible en el sitio web: http://bit.ly/1VFlp07 (Fecha de consulta 30 de abril de 2016).*

protección de datos personales. Pretende, partiendo de los principios recogidos en el Convenio n.º 108, garantizar que exista un mismo nivel de protección de los derechos y libertades de las partes y, en particular, de su intimidad en toda la UE evitando así que la elaboración de legislaciones nacionales pueda incidir negativamente en la libre circulación de datos, bienes y servicios, capitales y personas en el mercado interior.

Cabe destacar que esta Directiva resulta de aplicación no solo a los Estados miembros de la UE sino también a ciertos Estados no miembros que formaban parte del Espacio Económico Europeo (EEE)[95] como ocurre en el caso de Islandia, Liechtenstein y Noruega.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo (RLOPD)

La LOPD permitió la transposición de la Directiva 95/46/CE al ordenamiento jurídico español y, al igual que el RLOPD, resulta de aplicación tanto a las actividades realizadas por un responsable del tratamiento en territorio español como cuando, a pesar de no tenerlo, se recurra para el tratamiento a medios -automatizados o no- situados en territorio español salvo si estos se utilizan tan solo con fines de tránsito (art. 4.1 de la Directiva)[96].

Según el art. 5.1.s) del RLOP, una transferencia internacional de datos (TID) es aquel tratamiento de datos personales que implica su transmisión fuera del EEE, ya sea una cesión o una comunicación de los datos o tenga por objeto su tratamiento por cuenta del responsable del fichero establecido en territorio español. A nivel nacional, la TID queda regulada en los arts. 33 y 34 de la LOPD y arts. 65 a 70 y 137 a 140 del RLOPD.

En este sentido, el exportador de datos personales será la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una TID y el importador aquella persona física o jurídica, pública o privada, u órgano administrativo que reciba la TID como responsable del tratamiento, encargada del mismo o tercero que, teniendo en cuenta nuestro ámbito de estudio, deberá encontrarse necesariamente en un país iberoamericano (letras j) y ñ) del art. 5.1 del RLOPD). Todas las TID realizadas desde España deberán cumplir la LOPD y el RLOPD y comunicarse a la AEPD para su inscripción en el Registro General de Protección de Datos (art. 65 del RLOPD).

El Reglamento Europeo de Protección de Datos Personales

El pasado 8 de abril de 2016 el Consejo de Europa adoptó en primera lectura el Reglamento europeo de protección de datos y el 14 de abril hizo lo propio el Parlamento Europeo. El Reglamento será de aplicación dos años después de su entrada en vigor; momento en el que sustituirá a la Directiva 95/46/CE.

El Reglamento pretende poner fin a las diferencias generadas por la transposición de la Directiva 95/46/CE a los ordenamientos nacionales de los Estados miembros y, por tanto, acabar con los posibles obstáculos que pueden generarse en el ámbito de las transacciones transfronterizas intracomunitarias de datos personales.

El Reglamento establece unas reglas detalladas y comprensibles para las TID e introduce algunas herramientas nuevas como, por ejemplo, los códigos de conducta o los mecanismos de certificación que

---

[95] *El Espacio Económico Europeo (EEE) lo forman: los Estados de la UE; Islandia; Liechtenstein; y Noruega. Disponible en el sitio web: http://bit.ly/1O3ci1n (Fecha de consulta 20 de abril de 2016).*

[96] *Entre otras, la STJUE de 13.05.2014, asunto Google Spain C-131/12 sobre la aplicación del Derecho comunitario y la STJUE de 1.10.2015, asunto Weltimmo C-230/14 sobre la determinación de la ley nacional aplicable y la autoridad nacional competente. Disponibles en los sitios web: http://bit.ly/2a332A6 y http://bit.ly/29PS8LF, respectivamente (Fecha de consulta 21 de julio de 2016).*

podrán utilizarse junto con las habituales cláusulas contractuales tipo (CCT) o las reglas corporativas vinculantes (RCV) de las que hablaremos más adelante.

Además, hace referencia expresa a la facultad de las autoridades nacionales de control (ANC) para suspender el flujo de datos a un tercer país u organización internacional y establece un catálogo preciso y detallado de los elementos que la Comisión Europea deberá tener en cuenta para evaluar si un determinado país cuenta con un nivel adecuado de protección. Entre estos aspectos figuran los siguientes: el acceso de las autoridades públicas a los datos personales; la eficacia de los mecanismos de protección existentes; su posible ejecución; o los recursos con los que se cuenta para solicitar, de forma efectiva, una compensación administrativa y judicial en línea con la Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 asunto Schrems[97]. Sin embargo, también nos parece interesante la obligación que impone a la Comisión Europea de revisar, al menos cada cuatro años, todas las decisiones sobre adecuación que emita; medida que permitirá detectar lo antes posible los cambios que vayan produciendo respecto al nivel de protección de los datos personales.

IV. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES DESDE ESPAÑA A PAÍSES IBEROAMERICANOS CON UN NIVEL ADECUADO DE PROTECCIÓN

Al amparo del art. 25 de la Directiva 95/46/CE, la transferencia a terceros países de datos personales que sean objeto de tratamiento o estén destinados a ser objeto de tratamiento con posterioridad a su transferencia solo puede permitirse cuando el país tercero garantice un nivel de protección adecuado. Por tanto, queda prohibida la TID a países que no cuenten con un nivel adecuado de protección.

Su adecuación se medirá con relación al nivel de protección garantizado en el ámbito de la UE y teniendo en cuenta todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos y, en particular, las siguientes: la naturaleza de los datos; la finalidad y la duración del tratamiento o de los tratamientos previstos; el país de origen y el país de destino final; las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate; así como las normas profesionales y las medidas de seguridad en vigor en dichos países (art. 25.2 de la Directiva 95/46/CE).

Estos requisitos de adecuación han sido desarrollados por parte del Grupo del Artículo 29[98] y pueden clasificarse en dos bloques: a) por un lado, el contenido de las normas aplicables a los datos personales transferidos a un tercer país cuyo examen comprendería los siguientes aspectos: la limitación de objetivos; la proporcionalidad y la calidad de los datos; la transparencia; la seguridad; el acceso, la rectificación y la oposición; y cuando se trate de transferencias sucesivas a otros terceros países aquellos que deban analizarse si además son datos sensibles, mercadotecnia directa o decisión individual automatizada; y b) por el otro, los mecanismos del procedimiento/de aplicación que garantizan su eficacia y, por tanto, las disposiciones sobre responsabilidades, sanciones, recursos, autoridades de control y notificaciones para comprobar si ofrecen un nivel satisfactorio de cumplimiento de las normas, apoyo y asistencia a los interesados en el ejercicio de sus derechos y vías adecuadas de recurso para quienes resulten perjudicados por inobservancia de las normas.Con relación a los países iberoamericanos, la

---

[97] *Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2013. Maximillian Schrems contra Data Protection Commissioner. Asunto C-362/14. Disponible en el sitio web: http://bit.ly/1NaSe2d (Fecha de consulta 20 de abril de 2016).*

[98] *Grupo del Artículo 29, Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE aprobado el 24 de julio de 1998 (WP 12). Disponible en el sitio web: http://bit.ly/1NaJiKh (Fecha de consulta 28 de abril de 2016).*

Comisión Europea ha declarado que cuentan con un nivel adecuado de protección[99] Argentina[100] y Uruguay. En consecuencia, las TID que se efectúen desde España a estos países no requieren ningún tipo de trámite o autorización especial (art. 34.k) de la LOPD y arts. 66.2, 67.1 y 68 del RLOPD). Además, Uruguay se ha adherido al Convenio n.º 108 en 2013 lo que aumentará notablemente su atractivo como posible país destinatario de las TID no solo cuando para TID realizadas desde España o desde cualquier otro Estado miembro de la UE -como consecuencia de la Decisión de la Comisión Europea- sino también con relación a aquellas TID efectuadas por Estados parte del Convenio n.º 108 que establece un marco de libertad para las TID que realicen entre ellos.

La decisión de la Comisión Europea sobre la adecuación de un determinado país vincula a los Estados miembros y a los órganos que forman parte de aquellos lo que incluye tanto a los tribunales nacionales como a las autoridades nacionales de control (ANC) que estarán obligadas a adoptar las medidas necesarias para garantizar el cumplimiento de la decisión.

En consecuencia, cuando la Comisión haya dictado una decisión sobre el nivel adecuado de protección de un determinado país y la AEPD tenga conocimiento mediante la solicitud de una persona cuyos datos personales hubieran sido o pudieran ser objeto de transferencia a aquellos de que quizás ese país no cumple los estándares necesarios solo tendrá dos opciones: a) si considera fundada la solicitud, comparecer ante los tribunales para que estos planteen una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europeo (TJUE) que deberá resolver sobre la posible invalidez de la decisión de la Comisión; o b) cuando la considere infundada, desestimar la solicitud de manera que sea el interesado quien recurra a los tribunales para que, en su caso, planteen la correspondiente cuestión prejudicial ante el TJUE.

Aunque ningún Estado miembro ha utilizado esta posibilidad, pueden declarar que un determinado país cuenta con un adecuado nivel de protección. En el caso español, el Director –actualmente Directora- de la AEPD debería emitir una resolución, previo examen de todas las circunstancias que concurren en la transferencia o categoría de transferencia de datos y, en particular, de 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 UE; así como de las normas profesionales y las medidas de seguridad vigentes en aquel país. Esta resolución se publicaría en el BOE y se procederá a actualizar la relación de países con un nivel de protección adecuado (art. 67 del RLOPD).

V. TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES A PAÍSES IBEROAMERICANOS QUE NO CUENTAN CON UN NIVEL ADECUADO DE PROTECCIÓN

Cuando la TID desde España se dirija a un país iberoamericano que no garantice un nivel adecuado de protección en los términos analizados en el apartado anterior, resultará necesario que el exportador obtenga, antes de llevarla a cabo, una autorización específica para esa transferencia (art. 26.2 de la Directiva). Esta regla general presenta una serie de excepciones cuando la TID: a) cuente con el consentimiento inequívoco del interesado[101]; b) sea necesaria para ejecutar el contrato entre el interesado

---

[99] *La Comisión Europea ha declarado que cuentan con un nivel adecuado de protección los siguientes países: Andorra, Argentina, Canadá (sector privado), Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda y Uruguay.*

[100] *Mediante Decisión 2003/490/CE de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y el Consejo sobre la adecuación de la protección de los datos personales en Argentina (texto pertinente a efectos del EEE), DOUE L 168/19 de 5 de julio de 2003 en base al Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina adoptado el 3 de octubre de 2002 (WP63). Disponible en el sitio web: http://bit.ly/24ctEpq (Fecha de consulta 20 de abril de 2016).*

[101] *Al amparo del art. 2.h) de la Directiva 95/46/CE, el consentimiento del interesado debe ser libre, específico e informado*

y el responsable del tratamiento[102] o las medidas precontractuales adoptadas a petición del interesado[103]; c) resulte precisa para la celebración o ejecución de un contrato celebrado o por celebrar en favor del interesado, entre el responsable del tratamiento y un tercero; d) sea indispensable o venga legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; e) se requiera para la salvaguardia del interés vital del interesado; f) tenga lugar desde un registro público concebido para facilitar información al público; g) resulte de la aplicación de tratados o convenios en que sea parte España; h) se haga a efectos de prestar o solicitar auxilio judicial internacional; i) se precise para la prevención o diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios; o j) sea una transferencia dineraria según su legislación específica (art. 26.1 de la Directiva y en los apdos. a) a j) del art. 34 de la LOPD).

En los demás casos, la TID de datos personales desde España a un país que no cuente con un nivel adecuado de protección exige autorización previa y específica del Director de la AEPD. El exportador de datos personales deberá efectuar la correspondiente solicitud y prestar garantías en torno a la protección de la vida, de los derechos y libertades fundamentales de las personas y del ejercicio de los respectivos derechos (arts. 26.2 de la Directiva y 70.2 del RLOPD) mediante: la incorporación en el contrato celebrado con el importador de determinadas cláusulas contractuales ya sean cláusulas contractuales tipo (CCT) o cláusulas *ad hoc;* o la adopción de reglas corporativas vinculantes (RCV) por el grupo multinacional de empresas donde se desarrolle la transferencia.

> Mediante incorporación de determinadas cláusulas contractuales tipo (CCT) en el contrato celebrado entre exportador e importador de datos personales

El exportador puede ofrecer garantías suficientes con relación a la protección de datos personales alegando la incorporación de ciertas CCT en el contrato celebrado entre el exportador y el importador de datos. Para que una CCT cumpla esta función debe compensar satisfactoriamente la ausencia de una protección general adecuada y, por tanto, incluir aquellos elementos que se consideran esenciales al analizar la adecuación del nivel de protección de los datos personales en un determinado país.

La solución contractual debe obligar a las partes de la TID a garantizar la aplicación íntegra del conjunto de principios básicos de protección de datos al tratamiento de los datos transferidos al país comunitario e incluso de los principios complementarios que resulten necesarios por tratarse de datos sensibles, mercadotecnia directa o decisiones automatizadas. Además, se debe estipular minuciosamente la forma en que el receptor de la TID debe aplicar estos principios y especificar otras cuestiones tales como: los fines de la transferencia, las categorías de los datos, el plazo límite de conservación o las medidas de seguridad.

La solución contractual debe tener además efectividad práctica en la línea sostenida al analizar el nivel de adecuación de un determinado. Con las CCT puede ser más difícil garantizar esta eficacia al tener que suplir la falta de mecanismos de supervisión y de aplicación y ofrecer a los interesados –incluso cuando no sean parte de contrato- apoyo, asistencia y, en última instancia, vías de recurso.

En consecuencia, puede ocurrir que las normas jurídicas generales del tercer país obliguen al receptor

---

de manera que cuando la aplicación de la excepción queda condicionada al cumplimiento de todos y cada uno de estos requisitos.

[102] *Todos los datos transferidos deben ser necesarios para celebrar o ejecutar el contrato de manera que cuando no lo sean quedarán fuera de la excepción.*

[103] *La excepción solo abarca aquellas situaciones iniciadas por el interesado mediante, por ejemplo, la petición de información sobre un servicio en particular. Por tanto, no incluye las propuestas de mercadotecnia planteadas por el responsable del tratamiento.*

de la TID a comunicar los datos personales a las autoridades en determinadas circunstancias y que esa obligación prevalezca sobre sobre las CCT que el exportador y el importador han incorporado a su contrato. Si bien la Directiva 95/46/CE exige que este tipo de comunicaciones se ciñan únicamente a las que resulten imprescindibles para cumplir los imperativos de orden público de las sociedades democráticas enunciados en su art. 13.1, el contrato puede resultar un instrumento demasiado frágil como para ofrecer garantías suficientes con relación a la protección de datos y, por tanto, no ser un instrumento útil para lograr la autorización de la TID.

Con carácter general, en las CCT deben tenerse en cuenta las siguientes cuestiones: a) una estipulación a favor de tercero para que el afectado pueda hacer valer el contrato en caso de vulneración; b) una cláusula de responsabilidad solidaria entre las partes (responsable-responsable) o basada en "*culpa in eligendo*" o "*in vigilando*" o subsidiaria (responsable-encargado); c) la restricción de las transferencias posteriores; d) una cláusula sobre seguridad y control del cumplimiento de las garantías y de los compromisos establecidos en las CCT; y e) una estipulación impidiendo la modificación de las cláusulas a favor de tercero.

A pesar de los posibles inconvenientes que puede plantear el uso de CCT, presenta importantes ventajas; especialmente, si se trata de TID similares y repetitivas al permitir su supervisión de un modo eficaz y rápido; cuestión de gran relevancia si tenemos en cuenta que el número de TID no deja de aumentar.

La Comisión Europea ha dictado una serie de decisiones reconociendo que cuando se incorporen determinadas CCT en el contrato entre exportador e importador de datos cabe presuponer que el exportador aporta las garantías necesarias para autorizar esa TID. En este sentido, si la TID se produce entre responsables de datos deben tenerse en cuenta la Decisión 2001/497/CE[104] y 2004/915/CE[105]; y cuando sea entre un responsable de datos y un encargado del tratamiento o un encargado acudir a la Decisión 2002/16/CE[106] que resulta también aplicable a TID entre encargados y subencargados del tratamiento ubicados en un país tercero.

Los Estados miembros también pueden declarar que la incorporación de ciertas CCT en el contrato entre exportador e importador de datos ofrece las garantías necesarias. La AEPD ha hecho uso de esta facultad al sostener que la inclusión de ciertas CCT[107] en el contrato se celebre entre un encargado del tratamiento y un subencargado ubicado en un país tercero[108] permite presuponer la existencia del nivel de protección requerido.

Mediante la adopción de reglas corporativas vinculantes (RCV) por parte del grupo empresarial en el que se realice la TID

---

[104] *Decisión 2001/497/CE de la Comisión de 15 de junio de 2001 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, DOCE L 181/19 de 4 de julio de 2001.*

[105] *Decisión 2004/915/CE de la Comisión de 27 de diciembre de 2004 por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países, DOUE L 385/74 de 29 de diciembre de 2004.*

[106] *Decisión 2002/16/CE de la Comisión de 27 de diciembre de 2001 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE, DOCE L 6/52 de 10 de enero de 2002.*

[107] *Resolución de autorización de transferencias internacionales de datos a Perú. Nº expediente: TI/00126/2012 de 16 de octubre de 2012 de la AEPD. Disponible en el sitio web: http://bit.ly/1VYRdxo (Fecha de consulta 28 de abril de 2016). El modelo definitivo de cláusulas contractuales entre encargados a subencargados del tratamiento. Disponible en el sitio web: http://bit.ly/1O3cBJF (Fecha de consulta 29 de abril de 2016).*

[108] *La posibilidad ya había sido señalada por el Dictamen 3/2009 sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (de los responsables a los encargados del tratamiento) emitido el 5 de marzo de 2009 por el Grupo del Artículo 29. Disponible en el sitio web: http://bit.ly/24rQuG1 (Fecha de consulta 20 de abril de 2016) y en el considerando 23 de la Decisión 2010/87/CE.*

Cuando la transferencia se efectúe desde una empresa exportadora española a otra que se encuentre ubicada en un país tercero y ambas formen parte del mismo grupo empresarial, resulta posible que la empresa exportadora al solicitar la correspondiente autorización alegue la adopción de RCV por el grupo empresarial en cuyo seno se pretende llevar a cabo la TID.

La adopción de RCV pretende facilitar la TID entre empresas del mismo grupo multinacional con base en estándares de protección de datos y procedimientos que garanticen -unilateral o contractualmente- su cumplimiento dentro y fuera de la empresa -incluso frente a los posibles afectados- y evitar que cada autoridad nacional de control resuelva de forma diferente.

Sin embargo, para considerar que las RCV ofrecen suficiente garantía y, por tanto, obtener la oportuna autorización deben ser vinculantes para las empresas del grupo empresarial y exigibles no solo por parte de la AEPD sino también por los interesados cuyos datos sean objeto de tratamiento conforme al ordenamiento jurídico español (art. 70.4 del RLOPD).

Las RCV deben elaborarse en el seno del grupo empresarial y presentarse una solicitud estándar ante la ANC considerada líder. Esta autoridad –en nuestro caso, la AEPD- revisará las RCV y elaborará un proyecto definitivo de las mismas dando traslado del mismo al resto de ANC bien para su conocimiento si forman parte del procedimiento de reconocimiento conjunto[109] o, en caso contrario, para que formulen los comentarios que consideren convenientes en el plazo de un mes. En todo caso, para la adopción de las RCV resulta necesario que la ANC líder notifique la conformidad de las RCV al solicitante y al GT29.

Las RCV pueden clasificarse según se dirijan a los responsables del tratamiento (WP74[110], WP107[111], WP108[112], WP133[113], WP153[114], WP154[115] y WP155[116] del GT29) o a los encargados del mismo (WP195a[117] y WP204[118] del GT29) pero siempre deberán regular los siguientes aspectos: a) el respeto a los principios de protección de datos de la UE y de los Estados miembros; b) la determinación de los flujos de información y de los fines del tratamiento; c) la posible limitación de las transferencias a entidades del grupo o de las transferencias posteriores bajo el esquema de garantías; d) la obligatoriedad interna y externa de las RCV; e) la posibilidad de obtener una reparación e indemnización por parte del afectado o de plantear, en su caso, recursos; f) los procedimientos para su ejecución; g) la cooperación con las autoridades de control; h) el procedimiento de actualización; y i) la jurisdicción competente.

---

[109] *Si la ANC control líder considera que las RCV cumplen los requisitos establecidos por el GT29, el resto de ANC del procedimiento de reconocimiento mutuo aceptarán su opinión.*

[110] *GT29, Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las CRV. Disponible en el sitio web: http://bit.ly/1WZE32a (Fecha de consulta 15 de abril de 2016).*

[111] *GT29, Documento sobre la competencia de las Autoridades de Control europeas en el procedimiento coordinado de aprobación de las CRV. Disponible en el sitio web: http://bit.ly/1SVxJsz (Fecha de consulta 20 de abril de 2016).*

[112] *GT29, Modelo de solicitud de autorización de transferencia internacional basada en CRV en el ámbito del procedimiento coordinado. Disponible en el sitio web: http://bit.ly/1NJjOnj (Fecha de consulta 18 de abril de 2016).*

[113] *GT29, Recomendación 1/2007 sobre la aplicación de las CRV a transferencias de datos personales. Disponible en el sitio web: http://bit.ly/1VFm5mh (Fecha de consulta 20 de abril de 2016).*

[114] *GT29, Cuadro que establece la relación de los elementos y principios que deben contener las CRV. Disponible en el sitio web: http://bit.ly/1TBVB1f (Fecha de consulta 26 de abril de 2016).*

[115] *GT29, Cuadro que establece la estructura de las CRV (WP 154). Disponible en el sitio web: http://bit.ly/26E5KBM (Fecha de consulta 20 de abril de 2016).*

[116] *GT29, Preguntas más frecuentes sobre CRV (WP155). Disponible en el sitio web: http://bit.ly/1O3f5b1 (Fecha de consulta 20 de abril de 2016).*

[117] *GT29, Recomendación 1/2012 sobre el modelo para la aprobación de CRV en la transferencia de datos personales. Disponible en el sitio web: http://bit.ly/1TbL61U (Fecha de consulta 20 de abril de 2016).*

[118] *GT29, Documento explicativo sobre las CRV. Disponible en el sitio web: http://bit.ly/1QHfsHW (Fecha de consulta 20 de abril de 2016).*

VI. CONCESIÓN O DENEGACIÓN DE LA AUTORIZACIÓN DE LA TID POR PARTE DE LA AEPD

Cuando para llevar a cabo una TID resulte necesario obtener la autorización previa y específica de la AEPD, el exportador debe: presentar una solicitud identificando el fichero de datos objeto de TID, su denominación y su código de inscripción en el Registro General de Protección de Datos así como la transferencia cuya autorización solicita; aportar la documentación acreditativa de las garantías de protección necesarias y los poderes de los otorgantes del contrato; y acreditar el cumplimiento del resto de requisitos exigidos para realizar la transferencia (art. 137 del RLOPD).

A continuación, se abrirá un período de información pública de diez días a contar desde la publicación en el BOE del correspondiente anuncio y, una vez finalizado, se dará traslado al solicitante de las alegaciones presentadas para que conteste en diez días (art. 138 del RLOPD). Posteriormente, el Director de la AEPD deberá emitir en un plazo de tres meses desde la presentación de la solicitud una resolución accediendo, denegando o archivando la solicitud de autorización; en caso contrario, la autorización se entenderá concedida por silencio administrativo positivo (art. 140 del RLOPD).

La autorización de la TID puede denegarse cuando: a) la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impida garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos garantizados en el mismo; b) la entidad destinataria haya incumplido previamente las garantías establecidas en CCT; c) existan indicios racionales de que el importador no está respetando o no respetará las garantías ofrecidas por el contrato o de que los mecanismos de aplicación del mismo no son o no serán efectivos; o d) la TID pueda generar una situación de riesgo y daño efectivo a los afectados (art. 70.3 del RLOPD).

VII. LA SUSPENSIÓN TEMPORAL DE UNA TID

El nivel de protección de un determinado país puede variar a lo largo del tiempo[119] y tener que suspender una TID autorizada previamente. En este sentido, la Comisión Europea debe comprobar periódicamente si la decisión que dictó declarando el nivel adecuado de protección en un determinado Estado «sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión»; especialmente, cuando existan indicios que hagan sospechar lo contrario, como sucedía en el marco del acuerdo de puerto seguro[120], al objeto de iniciar los trámites necesarios para restablecer el marco de protección[121].

---

[119] *Por este motivo, el nuevo Reglamento europeo exige a la Comisión revisar las decisiones alcanzadas sobre la adecuación del nivel de protección de un determinado país al menos cada cuatro años y el GT29 en su Documento de Trabajo (WP12) advertía de que, debido a la posibilidad de que el nivel de protección varíe, las decisiones emitidas al respecto no debían ser consideradas estáticas ni definitivas.*

[120] *El nuevo acuerdo entre EEUU-UE y la propuesta de Reglamento de protección de datos insisten en revisar el nivel de adecuación de los países de forma periódica.*

A nivel nacional, el Director de la AEPD también puede -en ejercicio de la facultad que le concede el art. 37.1.f) de la LOPD y previa audiencia del exportador- llegar a suspender temporalmente la TID a un determinado Estado. Si se trata de una TID a un país con relación al cual la Comisión haya constatado la existencia de un nivel adecuado de protección, será posible su suspensión temporal si: a) las autoridades de protección de datos del Estado importador o cualquier otra competente -si no existen las primeras- declaran la vulneración por parte del importador de las normas de protección de datos establecidas en su Derecho interno; o b) existen indicios racionales de que el importador está vulnerando las normas o los principios de protección de datos y las autoridades competentes de aquel Estado no hayan adoptado o no vayan a adoptar las medidas oportunas para resolver el caso a pesar de haber sido advertidas de la situación por la AEPD (art. 69.1 del RLOPD). La resolución del Director de la AEPD que declare la suspensión de la TID deberá comunicarse a la Comisión Europea (art. 69.2 del RLOPD).

Si, por el contrario, se trata de una TID autorizada por el Director de la AEPD cabe su suspensión, previa audiencia del exportador, si concurre alguna de las circunstancias que permiten denegar su autorización de acuerdo con el art. 70.3 del RLOPD. En este caso, el Director de la AEPD emitirá una resolución de la que quedará constancia en el Registro General de Protección de Datos y que, cuando resulte exigible, será notificada a la Comisión Europea y al resto de Estados miembros de la UE.

La suspensión se levantará cuando cesen los motivos que dieron lugar a la misma mediante resolución del Director de la AEPD que será anotada en el Registro General de Protección de Datos, comunicada al Ministerio de Justicia y notificada a la Comisión Europea y al resto de Estados de la UE (art. 144 del RLOPD).

[121] *Al suscitarse dudas sobre el nivel de protección ofrecido por el acuerdo de puerto seguro la Comisión inició en 2014 conversaciones con EEUU.*

VIII. CONCLUSIONES

En un entorno globalizado como el actual las transferencias internacionales de datos personales resultan imprescindibles no solo a nivel comunitario sino también con relación a terceros países y, en particular, cuando hablamos de Iberoamérica. Así, lo demuestra el hecho de que precisamente los países iberoamericanos sean el principal destino de las transferencias de datos personales autorizadas por la Agencia Española de Protección de Datos en el período 2000-2015. No obstante, el avance incuestionable de países como India en cuanto a receptores de transferencias internacionales de datos personales efectuadas desde España puede poner en peligro la posición preponderante en esta materia de los países iberoamericanos si no consiguen seguir siendo lo suficientemente atractivos para este tipo de transferencias.

Entendemos que representa una parte importante de este atractivo y, desde luego, una importante ventaja el hecho de que cada vez sean más los países que reúnan las condiciones necesarias para que la Comisión Europea les considere países con un nivel adecuado de protección; condición que permite realizar transferencias internacionales de protección de datos personales a aquellos sin tener que solicitar previamente autorizaciones específicas o cumplir requisitos adicionales. Actualmente, solo cuentan con esta declaración Argentina y Uruguay.

También resulta de especial interés la posible adhesión de los países iberoamericanos al Convenio n.º 108 tal y como ha hecho ya Uruguay. De este modo, aumentarán su atractivo como países destinatarios de este tipo de transferencias no solo con relación a los Estados miembros de la Unión Europea sino también respecto al resto de países que son parte del Convenio ya que establece un principio de libertad de transferencias de datos personales entre los países signatarios del mismo.

Cuando ninguna de las alternativas indicadas sea posible, los importadores de datos establecidos en aquellos países deberán ser proclives a introducir en el contrato que celebren con el exportador de datos las cláusulas contractuales tipo que permitan, de acuerdo con lo establecido por la Comisión Europea, presuponer que reúnen las garantías que resultan necesarias para obtener la oportuna autorización de la Agencia Española de Protección de Datos o bien, si se trata de transferencias de datos personales en el seno de un grupo empresarial, iniciar los trámites necesario para la adopción de reglas corporativas vinculantes.

Así mismo, resulta necesario que los países latinoamericanos, la Comisión Europea, la Agencia Española de Protección de Datos y el resto de autoridades nacionales de protección de datos trabajen conjuntamente para revisar las decisiones que actualmente existen de manera que, cuando el Reglamento europeo de protección de datos entre en vigor, pueda garantizarse su adecuación de manera automática y sin que, por tanto, deba pasarse por periodo de inseguridad jurídica equivalente al producido al declararse por parte del Tribunal de Justicia de la Unión Europea la invalidez del Acuerdo de Puerto Seguro *(Safe Harbour)* y llegar a impulsar incluso que otros países iberoamericanos suscriban acuerdos de adecuación similares.

SOBRE LA AUTORA

MARTA GRANDE SANZ es Doctora en Derecho y Licenciada en Administración de Empresas y en Derecho por la Universidad Pontificia Comillas de Madrid, Licenciada en Economía por la UNED y abogada.

Su correo electrónico es: grande_sanz_marta@yahoo.es

Este trabajo fue recibido el 13 de junio y aprobado el 7 de julio de 2016.