LAS TRANSFERENCIAS INTERNACIONALES DE DATOS: REGULACIÓN ACTUAL Y SU INCIDENCIA EN LAS RELACIONES EXTERIORES DE LA UNIÓN EUROPEA(*)

ANDONI POLO ROCA

SUMARIO: I. INTRODUCCIÓN.– II. DATOS PERSONALES Y DATOS NO PERSONALES: DISTINCIÓN NECESARIA A EFECTOS DE TRANSFERENCIA.– III. LA COMUNICACIÓN, REVELACIÓN Y CESIÓN DE DATOS PERSONALES A TERCEROS.– VI. LAS PRIMERAS REGULACIONES DE LOS «FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES», «TRANSFERENCIAS INTERNACIONALES DE DATOS» O «MOVIMIENTOS INTERNACIONALES DE DATOS».– V. LAS «TRANSFERENCIAS INTERNACIONALES DE DATOS» EN LA ACTUAL NORMATIVA SOBRE PROTECCIÓN DE DATOS: 1. El Reglamento General de Protección de Datos y la LOPDGDD. 2. Definiendo el concepto.– VI. LAS «TRANSFERENCIAS INTERNACIONALES DE DATOS» PERSONALES EN LA ACTUAL NORMATIVA SOBRE PROTECCIÓN DE DATOS: 1. Transferencias basadas en una decisión de adecuación. 2. Transferencias mediante garantías adecuadas. 3. Normas corporativas vinculantes o Binding Corporate Rules (BCRs): cobertura adicional a las transferencias de datos personales en el ámbito empresarial y el comercio internacional. 4. Excepciones del RGPD para la licitud de las transferencias internacionales. 5. Transferencias internacionales de datos personales penales: el flujo transfronterizo de datos personales del ámbito penal. 6. Las transferencias internacionales de datos respecto del Reino Unido: el flujo de datos personales UE-Reino Unido.– VII. EL PODER EXPANSIVO DEL RGPD: DE LA UE, AL MUNDO.– VIII. CONCLUSIONES.– IX. BIBLIOGRAFÍA.

RESUMEN: El Reglamento General de Protección de Datos ha supuesto dotar a la Unión Europea de una normativa uniforme en materia de protección de datos y, especialmente, en lo relativo a las transferencias internacionales de datos. Así, el RGPD ha superado el marco anterior, ha armonizado a todos los Estados miembros de la UE y ha regulado distintos instrumentos jurídicos relativos a las transferencias internacionales de datos personales. La actual regulación ha intentado aunar la libertad de circulación de datos personales con el derecho a la protección de datos: dos categorías de gran relevancia que necesitan de equilibrio. Esta regulación ha servido, además, para impulsar los flujos transfronterizos de datos personales y para expandir la aplicación del RGPD de una manera indirecta. En suma, se ha europeizado esta materia y se ha otorgado

(*) Trabajo recibido en esta REVISTA con fecha 04/03/2021 y evaluado favorablemente para su publicación el 13/09/2021.

una protección comunitaria a los movimientos internacionales de datos. A ello se le añade también la regulación de las normas corporativas vinculantes, un instrumento en lo que respecta a las transferencias de datos personales en el comercio internacional y el ámbito empresarial. En general, todo ello ha supuesto un nuevo marco que afecta directamente a las relaciones exteriores de la UE (acuerdos comerciales, cooperación internacional, etc.), y abre el camino a seguir en la futura construcción de flujos de datos personales.

Palabras clave: transferencias internacionales de datos personales; flujo transfronterizo de datos personales; movimiento internacional de datos personales; RGPD; datos personales; Unión Europea; normas corporativas vinculantes; NCV; negocios internacionales; comercio internacional; relaciones internacionales; mercado interior; espacio europeo de datos; derecho de la Unión Europea.

The international data transfers: current regulation and their impact on the external relations of the European Union

ABSTRACT: The General Data Protection Regulation has meant providing the European Union with uniform regulations on data protection and, especially, with regard to international data transfers. Thus, the RGPD has exceeded the previous framework, has harmonized all the EU Member States and has regulated different legal instruments related to international transfers of personal data. The current regulation has attempted to combine the free movement of personal data with the right to data protection: two highly relevant categories that need to be balanced. This regulation has also served to boost cross-border flows of personal data and to expand the application of the GDPR in an indirect way. In short, this matter has been Europeanized, and community protection has been granted to international data movements. To this is also added the regulation of the Binding Corporate Rules, an instrument regarding transfers of personal data in international trade and business field. In general, all of this has created a new framework that directly affects the EU's external relations (trade agreements, international cooperation, ...), and opens the way for the future construction of personal data flows.

Key words: cross-border data flows; international data transfers; international data movement; GDPR; personal data; European Union; binding corporate rules; BCRs; international business; international trade; international relations; common market; European data space; EU law.

I. INTRODUCCIÓN

La transmisión de datos es fundamental en un mundo globalizado: tanto Estados como particulares y empresas transfieren millones y millones de datos en sus actividades diarias; en especial, aquellas que operan a nivel internacional.

La protección de datos personales fue ganando relevancia durante el siglo XX, y, siendo ésta una materia de tal importancia, se puso de manifiesto la

necesidad de regular la transmisión de este tipo de datos, para garantizar, al mismo tiempo, su protección.

Las transferencias internacionales de datos personales suponen un alto riesgo para el derecho a la protección de datos (1); será necesario, por ello, controlar los flujos transfronterizos de datos personales (2).

Las nuevas tecnologías han supuesto un impulso sin precedentes para las transferencias internacionales de datos personales (3), y era necesario regular un ámbito tan relevante como éste, aunando la libre circulación de información y el derecho a la protección de datos personales. Estaremos, por tanto, ante una materia muy compleja (4), ya que deberá conciliar los siguientes elementos: la protección de datos y la intimidad, el interés público del Estado, la actividad de las empresas a nivel internacional y la libertad de información y comunicación (5).

Es por ello, que nos es preciso analizar si la actual normativa sobre protección de datos —en especial, el Reglamento General de Protección de Datos (RGPD)— ha conseguido este fin, y si se ha conseguido regular una materia tan delicada como son las transferencias internacionales, garantizando la máxima protección a la ciudadanía respecto de sus datos personales, ya que, si no, se vulneraría el derecho fundamental a la protección de datos: un derecho reconocido en el artículo 18.4 de la CE, el artículo 8 de la CDFUE y el artículo 16 del TFUE que reconoce a la ciudadanía un poder de disposición total sobre sus datos personales (6) y la oposición de que sean utilizados para fines distintos de aquel legítimo que justificó su obtención (7).

II. DATOS PERSONALES Y DATOS NO PERSONALES: DISTINCIÓN NECESARIA A EFECTOS DE TRANSFERENCIA

En primer lugar, debemos poner el acento en qué constituye un dato personal y qué no, ya que debemos diferenciar las transferencias internacionales de datos personales y las transferencias internacionales de datos no personales; ello se debe a que cada una de las dos categorías tiene su propia regulación.

La segunda categoría, las transferencias internacionales de datos no personales, es regulada en virtud del Reglamento (UE) 2018/1807, del Parlamento

(1) U. Aberasturi Gorriño (2011: 331).

(2) L. Serrano de Pablo Valdenebro (2008: 578).

(3) O. Estadella Yuste (1995: 109).

(4) A. Ortega Giménez (2016: 29).

(5) O. Estadella Yuste (1996: 195).

(6) STC 17/2013, de 31 de enero, FJ 4º, y STC 292/2000, de 30 de noviembre, FJ 6º, *in fine*.

(7) STC 96/2012, de 7 de mayo, FJ 6º.

Europeo y del Consejo, de 14 de noviembre de 2018 (8), que establece un marco de libre circulación de datos no personales en la UE. Por tanto, la clave en esta cuestión será qué constituye un dato personal, puesto que la consideración de dato personal nos lleva a la aplicación de una normativa mucho más restrictiva (y, por ello, más protectora): el RGPD.

Estaremos ante una transferencia internacional de datos personales cuando el objeto de la transferencia sea toda información sobre una persona física identificada o identificable (9). La información del dato personal debe, así, poder vincularse a una persona (10). Serán dato personal, por tanto, todos aquellos que identifican o permitan identificar a cualquier persona (11). En estos supuestos, las trasferencias deberán realizarse bajo la regulación del RGPD.

Por su parte, el Reglamento (UE) 2018/1807 ha optado por una nota negativa para definir los datos no personales: según la norma, serán todos aquellos que no sean datos personales tal como se definen en el RGPD (12). Ello conllevará la aplicación material del Reglamento (UE) 2018/1807, y no del RGPD, en las transferencias internacionales de este tipo de datos.

De este modo, la debida distinción entre dato personal y no personal nos lleva a que las transferencias internacionales se rijan por el Reglamento (UE) 2018/1807 o por la normativa sobre protección de datos.

III. LA COMUNICACIÓN, REVELACIÓN Y CESIÓN DE DATOS PERSONALES A TERCEROS

Por otro lado, no es preciso, a efectos de análisis, distinguir la transferencia internacional de datos personales de la comunicación o cesión de datos personales a terceros.

En primer lugar, no toda comunicación o revelación de datos a un tercero implica una cesión de datos a efectos legales. La (antigua) Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) definía la cesión o comunicación de datos como «toda revelación de

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

(9) Art. 4, apartado 1, del RGPD.

(10) M. Arias Pou (2016: 118); y J. L. Piñar Mañas (2010: 193 y 194).

(11) STEDH 27798/1995, de 16 de febrero de 2000, Amann contra Suiza, ap. 65; y STC 292/2000, de 30 de noviembre, FJ 6º. También SAN de 24 de enero de 2003, nº rec. 400/2001, FJ 5º.

(12) Art. 3, apartado 1), del Reglamento (UE) 2018/1807.

datos realizada a una persona distinta del interesado» (13); nos encontramos, de este modo, ante una definición bastante amplia, ya que «revelación» puede ser: entrega, difusión, consulta, transferencia, comunicación, etc. Es decir, cualquier forma que facilitara el acceso a los datos de un fichero a un tercero, distinto de la persona interesada. En este sentido, estaremos ante una cesión de datos, si el tercero que recibe los datos decide sobre el objeto y finalidad del tratamiento de dichos datos recibidos y puede aplicarlos a sus propias finalidades; pero, si este no decidiese sobre su finalidad y se limitase a realizar algunas operaciones sobre dichos datos, estaremos ante un simple acceso a dichos datos (14).

Al hablar de cesión de datos personales, nos referimos a que los datos personales salen de la inicial esfera de control de su titular, quien los había transmitido directamente a otra persona, para incorporarse a otro ámbito en el que actúa un tercer sujeto ajeno a la relación entre el titular de los datos y el primer responsable del fichero (15). Así, los datos salen del contexto en el cual han sido recogidos y registrados en el fichero, pasando a otro que puede obedecer a unos fines distintos; el dato situado dentro de un contexto y finalidad distinta permite la obtención de información del interesado distinta a aquella para la que consintió el tratamiento (16). La cesión, asimismo, precisa del consentimiento del interesado (con excepciones legales tasadas); recordemos que el consentimiento del interesado resulta la piedra angular de la protección de datos y su tratamiento (17), formando parte del contenido esencial del derecho (18).

En suma, deberemos diferenciar la revelación o comunicación, la cesión y las transferencias internacionales de datos: todas las transferencias interna-

(13) Art. 3, letra i), de la LOPD.

(14) Art. 3, letra c), de la LOPD. La LOPD recoge la cesión como tratamiento de datos (tratamiento específico con objeto y finalidad propios), pero no así la comunicación. La definición de tratamiento de datos recoge expresamente: «las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias», por lo tanto, no todas las revelaciones o comunicaciones de datos serán cesión de datos personales a efectos legales.

(15) U. Aberasturi Gorriño, I. Lasagabaster Herrarte (2011: 232).

(16) SAN 5776/2004, de 22 de septiembre, n.° rec. 888/2002, FJ 3°. «Así, al regular la cesión de datos a terceros, el legislador tiene en cuenta el riesgo potencialmente mayor de uso indebido de los datos, dado que los datos salen del contexto en el cual han sido recogidos y registrados en el fichero, pasando a otro que puede obedecer a unos fines distintos. De forma tal que el dato situado dentro de un contexto y finalidad distinta permite la obtención de información del afectado o interesado distinta a aquella para la que consintió el tratamiento. Por eso el legislador, con una finalidad preventiva, establece dos restricciones: la necesidad del previo consentimiento del afectado (con las excepciones establecidas en el Art. 11.2) y que la comunicación obedezca a fines directamente relacionados con las funciones legítimas de cedente y cesionario».

(17) P. N. Howard, S. Jones (2005: 323).

(18) M. M. Serrano Pérez (2005: 255).

cionales de datos serán una revelación, comunicación o cesión de datos (pero con el complemento internacional), pero no toda revelación, comunicación o cesión serán transferencias internacionales; asimismo, todas las cesiones serán revelaciones de datos, pero no todas las revelaciones de datos supondrán una cesión.

IV. LAS PRIMERAS REGULACIONES DE LOS «FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES», «TRANSFERENCIAS INTERNACIONALES DE DATOS» O «MOVIMIENTOS INTERNACIONALES DE DATOS»

Si bien el término «transferencia internacional de datos» debe considerarse de modo genérico aplicable a todos los flujos de datos a través de las fronteras, independientemente de cuál sea el soporte utilizado para ello o la forma de tratamiento (19), esta figura ha tenido distintas denominaciones a lo largo de las distintas regulaciones que se han ido sucediendo. Entre otros: «flujos transfronterizos de datos personales», «transferencia de datos personales a países terceros», «movimiento internacional de datos», etc. (20).

En 1980 la Organización para la Cooperación y el Desarrollo Económico (OCDE) ya se refería a lo que denominaba «flujos transfronterizos de datos personales» (*cross border flows of personal data,* en su versión inglesa) y reconocía la necesidad de que la protección de los datos de carácter personal no supusiera un obstáculo para el cumplimiento de fines económicos en sectores como el bancario o el de los seguros (21). La OCDE entendía por «flujos transfronterizos de datos personales» los desplazamientos de datos personales más allá de las fronteras nacionales, y declaró que los Estados debían evitar restringir los flujos transfronterizos de datos personales entre ellos y elaborar leyes, políticas y prácticas en nombre de la protección de la privacidad y las libertades individuales que pudieran crear obstáculos a los flujos transfronterizos de datos personales que se excedieran en requisitos para esa protección (22).

A nivel internacional, una de las primeras normas específicas en la materia de protección de datos fue el Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos

(19) A. Ortega Giménez (2016: 41).

(20) *Cfr.* J. Piñol i Rull, O. Estadella Yuste (1993: 78 y 79); E. Suñé Llinás (1999: 267 a 269); M. Á. Davara Rodríguez (2006: 23 y 24); y D. Sancho Villa (2010: 23).

(21) Recomendación del Consejo (de la OCDE), de 23 de septiembre de 1980, relativa a las Directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales.

(22) *Ibídem*.

de carácter personal (23) («Convenio n.º 108»), sustituido en la actualidad por el «Convenio n.º 108+» del año 2018 (24). Este convenio estableció los fundamentos de la protección de datos a nivel internacional (25).

El Convenio de 1981 tenía como objeto conjugar la protección de datos y la libre circulación transfronteriza de los datos (26), ya que este último tenía un gran valor económico para los Estados y traía muchas inversiones (27).

Además de armonizar la legislación interna de los Estados parte, esta norma internacional supuso un primer paso para construir una vertebración legislativa en materia de protección de datos (28). Lo que el Convenio trató como «circulación a través de las fronteras de los datos de carácter personal» (29) fue denominado como «flujos transfronterizos de datos» y regulado en el Capítulo III (30) de la norma.

En España, el legislador quiso elaborar una norma interna en materia de protección de datos siguiendo los criterios del Convenio n. 108 y aprobó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). En dicha ley se partía de los fundamentos del Convenio, especialmente del Capítulo III (31), y se reconocía que era necesario conciliar la «protección de la integridad de la información personal» con el libre «flujo transfronterizo de datos», que constituía «una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra» (32). Así, la LORTAD denominó a este fenómeno como «movimiento internacional de datos» y lo recogió en su Título V (33); todo ello partiendo de

(23) Convenio n.º 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España el 27 de enero de 1984.

(24) Nombre completo: Convenio n.º 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, modificado por el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 108), adoptado por el Comité de Ministros en su Sesión n.º 128ª el 18 de mayo de 2018. Accesible en: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

(25) C. J. Bennett, C. D. RAAB (2006: 85 y ss).

(26) G. Buquicchio (1986: 99).

(27) A. Madec (1984: 84).

(28) H. Campuzano Tomé (2002: 79).

(29) Preámbulo del Convenio n.º 108.

(30) Art. 12 del Convenio n.º 108.

(31) Art. 12 del Convenio n.º 108.

(32) Exposición de motivos n.º 4 de la LORTAD.

(33) Art. 32 y 33 de la LORTAD.

una norma general básica: no podían realizarse transferencias temporales ni definitivas de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable al que presta la LORTAD (34).

La UE, siguiendo el camino marcado por el Convenio, elaboró 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, la norma con la que se le dio inicio a la normativa comunitaria sobre protección de datos (35).

Esta norma europea quiso armonizar y unir la protección de los derechos fundamentales de las personas en materia de datos personales y la libre circulación de datos personales de un Estado miembro a otro (36), resultando esto necesario para la libre circulación de mercancías, personas, servicios y capitales.

Además, la Directiva 95/46/CE completó el Convenio n.º 108 de 1981, y tuvo como uno de sus fines la creación de un «espacio europeo de la información» (37) (es decir, de datos).

La norma europea reguló en su Capítulo IV la «transferencia de datos personales a países terceros» (38), estableciendo con carácter general que la transferencia a un país tercero de datos personales únicamente podía efectuarse cuando el país tercero de que se trate garantice un nivel de protección adecuado (39).

Por su parte, España aprobó en el año 1999 la LOPD que traspuso la Directiva 95/46/CE y actualizó la LORTAD. En dicha norma, se mantuvo la denominación de la LORTAD («movimiento internacional de datos»), no la de la Directiva («transferencia de datos personales a países terceros»), ni del Convenio («flujos transfronterizos de datos»), y ello se reguló en su Título V (40). La regulación de la LOPD en este sentido fue bastante parecida a la de la LORTAD [no podían realizarse transferencias temporales ni definitivas con destino a países que no proporcionen un nivel de protección equiparable a la ley española (41)], con algunas modificaciones y algunas excepciones más que las que tenía la norma de 1992.

---

(34) Art. 32 de la LORTAD.

(35) C. J. Bennett, C. D. RAAB (2006: 93 y ss).

(36) Considerando n.º 3º y art. 1 de la Directiva 95/46/CE.

(37) C. Conde Ortiz (2005: 55).

(38) Art. 25 y 26 de la Directiva 95/46/CE.

(39) Art. 25.1 de la Directiva 95/46/CE.

(40) Art. 33 y 34 de la LOPD.

(41) Art. 33.1 de la LOPD.

V. LAS «TRANSFERENCIAS INTERNACIONALES DE DATOS» EN LA ACTUAL NORMATIVA SOBRE PROTECCIÓN DE DATOS

1. El Reglamento General de Protección de Datos y la LOPDGDD

El Reglamento General de Protección de Datos (42) (RGPD), aprobado por la UE en 2016 y efectivamente aplicable desde el año 2018 (43), supuso dotar a la UE de una norma básica fundamental en materia de protección de datos.

La importancia de esta norma se basa esencialmente en su carácter de reglamento, de alcance general obligatorio en todos sus elementos (44), a diferencia de la anterior norma europea que tenía carácter de directiva, lo que suponía una descompensación en la normativa de los Estados miembros (45), consiguiéndose actualmente el buscado intento de lograr una uniformidad legislativa a nivel comunitario (46); y, también, en su expansión en lo relativo a la aplicación, conceptos, contenido, etc.

En lo que respecta a las transferencias internacionales de datos, la norma comunitaria ha denominado a este fenómeno «transferencias de datos personales a terceros países u organizaciones internacionales» y lo ha regulado en su Capítulo V con bastante contenido normativo (47).

Por su parte, a nivel legislativo español, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) lo ha denominado «transferencias internacionales de datos», regulándolo en su Título VI (48), aunque la ley se limita a completar lo no regulado por el RGPD, ya que éste es directamente aplicable; en especial, en aquellos apartados no regulados por el RGPD o en los que el reglamento ha permitido a los Estados miembros cierta flexibilidad normativa.

---

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

(43) El RGPD entró en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea; no obstante, comenzó a ser aplicable a partir del 25 de mayo de 2018. Véase: art. 99 del RGPD.

(44) Art. 288 del TFUE.

(45) A. Rallo Lombarte (2012: 37 y ss.). En palabras del propio autor: «la Directiva se tradujo en una pavorosa asimetría europea sobre la que, sin duda, se ha construido una *doble velocidad europea* en el ritmo de garantía efectiva del derecho a la protección de datos personales» (cursiva del autor).

(46) *Vid.* P. Solar Calvo (2012).

(47) Art. 44, 45, 46, 47, 48, 49 y 50 del RGPD.

(48) Art. 40, 41, 42 y 43 de la LOPDGDD.

Comienza el Reglamento pronunciándose sobre que en la presente transformación tecnológica que vivimos, se «ha de facilitar aún más la libre circulación de datos personales 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» (49) y, de igual modo, para garantizar dicha protección y «evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia»; todo ello teniendo en cuenta que «el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales» (50).

Podemos ver, por tanto, que es voluntad de la norma comunitaria conjugar la protección de datos y la libre circulación de los datos dentro de la Unión y fuera.

Deducimos por todo ello que el RGPD ha querido seguir uno de los objetivos clave que ya se marcó la Directiva 95/46/CE y que hemos mencionado anteriormente: la creación de un «espacio europeo de la información» (51) (o «espacio europeo de datos»).

2. Definiendo el concepto

El Reglamento de la LORTAD de 1994 (52) (RLORTAD) definió la transferencia de datos como «el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional» (53); pero, sin duda, fue la Agencia Española de Protección de Datos (AEPD) quien proporcionó una definición más completa, en una instrucción del año 2000 donde dio una definición a la transferencia internacional de datos y la consideró «toda transmisión de los mismos fuera del territorio español» y, en particular, «las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero» (54).

(49) Considerando n.º 6º del RGPD.

(50) Considerando n.º 13º del RGPD.

(51) C. Conde Ortiz (2005: 55).

(52) Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

(53) Art. 1.6 del RLORTAD.

(54) Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos. Publicada en: «BOE» núm. 301, de 16 de diciembre de 2000.

La Directiva 95/46/CE y la LOPD de 1999, por otro lado, no ofrecieron una definición, pero sí, en cambio, el Reglamento de la LOPD de 2007 (55) (RLOPD). El reglamento entendía por transferencia internacional de datos todo «tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, 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» (56).

De este modo, para el RLOPD de 2007, serán transferencia internacional las que supongan una transmisión fuera del Espacio Económico Europeo (EEE), pero no las que lo supongan fuera de los países que sean miembro del EEE entre ellos (57); el RLOPD dio, así, un paso más allá del Convenio n.º 108 y de la Directiva 95/46/CE (58), incluso de la propia LOPD que desarrollaba (59). Se aseguraba así una mayor libertad en las transferencias de datos en el EEE (60).

El actual RGPD no ha sido claro sobre qué es una transferencia internacional de datos personales a efectos del reglamento y no ha ofrecido una definición de esta (61); tampoco lo han hecho ni la LOPDGDD, ni el Convenio 108+ de 2018.

El Consejo de Europa, en cambio, sí ha definido la transferencia internacional en su informe explicativo del Convenio 108+, y ha declarado que habrá transferencia internacional (62) de datos personales «cuando los datos personales se divulgan o se ponen a disposición de un destinatario sujeto a la jurisdicción de otro Estado u organización internacional» (63). El intercambio

(55) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

(56) Art. 5.1 letra s) del RLOPD.

(57) J. M. Fatás Monforte, J. García Sanz (2008: 140).

(58) U. Aberasturi Gorriño (2011: 334).

(59) La LOPD en su artículo 34 letra *k)* sí las consideraba transferencias internacionales de datos, si bien les daba un carácter especial o privilegiado.

(60) L. Serrano de Pablo Valdenebro (2008: 578); y, también, STS 5484/2006, de 25 de septiembre, rec. n.º 3223/2002, FFJJ 4º y 5º.

(61) M. Tudorica, T. Mulder (2019: 194).

(62) En realidad, tanto el Convenio 108+ como el Consejo de Europa en su informe lo denominan «transferencia transfronteriza de datos» (*«transborder data transfer»),* pero nos es conveniente denominarlo transferencia internacional, ya que, como luego veremos, a efectos del RGPD se diferencian los dos conceptos.

(63) Consejo de Europa, *Council of Europe Treaty Series*, n.º 223. Informe explicativo del Protocolo que modifica el Convenio para la protección de las personas con respecto al procesamiento automático de datos personales, p. 17, ap. 102. «*A transborder data transfer occurs when personal data is disclosed or made available to a recipient subject to the jurisdiction of another State or international organisation*». Accesible en: https://rm.coe.int/16808ac91a.

de datos personales, por su parte, lo ha definido como una «comunicación de información a un destinatario claramente identificado por un transmisor conocido» (64). De esto se deduce que: la transferencia internacional de datos no tiene una definición legal; sí, en cambio, un significado natural marcado por la práctica; la transferencia se realiza por cualquier medio; y los datos se ponen a disposición de un destinatario (65).

Debemos tener en presente, además, lo establecido por el TJUE en el caso Lindqvist de 2003 (66) que interpretó la Directiva 95/46/CE. El tribunal declaró que publicar datos personales en una *web* en la que se puede acceder desde cualquier lugar no suponía una transferencia internacional de datos personales, ni siquiera aun siendo accesibles desde países terceros (67), si bien sí un tratamiento de datos, y argumentó que no había «una transferencia directa entre estas dos personas» (68). Por lo que podemos intuir que a en una transferencia internacional de datos necesitamos: una transferencia de datos entre dos sujetos, un exportador de datos y un importador de los mismos.

El vigente RGPD ha diferenciado las «transferencias de datos transfronterizas» (*cross-border data transfers)* y las «transferencias de datos personales a terceros países u organizaciones internacionales», que serán las «transferencias internacionales de datos» *(international data transfers)*.

Según el Reglamento, las «transferencias de datos transfronterizas» son: transferencias de datos personales desde y hacia diferentes establecimientos de un responsable o un encargado del tratamiento, establecido en más de un Estado miembro de la UE, o transferencias de datos personales de interesados de más de un Estado miembro de la UE al establecimiento de un responsable o un encargado del tratamiento con sede en un único Estado miembro de la UE (69).

---

(64) Consejo de Europa, Informe introductorio para la actualización de la recomendación n.° R (97) 5 del Consejo de Europa sobre la protección de datos médicos, de 15 de junio de 2015, p. 5. Accesible en: https://rm.coe.int/introductory-report-for-updating-recommendation-r-97-5-of-the-council-/168073510c.

(65) M. Tudorica, T. Mulder (2019: 195).

(66) STJUE (Gran Sala), de 6 de noviembre de 2003, asunto C-101/01, Göta hovrät (Suecia) c. Lindqvist.

(67) M. Pulido Quecedo (2003: 15).

(68) STJUE (Gran Sala), de 6 de noviembre de 2003, asunto C-101/01, Göta hovrät (Suecia) c. Lindqvist, ap. 61.

(69) Todo ello lo deducimos del art. 3 (ámbito territorial de aplicación del RGPD) y del art. 4, apartado 23°, del RGPD que define el «tratamiento transfronterizo» como: «a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único

Actualmente, por lo tanto, se diferencian, a efectos del RGPD, tres casos en la comunicación de datos: el primero, dentro de la Unión, en lo que respecta a los datos personales entre Estados miembros (mercado interior), rige la libre circulación de dichos datos (excepto la libre circulación de datos personales relacionada con actividades excluidas del ámbito del Derecho de la Unión (70)); el segundo, serán las «transferencias de datos transfronterizas»; y, el tercer y último caso, serán las «transferencias internacionales de datos».

En esta regulación, asimismo, nos es necesario tener en cuenta que dentro de la UE rigen las normas sobre Espacio Schengen, libre circulación (sin restricciones de personas, bienes, servicios y capital) y mercado interior, por lo que, los movimientos de datos entre Estados miembro no serán transferencias internacionales *stricto sensu,* ni tampoco las realizadas en el EEE (como luego analizaremos); tampoco lo serán las «transferencias de datos transfronterizas» *(cross-border data transfers)*.

Así, para hablar de transferencia internacional de datos personales, debe haber un traslado de datos personales de un lugar del EEE a cualquier otro país u organización internacional, es decir, el lugar de destino debe encontrarse en un territorio externo al EEE (71).

Por tanto, parece que, basándonos a efectos teóricos en la definición que recogió el RLOPD (72), podemos definir la transferencia internacional como «una transmisión de datos personales fuera del territorio del EEE, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable».

Por último, como hemos señalado al principio, el dato objeto de la transferencia deberá ser personal; si no, dejaríamos de estar en el ámbito del RGPD y regiría el Reglamento (UE) 2018/1807.

VI. LAS «TRANSFERENCIAS INTERNACIONALES DE DATOS» PERSONALES EN LA ACTUAL NORMATIVA SOBRE PROTECCIÓN DE DATOS

Como hemos mencionado, el RGPD ha regulado las «transferencias de datos personales a terceros países u organizaciones internacionales» (transferencias internacionales de datos) en su Capítulo V, diferenciándolas de las

establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro».

(70) Considerando n.° 16° del RGPD.

(71) A. Ortega Giménez (2016: 41); y A. Ortega Giménez (2015: 23 y ss.).

(72) Art. 5.1 letra s) del RLOPD.

«transferencias de datos transfronterizas», y ha establecido el siguiente régimen sobre las transferencias internacionales de datos:

1. Transferencias basadas en una decisión de adecuación (art. 45).
2. Transferencias mediante garantías adecuadas (art. 46).
3. Normas corporativas vinculantes o *Binding Corporate Rules* (art. 47).
4. Normas finales para la licitud de las transferencias internacionales (art. 49).

1. Transferencias basadas en una decisión de adecuación

Señalaba la LOPD de 1999 que las transferencias a países que no proporcionen un nivel de protección equiparable a la ley española (LOPD) requerían autorización previa del Director de la AEPD, que solamente podía otorgarla si se obtienen garantías adecuadas (73); por lo que, *a sensu contrario,* podían realizarse transferencias a los países que presentaran un nivel de protección equiparable a la ley española, con total libertad, sin necesidad de autorización específica de la AEPD (74); «protección equiparable» significa semejante, «equivalente», pero no idéntico (75).

Según la Directiva 95/46/CE, además, Comisión Europea podía hacer constar que un país tercero garantiza un nivel de protección adecuado (76); así, la categoría «nivel de protección adecuado» hacía referencia al nivel de la protección, no a la protección como tal (77), siendo este concepto más débil y abierto, así como menos restrictivo, que el de «protección equivalente» (78).

Actualmente, rige un sistema parecido, pero al ser la protección de datos una materia europeizada en su gran parte. Serán los organismos comunitarios los que realizarán dichos controles; ya no será «hacer constar», sino que serán las instituciones europeas quienes decidan y controlen.

De este modo, el RGPD ha establecido que para realizar transferencias de datos personales a un tercer país u organización internacional, será necesario una decisión de la Comisión Europea que establezca que dicho tercer país u organización internacional garantizan un nivel de protección adecuado (79).

---

(73) Art. 33.1 de la LOPD.

(74) U. Aberasturi Gorriño (2011: 338); y F. Coudert (2005).

(75) E. Ull Pont (2000: 148 y ss.); y J. Aparicio Salom (2000: 189).

(76) Art. 25.6 de la Directiva 95/46/CE.

(77) E. García-Cuevas Roque (2012: 178).

(78) M. Heredero Higueras (1997: 187); y J. Verdaguer López, M. A. Bergas Jané (2012: 361).

(79) Art. 45.1 del RGPD.

Es necesario, por tanto, una decisión de adecuación de la Comisión y, una vez dictada la decisión, las transferencias al tercer país u organización internacional recogidos en la decisión no requerirán ninguna autorización específica, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas (80). Las decisiones de adecuación son, en suma, el principal instrumento legislativo de la UE para permitir una mayor libertad de flujo transfronterizo de datos (81). Crear un flujo de datos personales entre dos o más países supone, así, que la información deberá circular tan libremente como en el interior de cada uno de los territorios respectivos, todo ello cuando se le reconozca al otro país un nivel de protección adecuado (82).

La Comisión establecerá su criterio de adecuación mediante un acto de ejecución (83), al tratarse de un ámbito en los que se requieran condiciones uniformes de aplicación; por tanto, como acto jurídico vinculante de la UE, tiene eficacia directa en los Estados. El efecto principal de una decisión de adecuación es hacer que la transferencia realizada a ese tercer país u organización internacional sea equivalente a la que se realiza entre países del EEE (84); es decir, reconocer a través de este instrumento una «protección adecuada» en un tercer país significa que dicha protección es «sustancialmente equivalente» a la dada en la UE (85).

Debemos, sin embargo, matizar el carácter de la decisión: parece que mediante la decisión la Comisión confiere a dicho tercer estado u organización internacional generalidad y «confianza» al garantizarlo como seguro, pero no es así: debemos tomarlo como una *presunción de garantía* según el TJUE, ya que dicha decisión será impugnable ante el tribunal si se constatase que el tercer país u organización internacional no garantiza un nivel de seguridad suficiente (86) (que es lo que sucedió con el caso *Schrems I* de 2016).

La Comisión, por su parte, además, también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional (87).

En lo que respecta a los países contratantes del Convenio 108+, debemos señalar un apunte: el convenio ha recogido la norma general de libre movi-

(80) Considerando n.º 103 del RGPD.

(81) J. J. Gonzalo Doménech (2019: 371).

(82) S. Ripoll Carulla (1994).

(83) Art. 291 del TFUE.

(84) J. J. Gonzalo Doménech (2019: 355).

(85) A. I. Mendoza Losana (2015: 217).

(86) STJUE (Gran Sala), de 6 de octubre de 2015, asunto C-362/14, Maximillian Schrems v. Data Protection Commissioner, ap. 73, 74 y 96.

(87) Considerando n.º 103 del RGPD.

miento de datos entre los países contratantes; sin embargo, un Estado de la UE no podrá enviar datos libremente a un Estado contratante del Convenio y no miembro de la UE. Para ello, el tercero Estado (contratante y no miembro) deberá cumplir la normativa europea en materia de protección de datos, lo que tiene como fin que la protección del movimiento internacional de datos de los habitantes de la Unión quede bajo la normativa comunitaria, dando mayor garantías a dichas transferencias (88). Los países que hayan ratificado los Convenios 108 y 108+, por tanto, estarán en una situación especial (89).

A la hora de evaluar la adecuación del nivel de protección, los elementos que la Comisión Europea deberá tener en cuenta para determinar si un tercer país u organización internacional garantiza un nivel de protección adecuado se basará en tres pilares (90): a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación (en general), el acceso de las autoridades públicas a los datos personales (normas, medidas de seguridad, etc.), normas sobre transferencias internacionales, jurisprudencia y el reconocimiento a los interesados de derechos efectivos y exigibles y de recursos y acciones efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en materia de protección de datos (funciones, poderes, controles, etc.), y c) los compromisos internacionales asumidos u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes o su participación en sistemas multilaterales o regionales, especialmente en materia de protección de datos. El RGPD, por último, no ha recogido el procedimiento para instar una decisión de adecuación (91).

Teniendo en cuenta, por otro lado, que el concepto de adecuado que exige el reglamento es bastante ambiguo (92), el Grupo de Trabajo del Artículo 29 (GT 29) —en la actualidad, Comité Europeo de Protección de Datos (CEPD) (93)— dio

(88) European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxemburgo, Publications Office of the European Union, 2018, p. 52. Accesible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.

(89) V. Guasch Portas (2012: 428 y ss.); y C. Álvarez Rigaudias (2010).

(90) Art. 45.2 del RGPD.

(91) *Vid.* J. L. Piñar Mañas (2016: 441).

(92) A. Cerda Silva (2011: 335).

(93) El Grupo de Trabajo sobre Protección de Datos del Artículo 29 (GT 29) fue creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, en su artículo 29 (de ahí el nombre). Sin embargo, el RGPD (art. 68-76) ha creado el Comité Europeo de Protección de Datos (CEPD), un organismo europeo independiente que ha venido a sustituir al GT 29 y en el que también se ha incluido el Supervisor Europeo de Protección de Datos (SEPD).

algunos criterios a tener en cuenta a la hora de hacer este análisis en 1998 (94) y los actualizó en el año 2018 (95).

Tal como declara el GT 29, el documento de trabajo de 2018 tiene como finalidad proporcionar orientación a la Comisión Europea a la hora de evaluar el nivel de protección de datos en terceros países y organizaciones internacionales, pero, además, según el propio GT 29, el documento quiere servir también de orientación básica para aquellos terceros países y organizaciones internacionales interesadas en obtener la adecuación (96).

Así, se debe hacer un primer análisis del tercer país y organización internacional en su conjunto (Estado de Derecho, derechos humanos, legislación general, etc.) y, después, analizar la estructura general en materia de protección de datos (legislación, medidas, organismos de control, etc.); en especial, si se respetan los principios fundamentales de la protección de datos (derechos del interesado, licitud del tratamiento, etc.). La adecuación se debe lograr a través de la combinación de derechos para los interesados y las obligaciones de quienes procesan datos, o quienes ejercen control sobre dicho procesamiento y supervisión por parte de organismos independientes; las reglas de protección de datos solo son efectivas si son exigibles y se siguen en la práctica: es necesario considerar no solo el contenido de las normas aplicables a los datos personales transferidos, sino también el sistema establecido para garantizar la efectividad de tales reglas, ya que los mecanismos de aplicación eficientes son de suma importancia para la efectividad de reglas de protección de datos (97).

En lo que respecta a los terceros países u organizaciones internacionales que necesitan de una decisión de la Comisión Europea que establezca que estos garantizan un nivel de protección adecuado, debemos hacer unas matizaciones. La primera será que entre los Estados miembros de la UE habrá libertad de movimiento de dichos datos personales, ya que todos ellos están

---

(94) GT 29. Documento de trabajo n.° 12 sobre la transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, del Grupo de Trabajo del Artículo 29, de 24 de julio de 1998.

(95) GT 29. Documento de trabajo n.° 254 rev. 01 sobre la Referencia de Adecuación, del Grupo de Trabajo del Artículo 29, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018.

(96) GT 29. Documento de trabajo n.° 254 rev. 01 sobre la Referencia de Adecuación, del Grupo de Trabajo del Artículo 29, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018, p. 2: «*This document aims to provide guidance to the European Commission and the WP29 under the GDPR for the assessment of the level of data protection in third countries and international organizations [...]. In addition, it may guide third countries and international organizations interested in obtaining adequacy*».

(97) GT 29. Documento de trabajo n.° 254 rev. 01 sobre la Referencia de Adecuación, del Grupo de Trabajo del Artículo 29, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018, p. 3.

bajo la aplicación común, igual e armonizada del RGPD, creando un flujo europeo de datos personales (libre circulación). Ya con la Directiva 95/46/CE, en medida en que los Estados miembros estaban obligados a incorporar la directiva a sus ordenamientos, podía deducirse que no se requería de autorización previa entre estos (98).

Por tanto, teniendo en cuenta el carácter obligatorio y general de un reglamento como el RGPD y el hecho de haberse armonizado, uniformizado e igualado toda la normativa todos los Estados miembros, las transferencias entre estados miembros no serán transferencias internacionales, sino que habrá libertad de circulación de dichos datos: la UE será como una unidad, como si fuese un solo Estado a efectos de circulación de datos personales. Recordemos, además, que según el TJUE, la difusión de datos personales en una página *web* realizada por un interesado ubicado en un Estado miembro no se considerará una transferencia internacional (99).

La segunda cuestión, por otro lado, será en lo que respecta al EEE: en el año 2018, el RGPD se incorporó al Acuerdo EEE (100), por lo tanto, el RGPD se aplica a todo el EEE, que incluye todos los países de la UE, más Islandia, Liechtenstein y Noruega.

No obstante lo anterior, algunos autores defienden que los países del EEE deben ser considerados «países terceros», ya que el RGPD no les excluye en ningún momento de tal consideración (101) —no, en cambio, los Estados miembros de la UE—; así, definen las transferencias internacionales de datos personales como «un tratamiento de datos en el que hay implicado, al menos, un Estado miembro de la UE y un país tercero (de fuera de la UE) o una organización internacional» (102). Recordemos que no lo entendía así el RLOPD de 2007 en su definición jurídica (103).

La creación del EEE permitió a los países de la Asociación Europea de Libre Cambio (AELC) participar en el mercado interior de la UE, sin tener que adherirse directamente a la UE; ello significa que en todos los acuerdos que sean parte los países del AELC serán considerados como otro Estado parte a efectos del mercado interior (104), suponiendo, así, un acuerdo de asociación de carácter multilateral que crea un sistema institucional complejo y de naturaleza peculiar (105).

---

(98) U. Aberasturi Gorriño (2011: 342).

(99) STJUE (Gran Sala), de 6 de noviembre de 2003, asunto C-101/01, asunto Göta hovrät (Suecia) c. Lindqvist.

(100) Art. 217 del TFUE.

(101) J. L. Piñar Mañas (2017: 2063).

(102) *Ibíd.*

(103) Art. 5.1 letra s) del RLOPD.

(104) N. Stoffel Vallotton (2003: 585 y ss.).

(105) *Ibíd.*

Por ello, no es posible considerarlos como «países terceros», ya que la definición jurídica de transferencia internacional de datos parte de la misma EEE (no de la UE), y, por otro lado, ya que la esencia misma del EEE es participar en ese mercado interior de la UE, por lo que el hecho de que el RGPD haya sido incluido al EEE supone que los países del EEE entran al mencionado «espacio europeo de la información» que el reglamento ha querido construir; no podemos, por lo tanto, calificarlas de transferencia internacional, ya que, si fuese ese el caso, sería necesario alguno de los instrumentos del RGPD (una decisión de adecuación, garantías adecuadas, etc.) y no es el caso: se ha incluido el RGPD al EEE (106).

En las transferencias basadas en una decisión de adecuación, por otro lado, se incluyen actualmente todos aquellos países y organizaciones que la Comisión entendió que mantenían un adecuado nivel de protección (107); si bien todas estas decisiones son anteriores a 2016, las decisiones adoptadas por la Comisión en virtud de la Directiva 95/46/CE (108) permanecerán en vigor en la categoría de transferencias basadas en una decisión de adecuación, hasta que sean modificadas, sustituidas o derogadas por una posterior Decisión de la Comisión (109). De este modo, la Comisión ha entendido que mantienen un adecuado nivel de protección: Andorra (110), Argentina (111), Canadá (112), Guernesey (113), Isla de Man (114), Islas

(106) Podemos decir que se ha creado, de este modo, una especie de mercado interior en lo que respecta a los datos personales, por medio del RGPD que será aplicable en todo el EEE; respondiendo, además, los países del EEE por los incumplimientos del RGPD que realicen.

(107) Art. 45.9 del RGPD.

(108) Art. 25.6 de la Directiva 95/46/CE.

(109) Art. 45.9 del RGPD.

(110) Decisión 2010/625/UE, de la Comisión, de 19 de octubre de 2010, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra. OJ L 277, 21.10.2010.

(111) 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 del Consejo sobre la adecuación de la protección de los datos personales en Argentina. OJ L 168, 5.7.2003.

(112) Decisión 2002/2/CE, de la Comisión, de 20 de diciembre de 2001, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act. OJ L 2, 4.1.2002.

(113) Decisión 2003/821/CE, de la Comisión, de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernsey. OJ L 308, 25.11.2003.

(114) Decisión 2004/411/CE, de la Comisión, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man. OJ L 151, 30.4.2004.

Feroe (115), Israel (116), Jersey (117), Nueva Zelanda (118), Suiza (119) y Uruguay (120).

Cabe señalar que aunque la decisión de la Comisión sobre Nueva Zelanda y Uruguay fuese más tardía que las demás, anteriormente el GT 29 ya les había dado su aprobación (121); además, algunos de estos actos de ejecución no se aplican a todos los tratamientos de datos personales: es el caso de Canadá (122).

En lo que respecta a Hungría, es cierto que le fue reconocido un adecuado nivel de protección por parte de la Comisión con su respectiva Decisión (123); sin embargo, Hungría es actualmente Estado miembro de la UE y, por ello, ya no lo podemos considerar «país tercero», sino Estado miembro.

---

(115) Decisión 2010/146/UE, de la Comisión, de 5 de marzo de 2010, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales. OJ L 58, 9.3.2010.

(116) Decisión 2011/61/UE, de la Comisión, de 31 de enero de 2011, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales. OJ L 27, 1.2.2011.

(117) Decisión 2008/393/CE, de la Comisión, de 8 de mayo de 2008, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey. OJ L 138, 28.5.2008.

(118) Decisión de Ejecución 2013/65/UE, de la Comisión, de 19 de diciembre de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda. OJ L 28, 30.1.2013.

(119) Decisión 2000/518/CE, de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza. OJ L 215, 25.8.2000.

(120) Decisión de Ejecución 2012/484/UE, de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales. OJ L 227, 23.8.2012.

(121) *Cfr.* GT 29. Dictamen 6/2010, del Grupo de Trabajo del Artículo 29, de 12 de octubre de 2010; Dictamen 11/2011, del Grupo de Trabajo del Artículo 29, de 4 de abril de 2011.

(122) Respecto de Canadá debemos matizar que, según la Decisión 2002/2/CE, de la Comisión, de 20 de diciembre de 2001, tiene reconocido el nivel adecuado de protección por la Comisión Europea respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

(123) Decisión 2000/519/CE, de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Hungría. OJ L 215, 25.8.2000.

Asimismo, en cuanto a EEUU, este ámbito ha sido bastante controvertido. Hasta 2015, se les reconocía un adecuado nivel de protección a aquellas entidades que respetasen los principios de «Puerto Seguro» *(Safe Harbor)* (124); no obstante, ello fue anulado por el TJUE en el caso *Maximillian Schrems v. Data Protection Commissioner de 2016* (125).

Ante esa situación, ello fue sustituido por el «Escudo de Privacidad UE-EEUU» (*EU-US Privacy Shield),* aprobado en el año 2016 por la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016 (126): los que respetaran los principios de dicha Decisión se les reconocía un nivel adecuado de protección. El TJUE, en cambio, volvió a anularlo y declaró inválido el Escudo de Privacidad en el caso *Data Protection Commissioner v. Facebook Ireland Limited y Maximillian Schrems* (caso Schrems II) de 2020 (127) —escudo que dejó de ser un mecanismo aplicable, de manera inmediata desde la publicación de la sentencia—.

Sin abordar un análisis profundo de esta cuestión, una de las consideraciones más relevantes sobre la sentencia del caso *Schrems II* es la de que, según el Tribunal, tanto el Escudo como cualquier Decisión se deberá siempre interpretar (y adaptarse) a la luz de las disposiciones del RGPD y de la Carta de Derechos Fundamentales de la UE (128).

De igual modo lo declaró el Supervisor Europeo de Protección de Datos (SEPD) en su estrategia para que las instituciones de la UE cumplan con la sentencia *Schrems II* de 2020, al afirmar que las transferencias de datos personales a terceros países deben cumplir con la Carta de los Derechos Fundamentales de la UE, así como con la legislación de protección de datos de la UE aplicable, en la que también declaró que la UE debía evitar transferencias internacionales a EEUU (129).

---

(124) L. A. Bygrave (2010: 41).

(125) STJUE (Gran Sala), de 6 de octubre de 2015, asunto C-362/14, Maximillian Schrems v. Data Protection Commissioner.

(126) Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. OJ L 207, 1.8.2016.

(127) STJUE (Gran Sala), de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner v. Facebook Ireland Limited y Maximillian Schrems.

(128) STJUE (Gran Sala), de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner v. Facebook Ireland Limited y Maximillian Schrems, ap. 140 y ss.

(129) Supervisor Europeo de Protección de Datos (SEPD). Estrategia para que las instituciones de la UE cumplan con la sentencia «Schrems II», de 29 de octubre de 2020. Accesible en: https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en.

Con la regulación actual que requiere una decisión de adecuación, la primera Decisión fue la relativa a Japón (130) en 2019, que creó la mayor área mundial de flujo transfronterizo de datos personales seguro.

Por lo tanto, en esta categoría de transferencias tendremos a Islandia, Liechtenstein y Noruega (miembros del EEE) y a Andorra, Argentina, Canadá, Guernesey, Isla de Man, Islas Feroe, Israel, Japón, Jersey, Nueva Zelanda, Suiza y Uruguay (EEUU ya no). También debemos incluir en la lista a Reino Unido, desde el año 2021, pero con cietros matices, como se analizará más adelante.

Por último, cabe mencionar que, en el año 2021, la Comisión Europea inició el proceso para la adopción de una decisión de adecuación respecto a Corea del Sur-República de Corea.

2. Transferencias mediante garantías adecuadas

En esta categoría de transferencias nos encontramos ante una situación en la que la Comisión no ha emitido una decisión de adecuación, pero en la que el responsable o el encargado del tratamiento podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas (131). Es decir, en este caso, se podrán efectuar transferencias a un tercer país u organización internacional que no tenga el visto bueno de la Comisión si se cumplen una serie de garantías tasadas recogidas por el RGPD, sin que sea necesaria una autorización expresa de una autoridad de protección de datos para ello (autorización de la AEPD, en el caso de España).

Esta disposición supone una especie de norma supletoria para todos aquellos casos en los que no haya un acto de ejecución de la Comisión que determine si un tercer país u organización internacional garantiza un nivel de protección adecuado; sin embargo, la LOPDGDD ha establecido que podrán hacerse transferencias internacionales de datos personales a países u organizaciones internacionales que no cuenten con decisión de adecuación de la Comisión, previa autorización de la AEPD o, en su caso, de autoridades autonómicas de protección de datos (132). Teniendo en cuenta el principio de primacía del Derecho de la Unión y que un reglamento es un acto jurídico de

(130) Decisión de Ejecución (UE) 2019/419, de la Comisión, de 23 de enero de 2019, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal. OJ L 76, 19.3.2019.

(131) Art. 46.1 del RGPD.

(132) Art. 42.1 de la LOPDGDD.

alcance general obligatorio en todos sus elementos y directamente aplicable en todos los Estados miembros (133), el orden de prelación de estas normas sería el siguiente: 1) decisión de la Comisión sobre la protección adecuada, 2) a falta de dicha decisión, que haya garantías adecuadas y que los interesados cuenten con derechos exigibles y acciones legales efectivas, y 3) a falta de la anterior, previa autorización de la AEPD o, en su caso, de autoridades autonómicas de protección de datos.

Entre las garantías adecuadas tasadas que recoge el reglamento para permitir las transferencias sin decisión de la Comisión ni autorización de la autoridad de control competente encontramos las siguientes: un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos, normas corporativas vinculantes o *Binding Corporate Rules,* cláusulas tipo de protección de datos adoptadas por la Comisión, cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión, un código de conducta o un mecanismo de certificación (134).

En cambio, sí será necesaria la autorización de la autoridad de control competente, si bien no decisión de la Comisión, en los casos en los que estemos ante cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o de disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados (135).

Al hablar de un instrumento jurídicamente vinculante y exigible, el RGPD hace referencia a acuerdos o convenios vinculantes, para los casos que haya una transferencia internacional entre autoridades y organismos públicos; su uso, por tanto, queda limitado al ámbito de Administraciones Públicas (136).

En cuanto a las cláusulas tipo de protección de datos adoptadas por la Comisión o por la autoridad de control y Comisión, éstas serán cláusulas para incluir en los contratos que servirán de garantía en las transferencias que se realicen.

De este modo, podrán llevarse a cabo transferencias internacionales de datos a territorios que no han obtenido la declaración de nivel adecuado de protección, en base a un contrato celebrado entre el exportador y el importador de datos (137). Actualmente, existen las siguientes decisiones de la Comisión Europea sobre cláusulas tipo: la Decisión 2001/497/CE de la Comisión, de 15

(133) Art. 288 del TFUE.

(134) Art. 46.2 del RGPD.

(135) Art. 46.3 del RGPD.

(136) M. Recuero Linares (2019: 423).

(137) V. Guasch Portas (2017: 342).

de junio de 2001 (138) y la Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004 (139), para transferencias entre responsables del tratamiento, y la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010 (140), para transferencias de responsables del tratamiento a encargados del tratamiento.

No obstante, en todo ello, deberemos tener en cuenta la Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 (141). Según ésta, las cláusulas contractuales de la Decisión 2001/497/CE y de la Decisión 2010/87/UE quedarán derogadas a partir del 27 de septiembre de 2021 (también de la Decisión 2004/915/CE (142)); si bien los contratos celebrados antes de dicha fecha con arreglo a las decisiones 2001/497/CE o 2010/87/UE se considerarán que ofrecen garantías adecuadas *ex* RGPD hasta el 27 de diciembre de 2022, siempre que las operaciones de tratamiento permanezcan inalteradas y que las cláusulas contractuales tipo garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas (143).

Esto responde, según recoge la Decisión en sus considerandos, a que los importadores y exportadores de datos deben poder seguir utilizando las cláusulas contractuales tipo establecidas en las Decisiones 2001/497/CE y 2010/87/UE para la ejecución de contratos celebrados entre ellos antes de la fecha de derogación de las Decisiones (27 de septiembre de 2021), durante un período adicional de quince meses (27 de diciembre de 2022), siempre que, como se ha mencionado, las operaciones de tratamiento que sean objeto del contrato permanezcan inalteradas y que las cláusulas garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas en el sentido del RGPD (144).

---

(138) Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE. DO L 181 de 4.7.2001.

(139) 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. DO L 385 de 29.12.2004.

(140) Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, 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 del Parlamento Europeo y del Consejo. DO L 39 de 12.2.2010.

(141) Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

(142) La Decisión 2004/915/CE fue una norma en virtud de la cual se modificó la Decisión 2001/497/CE; por ello derogar ésta significa derogar aquélla.

(143) Art. 4 de la Decisión de Ejecución (UE) 2021/914.

(144) Véase: Considerando n.º 24 de la Decisión de Ejecución (UE) 2021/914.

Las cláusulas contractuales tipo (145) solamente están relacionadas con la protección de datos; ambas partes tienen plena libertad para incluir cualquier otra cláusula sobre cuestiones relacionadas con sus negocios que consideren pertinente para el contrato, siempre que no contradiga las cláusulas contractuales tipo. Las decisiones de la Comisión han establecido las características y contenido que deben reunir estas cláusulas tipo y también formulario con las cláusulas para facilitar su inclusión en el contrato (146). Suponen, de este modo, uno de los mecanismos más utilizados en la práctica para realizar transferencias internacionales con países u organizaciones con los que no existen Decisiones de adecuación (147).

Las cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión son parecidas a las anteriores; serán aprobadas por una autoridad competente (como la AEPD (148)) y aprobadas por la Comisión, siendo necesaria la aprobación de esta última para que sean jurídicamente válidas a efectos del RGPD (149).

En lo que respecta al código de conducta, éste será elaborado por los Estados miembros, autoridades de control, Comité y Comisión Europea, y tendrán como objeto la correcta aplicación del RGPD (150). Constituyen, en sí mismos, mecanismos de autorregulación, además de estar bajo la regulación del reglamento (151).

Así, los códigos de conducta no serán instrumentos específicos previstos para las transferencias internacionales, sino que las transferencias internacionales podrán ser parte de los códigos de conducta (152), y una vez aprobado, si estas se hubieran incluido, serán tomadas como garantías adecuadas (153).

---

(145) D. Sancho Vila (2010: 124 a 128, y 135 y ss.).

(146) Entre estas cláusulas tenemos: cláusula de definiciones, de detalles de la transferencia, de tercero beneficiario, de obligaciones del exportador de datos, de obligaciones del importador de datos, de responsabilidad, etc. Véase: Anexo de la Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010.

(147) M. Recuero Linares (2019: 424).

(148) Entre éstas, tenemos la siguiente, por ejemplo: AEPD. Resolución Autorización Comisión Nacional del Mercado de Valores (CNMV), de 14 de mayo de 2019, de la Agencia Española de Protección de Datos. Nº Expediente: TI/00001/2019. Accesible en: https://www.aepd.es/es/documento/ti-00001-2019-resolucion-autorizacion-cnmv.pdf.

(149) Guasch Portas (2017: 343).

(150) Art. 40.1 del RGPD.

(151) Serrano Pérez (2021: *in toto*). La autora denomina a este fenómeno «autorregulación regulada».

(152) Art. 40.2, letra j), del RGPD.

(153) Véase: Helguero Sáinz (2010: *in toto)*.

El CEPD elaboró las Directrices 1/2019 sobre códigos de conducta y organismos de supervisión (154), en las que estableció los criterios básicos para el funcionamiento de esta figura, en virtud del RGPD; además de recoger los requisitos mínimos que deben cumplir estos códigos de conducta, y los requisitos mínimos para su supervisión efectiva.

El mecanismo de certificación, por último, será expedido por los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos, una vez informada la autoridad de control (155).

3. Normas corporativas vinculantes o *Binding Corporate Rules* (*BCRs*): cobertura adicional a las transferencias de datos personales en el ámbito empresarial y el comercio internacional

La expansión y globalización del comercio internacional ha impulsado la internacionalización necesaria de las empresas, lo que ha supuesto la difícil tarea de compatibilizar derechos fundamentales con las exigencias del comercio internacional (156). Tal como reconoce la doctrina, los movimientos internacionales de datos personales tienen una gran relevancia para la expansión del comercio (157). Es por ello que, como hemos comentado desde el principio, las transferencias internacionales deben conjugar ambas.

Los flujos transfronterizos de datos personales se han vuelto esenciales para el comercio internacional (158); el uso comercial de datos personales potencia el comercio digital y contribuye al crecimiento económico (159), con lo que será necesario conseguir el equilibrio entre dicho uso y la protección de la ciudadanía.

Este supuesto hace referencia al ámbito mercantil: partimos de un supuesto en el que grupos empresariales o uniones de empresas con empresas en distintos países deben traspasarse determinada información. En este caso, sería un obstáculo para el tráfico jurídico tener que solicitar una autorización administrativa para cada vez que una empresa necesite información de otra de su mismo grupo empresarial; al fin y al cabo, las comunicaciones de datos

(154) CEPD. Directrices 1/2019 sobre códigos de conducta y organismos de supervisión con arreglo al Reglamento (UE) 2016/679, de 4 de junio de 2019, del Comité Europeo de Protección de Datos. Accesible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_es.pdf.

(155) Art. 43.1 del RGPD.

(156) A. Ortega Giménez (2016: 29).

(157) J. Oster (2017: 351).

(158) Véase: S. Yakovleva (2020: *in toto).*

(159) S. Yakovleva (2020: 882).

entre filiales multinacionales y/o la gestión de procesos de recursos humanos en una multinacional, entre otras, están a la orden del día (160).

El RGPD ha resuelto esto mediante las normas corporativas vinculantes o *binding corporate rules,* normas corporativas de carácter vinculante aprobadas por la autoridad de control, a las que se podrán unir los grupos de empresas, permitiendo salvaguardar la transferencia de datos y el correcto funcionamiento empresarial. La regulación de esta categoría constituye un importante avance en la agilidad e intereses del tráfico mercantil (161).

Estas normas no serán regulación en sí misma, sino el criterio para concluir si se dan o no garantías suficientes en las transferencias (162). El GT 29 definió las normas corporativas vinculantes o *binding corporate rules* como «códigos de conducta que redactan y siguen organizaciones multinacionales y que contienen medidas internas pensadas para poner en práctica principios de protección de datos (como auditoría, programas de formación, red de funcionarios de privacidad, sistema de tratamiento de quejas)» (163).

Esta categoría no fue recogida por la Directiva 95/46/CE; sin embargo, antes del RGPD, el GT 29 introdujo el concepto de normas corporativas vinculantes y recogió la posibilidad de recurrir a las mismas para la transferencia internacional de datos en su documento de trabajo del año 2003 (164), y elaboró unas directrices y principios sobre las normas corporativas vinculantes, al entender necesaria esta figura jurídica para articular un mecanismo de correcto funcionamiento empresarial en relación con la protección de datos en el año 2008 (165), actualizado en el año 2017 (166) [en 2017 el RGPD ya estaba aprobado, pero aún no era aplicable (167)]. Asimismo, el GT 29 siguió dotando de contenido a esta figura que él creó: estructura de las normas cor-

(160) R. García del Poyo, F. Gari (2007).

(161) A. I. Herrán Ortiz (2002: 312).

(162) P. Fernández-Longoria, J. Fernández-Samaniego (2010: 1789).

(163) GT 29. Dictamen 3/2010 sobre el principio de responsabilidad, del Grupo de Trabajo del Artículo 29, de 13 de julio de 2010, ap. 19.

(164) GT 29. Documento de trabajo n.º 74: Transferencias de datos personales a terceros países: aplicación del artículo 26 (2) de la Directiva de protección de datos de la UE a las normas corporativas vinculantes para las transferencias internacionales de datos, del Grupo de Trabajo del Artículo 29, de 3 de junio de 2003.

(165) GT 29. Documento de trabajo n.º 153 que establece una tabla con los elementos y principios que se encuentran en las normas corporativas vinculantes, del Grupo de Trabajo del Artículo 29, de 24 de junio de 2008.

(166) GT 29. Documento de trabajo n.º 256 que establece una tabla con los elementos y principios que se encuentran en las normas corporativas vinculantes, del Grupo de Trabajo del Artículo 29, de 29 de noviembre de 2017.

(167) Si bien el RGPD fue aprobado en el año 2016, no fue aplicable hasta el 25 de mayo de 2018 (art. 99 del RGPD).

porativas vinculantes (168), preguntas frecuentes (169), elementos y principios a tener en cuenta por el encargado del tratamiento (170), etc.

Actualmente, el hecho de que el RGPD las haya recogido de forma expresa, confiere, por primera vez, rango legal a las normas corporativas vinculantes (171).

A efectos del reglamento, se definen como «las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta» (172); en sus considerandos, además, el reglamento ha establecido que todo «grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta)» (173).

Así, las normas corporativas vinculantes suponen un instrumento jurídico que vincula a las partes de una transferencia internacional de datos y que sirve para ofrecer garantías adecuadas cuando dicha transferencia es a un tercer país sin nivel adecuado decidido por la Comisión. Esta categoría, asimismo, supone una transferencia mediante garantías adecuadas (174), por lo que no será necesaria una autorización expresa de una autoridad de protección de datos para la transferencia internacional de datos basada en normas corporativas vinculantes (estas ya habrán sido aprobadas por una autoridad de protección de datos personales).

De este modo, las normas corporativas vinculantes constituyen el instrumento idóneo para regular las transferencias internacionales de datos personales en estructuras empresariales multinacionales, tanto dentro de las sociedades

(168) GT 29. Documento de trabajo n.° 154 que establece una estructura de las normas corporativas vinculantes, del Grupo de Trabajo del Artículo 29, de 24 de junio de 2008.

(169) GT 29. Documento de trabajo n.° 155 rev. 05 relativo a las preguntas frecuentes sobre las normas corporativas vinculantes, del Grupo de Trabajo del Artículo 29, de 7 de febrero de 2017 (rev.).

(170) GT 29. Documento de trabajo 02/2012 n.° 195 que establece una tabla de elementos y principios a tener en cuenta por el Encargado del Tratamiento en las normas corporativas vinculantes, del Grupo de Trabajo del Artículo 29, de 6 de junio de 2012.

(171) Cordero Álvarez (2019: 71 y 72).

(172) Art. 4, apartado 20°, del RGPD.

(173) Considerando n.° 110 del RGPD.

(174) Art. 46.2, letra b), del RGPD.

del mismo grupo, como aquellas uniones de empresas dedicadas a una actividad económica conjunta. Asimismo, aportan una solución única y homogénea para toda la estructura empresarial, quedando las sociedades con residencia fuera de la UE bajo la normativa comunitaria, de una manera indirecta, ya que a estas se les aplicarán estas normas cuyo contenido se ajustará a las normas europeas.

El RGPD, además, no ha querido que hubiese una remisión normativa sobre el concepto de grupo empresarial y él mismo lo ha definido entendiéndolo, a efectos del reglamento, como «grupo constituido por una empresa que ejerce el control y sus empresas controladas» (175).

Resulta una definición parecida al concepto de grupo en el Derecho español (176) o en la doctrina que la concibe como un agregado empresarial de varias sociedades jurídicamente autónomas que actúan bajo una dirección económica común (177); pero habrá una pequeña diferencia en lo que respecta a los grupos con integración paritaria u horizontal (178), donde no habrá tanta subordinación hacia una sociedad matriz dominante (179). A pesar de ello, aunque anteriormente la figura de las normas corporativas vinculantes se limitaba a entidades pertenecientes a un mismo grupo de empresas, con el RGPD esta figura servirá también para uniones de empresas dedicadas a una actividad económica conjunta, sin que estas tengan que pertenecer necesariamente al mismo grupo empresarial (180). Es por ello que ha sido voluntad del reglamento que todas las concentraciones empresariales (181), aún cuando no pudiesen

(175) Art. 4, apartado 19º, del RGPD.

(176) Art. 18 de la Ley de Sociedades de Capital, en relación al art. 42 del Código de Comercio: «Existe un grupo cuando una sociedad ostente o pueda ostentar, directa o indirectamente, el control de otra u otras».

(177) J. M. Embid Irujo (2003); J. M. Embid Irujo (2012); J. M. Embid Irujo (2013); y J. M. Embid Irujo (2008: 86): «un grupo es un agregado empresarial integrado por diversos sujetos de Derecho (normalmente sociedades) que, sin perjuicio de su personalidad jurídica propia, quedan sometidos en su actuación en el mercado a una dirección económica unificada, ejercida por la entidad cabecera del grupo». También, J. M. Embid Irujo (1987: 153): «empresa articulada, que consigue realizar sus fines mediante la integración de diversas sociedades bajo una dirección económica común, o dirección unitaria».

(178) La integración de los grupos empresariales puede ser jerárquica o vertical (relación de subordinación donde hay una sociedad dominante) o paritaria u horizontal (propiedad única con gestión descentralizada, otorgando un margen de actuación bastante independiente a todas las sociedades del grupo).

(179) *Cfr.* J. M. Embid Irujo (2008: 87 y 88).

(180) Comisión Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo, Intercambio y protección de los datos personales en un mundo globalizado. COM (2017) 7 final, de 10 de enero de 2017, p. 5.

(181) También podemos incluir figuras como el Joint Venture, las sociedades conjuntas, las Agrupaciones de Interés Económico (AIE) o las Uniones Temporales de Empresa (UTE);

incluirse en grupo empresarial, tuviesen a su disposición el uso de este instrumento jurídico a la hora de efectuar transferencias internacionales de datos, para no obstaculizar, así, el tráfico jurídico y el buen funcionamiento empresarial.

Como ya hemos mencionado, con las normas corporativas vinculantes no será necesaria una autorización expresa de una autoridad de protección de datos para la transferencia internacional, ya que estas ya habrán sido aprobadas por una autoridad de protección de datos personales (182): la competente en cada caso (en cada Estado miembro), según donde se encuentre establecido el responsable o el encargado del tratamiento (183). Dicha autoridad de control competente deberá aprobar las normas corporativas vinculantes siempre que: a) sean jurídicamente vinculantes y aplicables para todas las partes en todas las transferencias internacionales que vayan a efectuarse, b) confieran expresamente a los interesados derechos exigibles (teniendo lo previsto por el RGPD como contenido imperativo mínimo), y c) cumplan los requisitos mínimos de contenido exigidos por el reglamento. De igual modo, en el proceso de aprobación por parte de la autoridad de protección de datos competente deberemos tener en cuenta también los documentos (184) y formularios (185) del GT 29. La regulación actual del RGPD, además, reduce los trámites burocráticos al suprimir las obligaciones generales de notificación previa a las autoridades de protección de datos y autorización por estas de las transferencias a terceros países basadas en normas corporativas vinculantes (186).

---

pero, en su caso, las normas corporativas vinculantes cubrirán únicamente las transferencias realizadas desde el inicio de la figura asociativa, hasta el final de la misma; es decir, serán, al igual que la UTE, temporales. La Ley 18/1982, de 26 de mayo, sobre régimen fiscal de agrupaciones y uniones temporales de Empresas y de las Sociedades de desarrollo industrial regional define las UTE como «sistema de colaboración entre empresarios por tiempo cierto, determinado o indeterminado para el desarrollo o ejecución de una obra, servicio o suministro» (art. 7.1).

(182) Art. 57.1, letra s), del RGPD.

(183) Art. 55.1 del RGPD.

(184) GT 29. Documento de trabajo n.º 263 rev. 01 que establece un procedimiento de cooperación para la aprobación de «Reglas Corporativas Vinculantes» para responsables y encargados del tratamiento bajo el RGPD, del Grupo de Trabajo del Artículo 29, de 11 de abril de 2018.

(185) GT 29. Recomendación n.º 264 sobre el formulario de solicitud estándar para la aprobación de las reglas corporativas vinculantes del responsable del tratamiento para la transferencia de datos personales, del Grupo de Trabajo del Artículo 29, de 11 de abril de 2018; y GT 29. Recomendación n.º 265 sobre el formulario de solicitud estándar para la aprobación de las reglas corporativas vinculantes del encargado del tratamiento para la transferencia de datos personales, del Grupo de Trabajo del Artículo 29, de 11 de abril de 2018.

(186) Comisión Europea, Comunicación de la Comisión al Parlamento Europeo y al Consejo, Intercambio y protección de los datos personales en un mundo globalizado. COM (2017) 7 final, de 10 de enero de 2017, p. 5.

Por último, en lo que respecta al contenido de las normas corporativas vinculantes, el RGPD ha establecido un contenido imperativo mínimo que deberán incluir estas (187), entre otras: la estructura y los datos de contacto del grupo empresarial o de la unión de empresas, transferencias o conjuntos de transferencias de datos (categorías, tipo de tratamiento, fines, etc.), carácter jurídicamente vinculante de las normas, aplicación de los principios generales en materia de protección de datos, derechos de los interesados y los medios para ejercerlos, etc.

A parte de este contenido del RGPD, podemos remitirnos de igual modo a los elementos y principios de las normas corporativas vinculantes aprobadas por el GT 29 (188).

Entre las normas corporativas vinculantes (BCRs) que han sido aprobadas por la AEPD podemos mencionar las siguientes: Grupo *Fujikura Automotive Europe, S.A.U.,* de 11 de marzo de 2020, respecto del responsable (189); Grupo *Iberdrola, S. A.,* de 15 de diciembre de 2020, respecto del responsable (190); Grupo *Kumon Europe & Africa Limited, S.A.,* de 26 de febrero de 2021, respecto del responsable (191); y Grupo *Kumon Europe & Africa Limited, S.A.,* de 26 de febrero de 2021, respecto del encargado (192).

4. Excepciones del RGPD para la licitud de las transferencias internacionales

El RGPD, por último, ha previsto unas excepciones para situaciones específicas, para permitir transferencias internacionales; excepciones que se salen de las normas generales del reglamento.

---

(187) Art. 47.2 del RGPD.

(188) GT 29. Documento de trabajo 256 rev. 01 que establece una tabla con los elementos y principios en los que deben basarse las Normas Corporativas Vinculantes del responsable del tratamiento, del Grupo de Trabajo del Artículo 29, de 6 de febrero de 2018 (rev.); y GT 29. Documento de trabajo 257 rev. 01 que establece una tabla con los elementos y principios en los que deben basarse las Normas Corporativas Vinculantes del encargado del tratamiento, del Grupo de Trabajo del Artículo 29, de 6 de febrero de 2018 (rev.).

(189) AEPD. Resolución de Aprobación de las Normas Corporativas Vinculantes del Grupo Fujikura Automotive Europe (Grupo FAE). Expediente: TI/00001/2020. Accesible en: https://www.aepd.es/es/documento/ti-00001-2020-resolucion-aprobacion-bcr-fae.pdf.

(190) AEPD. Resolución de Aprobación de las Normas Corporativas Vinculantes del Grupo Iberdrola. Expediente: TI/00002/2020. Accesible en: https://www.aepd.es/es/documento/ti-00002-2020-resolucion-aprobacion-bcr-iberdrola.pdf.

(191) AEPD. Resolución de Aprobación de las Normas Corporativas Vinculantes del Grupo Kumon. Expediente: TI/00001/2021. Accesible en: https://www.aepd.es/es/documento/ti-00001-2021-resolucion-aprobacion-bcr-r-kumon.pdf.

(192) AEPD. Resolución de Aprobación de las Normas Corporativas Vinculantes del Grupo Kumon. Expediente: TI/00002/2021. Accesible en: https://www.aepd.es/es/documento/ti-00002-2021-resolucion-aprobacion-bcr-e-kumon.pdf.

Así, la primera de las excepciones dispone que, en ausencia de una decisión de adecuación o de garantías adecuadas, una transferencia a un tercer país u organización internacional únicamente se realizará cuando se dé el consentimiento informado y expreso del interesado; cuando sea necesario para la ejecución de un contrato entre el interesado y el responsable del tratamiento (o para ejecutar medidas precontractuales), o para la celebración o ejecución de un contrato entre el responsable y un tercero; por razones importantes de interés público; para la formulación, el ejercicio o la defensa de reclamaciones; para proteger los intereses vitales (del interesado o un tercero); o cuando la transferencia se realice desde un registro público con objeto de facilitar información al público y abierto a la consulta de éste (193).

No obstante ello, el Comité Europeo de Protección de Datos (CEPD) ha declarado, que, de conformidad con los principios inherentes al Derecho europeo, estas excepciones deben interpretarse restrictivamente, para que la excepción no se convierta en la regla general (194); ello siguiendo a la doctrina consolidada del TJUE, que tiene declarado que la protección del derecho fundamental al respeto de la vida privada al nivel de la Unión exige que las excepciones y limitaciones de la protección de los datos de carácter personal deberían aplicarse solamente en la medida en que sea estrictamente necesario (195).

Por otro lado, el RGPD ha recogido una excepción más, con objeto de dar la mayor cobertura posible a las transferencias internacionales. Según ésta, en caso de que no haya decisión de adecuación, garantías adecuadas o alguna de las condiciones citadas, se podrá realizar la transferencia internacional si: a) no es repetitiva, b) afecta a un número limitado de interesados, c) es necesaria a los fines de intereses legítimos del responsable del tratamiento, y d) el responsable del tratamiento ha evaluado todas las circunstancias concurrentes en la transferencia y ha ofrecido garantías (196).

---

(193) Art. 49.1 del RGPD.

(194) CEPD. Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679, del Comité Europeo de Protección de Datos, de 25 de mayo de 2018, p. 4. Accesible en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_es.pdf.

(195) STJUE (Gran Sala), de 16 de diciembre de 2008, asunto C-73/07, caso Satakunnan Markkinapörssi y Satamedia, ap. 56; STJUE (Gran Sala), de 9 de noviembre de 2010, acumulados C-92/09 y C-93/09, casos Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09), ap. 77; STJUE (Gran Sala) de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y Seitlinger y otros, ap. 52; STJUE (Gran Sala), de 6 de octubre de 2015, asunto C-362/14, Maximillian Schrems v. Data Protection Commissioner, ap. 92; y STJUE (Gran Sala), de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige y Watson y otros, ap. 96.

(196) Art. 49.1.II del RGPD.

Entre estas excepciones, la primera es en su mayoría idénticas a las bases de licitud del tratamiento que recoge el reglamento (197); la segunda, en cambio, parece pensada para casos no excepcionales, sino excepcionalísimos, que no se puedan subsumir en ninguna de las anteriores bases comentadas hasta ahora. Parece el RGPD quiere, así, dar mucha más cobertura normativa a las transferencias internacionales, con muchas «oportunidades normativas» que den cobertura a las transferencias que se vayan a realizar. Pero ello a la luz del CEPD y del TJUE supondrá siempre una categoría limitada y restrictiva que será siempre subsidiaria y excepcional, de conformidad con el Derecho de la Unión.

5. Transferencias internacionales de datos personales penales: el flujo transfronterizo de datos personales del ámbito penal

Como análisis final al marco relativo a las transferencias internacionales en la regulación actual de protección de datos, nos es necesario mencionar que, si bien el RGPD establece el marco general, debemos siempre tener en cuenta que puede haber *lex specialis* en este ámbito, que es lo que sucede en el ámbito penal, por ejemplo, con la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (198) (denominada *«Law Enforcement Directive»* o *«LED»*, en inglés), que tendrá una especialidad en las transferencias internacionales, al ser éstas relativas al ámbito penal —directiva que fue traspuesta al ordenamiento jurídico español en virtud de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales—.

En todo esto, también debemos tener en cuenta el Convenio n.º 185 del Consejo de Europa, sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 («Convenio de Budapest») (199). El ámbito del Convenio es la ciberdelincuencia; sin embargo, éste también incluye algunas disposiciones que afectan a la protección de datos, entre otros.

---

(197) Art. 6.1 del RGPD.

(198) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

(199) El Convenio de Budapest fue ratificado por España el 14 de septiembre de 2010 y entró en vigor en España el 1 de octubre de 2010. Véase: Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. «BOE» núm. 226, de 17 de septiembre de 2010.

Actualmente, está en vías de negociación el Segundo Protocolo adicional al Convenio de Budapest (200), que versará, sobre cooperación judicial en ámbito penal, y también sobre transferencias internacionales de datos personales en ámbito penal.

Por tanto, el Convenio de Budapest, la Directiva (UE) 2016/680 y el RGPD coexistirán, siendo éstas las bases de las transferencias internacionales en el marco de las investigaciones y sanciones penales. En dicho régimen, será la propia Directiva (UE) 2016/680 la que regule, como *lex specialis* en este ámbito, las transferencias de datos personales a terceros países u organizaciones internacionales y las decisión de adecuación específicas en este ámbito (art. 36), que serán independientes de las del RGPD analizadas, por lo que una no conlleva la otra, ni la otra conlleva la una (son necesarias decisiones de adecuación separadas).

Así, el régimen construido por la Directiva (UE) 2016/680 y por el Convenio de Budapest ahonda en la creación de flujos transfronterizos de datos personales del ámbito de enjuiciamiento criminal (para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales); un flujo especial relativo a reforzar la cooperación jurisdiccional penal, pero que nacerá de un régimen de transferencia internacional de datos personales.

6. Las transferencias internacionales de datos respecto del Reino Unido: el flujo de datos personales UE-Reino Unido

Una cuestión controvertida, por último, será la situación jurídica del Reino Unido respecto a las transferencias internacionales de datos personales.

Con el «Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica», en virtud del cual Reino Unido dejó de ser parte de la UE desde el 1 de enero del 2021, el país también quedó fuera de la aplicación del RGPD, *de iure*. Por tanto, el Reino Unido pasó de estar dentro del «espacio europeo de la información» a ser un país tercero, a efectos del RGPD; ello pese a que el Acuerdo de Retirada recogió una disposición específica en relación a la protección de datos (201) —si bien ello es cierto, también debemos tener en

(200) Recomendación de Decisión del Consejo por la que se autoriza la participación en las negociaciones sobre un Segundo Protocolo adicional al Convenio del Consejo de Europa sobre Ciberdelincuencia (STE n.o 185), COM(2019) 71 final. Accesible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52019PC0071.

(201) Véase: Artículo 71. Protección de los datos personales. Acuerdo sobre la retirada del Reino Unido de Gran Bretaña e Irlanda del Norte de la Unión Europea y de la Comunidad Europea de la Energía Atómica.

cuenta que, pese a ello, el RGPD sigue siendo aplicable en muchas empresas del Reino Unido, debido a su aplicación extraterritorial, en virtud de su criterio subjetivo (el interesado)—.

Al ser considerado país tercero, se le aplicará el régimen previsto en el RGPD y serán necesarios instrumentos como una decisión de adecuación o garantías adecuadas (202).

De este modo, dentro de las negociaciones ulteriores al Acuerdo de Retirada, Reino Unido y la Unión elaboraron el marco para la constitución de un flujo de datos personales Reino Unido-UE, que trajera consigo un espacio de movimiento de datos. Las negociaciones incluyeron tanto el RGPD (203) como la Directiva (UE) 2016/680, de 27 de abril, *(«Law Enforcement Directive»)* (204), con objeto de crear un flujo transfronterizo de datos personales, en una doble dimensión: el primero, respecto del RGPD, y, el segundo, en lo que respecta a los datos personales relativos a la jurisdicción penal.

En el año 2021, el Parlamento Europeo, por resolución de 21 de mayo de 2021, se pronunció acerca de la adecuación (205), y, finalmente, en virtud de la Decisión de Ejecución de la Comisión Europea, se declaró que Reino Unido mantiene un adecuado nivel de protección (206). Mediante dicha Decisión de Ejecución se constituyó el flujo de datos entre el Reino Unido y la Unión Europea.

Entre los distintos fundamentos en los que se basaron la Decisión de Ejecución tenemos la *UK Data Protection Act 2018* de 2018 del Reino Unido, que entró en vigor el 23 de mayo de 2018, y complementó la aplicación del RGPD y, a su vez, transpuso la Directiva (UE) 2016/680 en el Reino Unido. La

---

(202) Véase: A. Gascón Marcén (2020: *in toto)*.

(203) Borrador del Proyecto de Decisión de la Comisión Europea, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, sobre la protección adecuada de los datos personales por parte del Reino Unido. Accesible en: https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf.

(204) Borrador del Proyecto de Decisión de la Comisión Europea, de conformidad con la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, sobre la adecuada protección de los datos personales por parte del Reino Unido. Accesible en: https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_19_feb_2020.pdf.

(205) Resolución del Parlamento Europeo, de 21 de mayo de 2021, sobre la protección adecuada de los datos personales por parte del Reino Unido [2021/2594(RSP)]. Accesible en: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_ES.pdf.

(206) Decisión de Ejecución de la Comisión, de 28 de junio de 2021, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido. Accesible en: https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

Comisión analiza dicha norma respecto del RGPD, en la que, cuando aquella se elaboró, se adaptaron los principios básicos del reglamento europeo, lo que la Comisión denomina «Derecho de la UE conservado» *(«retained EU law»)* (207); es por ello que la Comisión Europea concluye que, dado que la *DPA* del Reino Unido se basa en la legislación de la UE, «las normas de protección de datos en el Reino Unido en muchos aspectos reflejan fielmente las normas correspondientes aplicables dentro de la Unión Europea» (208).

La Decisión de Ejecución, por otro lado, ha recogido una cláusula de extinción de la propia Decisión; así, transcurrido ese tiempo la Comisión valorará si Reino Unido sigue manteniendo el nivel adecuado de protección con su legislación, y, en ese caso, renovará la Decisión de Ejecución.

Así, a fecha de 2021, los países que tienen declarada la adecuación por la Comisión son trece: Andorra, Argentina, Canadá, Guernesey, Isla de Man, Islas Feroe, Israel, Japón, Jersey, Nueva Zelanda, Reino Unido, Suiza y Uruguay.

VII. EL PODER EXPANSIVO DEL RGPD: DE LA UE, AL MUNDO

Todo lo mencionado hasta aquí también afecta a otros ámbitos como son, entre otros, las relaciones exteriores de la Unión Europea (acuerdos comerciales, cooperación internacional, etc.), y, en especial, a las relaciones comerciales entre la UE y terceros países.

Así, que un país tercero tenga una legislación nacional robusta en materia de protección de datos que cumpla con todas las exigencias mencionadas para que se considere que tiene un nivel adecuado de protección en lo que respecta a datos personales será una ventaja para la creación de redes comerciales entre dicho país tercero y la UE, o entre dicho país tercero y un país europeo.

Ello, asimismo, tiene otra consecuencia: que los países terceros se esfuercen en elaborar marcos legislativos nacionales fuertes que cumplan las características de los cánones exigidos por el RGPD, para así no quedar excluidos en cualquier relación que pueda conllevar de un modo u otro que haya datos personales en juego.

Tal como reconoció la propia Comisión Europea en el año 2010, antes del RGPD, el carácter adecuado del nivel de protección era evaluado en primer lugar por el responsable del tratamiento y, después, por la autoridad de control en materia de protección de datos del Estado miembro correspondiente,

(207) Decisión de Ejecución de la Comisión, de 28 de junio de 2021, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido, p. 4 y 5.

(208) *Ibíd.*

lo que daba lugar a enfoques diferentes de la apreciación del nivel de protección garantizado por los terceros países u organizaciones internacionales y, por consiguiente, tal como se recogió el informe: «implica el riesgo de que el nivel de protección de los interesados previsto en un tercer país se juzgue diferentemente de un Estado miembro a otro. Asimismo, los instrumentos jurídicos existentes no establecen condiciones precisas y armonizadas en cuanto a las transferencias que pueden considerarse legítimas. Por ello, las prácticas varían de un Estado miembro a otro» (209).

Así, el RGPD ha traído que la protección de datos, y especialmente las transferencias internacionales de datos personales y las decisiones de adecuación, se conviertan en un ámbito europeo, lo que ha convertido a la Unión Europea en un bloque que ha unificado y armonizado este ámbito, y ello está haciendo que el reglamento adquiera un protagonismo y una relevancia a nivel global. Se ha consolidado, además, el «espacio europeo de la información», ese espacio interior de datos personales, con libertad de movimiento, que viene a reflejar el espíritu mismo de la UE: la unificación estatal y la libertad de circulación (de datos personales, en este caso).

Por lo tanto, la unificación que ha supuesto el hecho de que el RGPD tenga carácter de reglamento y que la protección de datos se haya europeizado, no solo ha armonizado las normativas nacionales en materia de protección de datos de los veintisiete Estados miembros de la UE, sino que, además, está marcando el camino a seguir en la elaboración de legislaciones nacionales a nivel mundial.

Al fin y al cabo, el propósito de las decisiones de adecuación de la Comisión Europea es confirmar formalmente, con efectos vinculantes para los Estados miembros, que el nivel de protección de datos en un tercer país o una organización internacional es esencialmente equivalente al nivel de protección de datos en la Unión Europea (210).

Tal como declara el GT 29, el documento de trabajo de 2018 tiene como finalidad proporcionar orientación a la Comisión Europea a la hora de evaluar el nivel de protección de datos en terceros países y organizaciones interna-

(209) Comisión Europea, «Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea», Bruselas, 04-11-2010, pp. 16 y 17. COM(2010) 609 final. Accesible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:ES:PDF.

(210) GT 29. Documento de trabajo n.º 254 rev. 01 sobre la Referencia de Adecuación, del Grupo de Trabajo del Artículo 29, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018, p. 3; y también STJUE (Gran Sala), de 6 de octubre de 2015, asunto C-362/14, Maximillian Schrems v. Data Protection Commissioner, ap. 52.

cionales, pero, además, según el propio GT 29, el documento quiere servir también de orientación básica para aquellos terceros países y organizaciones internacionales interesadas en obtener la adecuación (211).

Con todo este régimen, además, se consigue que en las relaciones exteriores de la Unión Europea, especialmente en los acuerdos comerciales internacionales, la protección de datos no sea negociable; por lo que, así, los derechos de privacidad y protección de datos no estarán sujetos a negociación en ningún acuerdo comercial internacional futuro con países no pertenecientes a la UE (212).

Por todo ello, el reglamento ésta siendo la punta de lanza de la regulación relativa a la protección de datos a nivel mundial, manteniéndose a la vanguardia en este ámbito, y, de un modo indirecto, está influyendo en las normas nacionales de otros Estados a nivel internacional, máxime cuando el TJUE ha establecido que cualquier decisión de adecuación —que conlleva la creación de flujos— se deberá adaptar siempre al marco del RGPD y la CDFUE (213).

De este modo, los países terceros, en caso de que quisieran mantener las relaciones (comerciales, por ejemplo) con la Unión, intentarán adecuarse lo máximo posible al RGPD (214); ello está haciendo que el RGPD se convierta en un modelo a seguir para los legisladores de todo el mundo.

---

(211) GT 29. Documento de trabajo n.º 254 rev. 01 sobre la Referencia de Adecuación, del Grupo de Trabajo del Artículo 29, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018, p. 2: «*This document aims to provide guidance to the European Commission and the WP29 under the GDPR for the assessment of the level of data protection in third countries and international organizations […]. In addition, it may guide third countries and international organizations interested in obtaining adequacy*».

(212) Véase: Supervisor Europeo de Protección de Datos (SEPD), «Data protection is non-negotiable in international trade agreements», 2021. Accesible en: https://edps.europa.eu/press-publications/press-news/press-releases/2021/data-protection-non-negotiable-international_en.

(213) STJUE (Gran Sala), de 16 de julio de 2020, asunto C-311/18, Data Protection Commissioner v. Facebook Ireland Limited y Maximillian Schrems, ap. 140 y ss.

(214) Podemos poner el siguiente caso a modo de ejemplo: en el año 2019 la República de Kenia aprobó la Ley n.º 24 de 2019, de protección de datos (*Data Protection Act, 2019).* Dicha norma es muy parecida al RGPD (en algunos apartados rozando la copia), y ello será muy beneficioso a la hora de relacionarse con la UE. No obstante, en este caso preciso, sí hay un impedimento: Kenia aún no tiene constituida una autoridad de control de protección de datos, lo cual dificulta la ya mencionada consideración de nivel adecuado de protección según el RGPD, ya que la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en materia de protección de datos es uno de los requisitos para ello (art. 45.2 del RGPD). Sin embargo, la norma keniata es un ejemplo de lo mencionado. La Ley está accesible en el Boletín Oficial de la República de Kenia *(Kenya Gazette):* http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.

Y también para consulta en línea: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019.

VIII. CONCLUSIONES

Los flujos transfronterizos de datos personales *(cross border flows of personal data)* son un fenómeno que nos aparecerá constantemente por la importancia que tienen los datos hoy en día y por vivir actualmente en un mundo globalizado.

De este modo, y como hemos analizado, todas las regulaciones sobre transferencias internacionales de datos personales tenían, y siguen teniendo, la voluntad de aunar la protección de los datos personales y la libre circulación de dichos datos personales a nivel internacional.

Las regulaciones que se han ido sucediendo han tenido un carácter normativo mínimo, dando, así, un punto de inicio a las transferencias internacionales de datos personales y dejando el desarrollo legislativo y normativo en manos de los Estados. Sin embargo, el RGPD ha supuesto un cambio sustancial en esta materia: ha dotado de bastante contenido la regulación sobre las transferencias internacionales de datos y, además, por su carácter de reglamento, ha supuesto una armonización y un auténtico paso adelante en este ámbito a nivel comunitario.

Las decisiones de adecuación suponen un instrumento jurídico fundamental para permitir una mayor libertad de flujo transfronterizo de datos, ya no será decidido por cada Estado miembro, sino de una manera comunitaria; a ello debemos añadirle las garantías adecuadas y las normas finales de transferencias internacionales de datos. Parece que el RGPD quiere, así, dar mucha más cobertura normativa a las transferencias internacionales, con muchas «oportunidades normativas» que den cobertura a las transferencias que se vayan a realizar, con dos fines: permitir que haya cuantas más transferencias posibles y, al mismo tiempo, asegurarse de que todas las transferencias que se realicen cumplan con lo establecido y den garantías y, sobre todo, protección a los sujetos de los datos transferidos.

El reglamento supera indudablemente la anterior regulación de la directiva y crea una mayor libertad de circulación de datos, mediante un flujo o espacio europeo libre de datos personales (toda la UE, más el EEE) y ampliaciones de dichos flujos llevabas a cabo a través de las decisiones de adecuación. Con dichas ampliaciones hechas por la Comisión, además, se consigue de manera indirecta que los estándares normativos europeos en materia de protección de datos sean incluidos en legislaciones de terceros países.

Como se ha mencionado, los flujos de datos personales suponen que los datos circularán tan libremente entre los dos países u organizaciones internacionales como dentro del país. Siendo así, por un lado, el RGPD ha unificado la libre circulación de datos; por otro, se ha expandido la norma al EEE, y, por último, se han creado distintos flujos de datos personales en virtud de decisiones

de adecuación que viene a construir redes exteriores de circulación de datos con base en el contenido del RGPD, expandiendo los principios básicos de la norma.

La inclusión, por otro lado, de las normas corporativas vinculantes como figura en el RGPD ha supuesto dotar a las empresas multinacionales de un instrumento jurídico muy beneficioso para el buen desarrollo empresarial; además, se logra así que las corporaciones que no tuvieren el domicilio en la UE queden bajo la aplicación de la normativa comunitaria en materia de protección de datos.

Recordando, asimismo, que tanto los movimientos internacionales de datos personales como los flujos transfronterizos de datos personales tienen una gran relevancia para la expansión del comercio, podemos afirmar que la UE ha conseguido su objetivo de construir las bases legales del «espacio europeo de la información», en la que se debe buscar el equilibrio entre la libre circulación de información y la protección de la ciudadanía y sus datos personales.

De este modo, el RGPD no solo ha creado un «espacio europeo de información» o un «espacio europeo de datos» (personales, en este caso) —que alcanza a los veintisiete Estados miembros y a los miembros del EEE—, sino que el RGPD también ha contribuido a esbozar las líneas fundamentales en materia de regulación de datos personales a nivel global, que hará que la norma influya sobre las legislaciones de los Estados a nivel mundial.

IX. BIBLIOGRAFÍA

Aberasturi Gorriño, Unai (2011): «Movimiento internacional de datos especial referencia a la transferencia internacional de datos sanitarios», *Revista de administración pública,* 186, pp. 329-369.

Aberasturi Gorriño, Unai, Lasagabaster Herrarte, Iñaki (2011): «La cesión de datos de salud fuera del ámbito sanitario. Análisis de supuestos concretos en que la información sanitaria se transmite para el cumplimiento de fines distintos al de la protección de la salud de las personas», *Revista Vasca de Administración Pública,* 91, pp. 17-101.

Álvarez Rigaudias, Cecilia (2010): «Las transferencias internacionales de datos personales Título V. Movimiento Internacional de Datos. Artículos 33 y 34», en Troncoso Reigada, Antonio (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Madrid, Civitas, pp. 1800-1834.

Aparicio Salom, Javier (2000): *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal,* Madrid, Aranzadi.

— (2014): «El tercero a quien se comunican los datos. Un tercer género entre quienes tratan datos», *Revista Aranzadi de derecho y nuevas tecnologías,* 34, pp. 23-42.

ARIAS POU, María (2016): «Definiciones a efectos del reglamento general de protección de datos», en PIÑAR MAÑAS, José Luis (dir.), ÁLVAREZ CARO, María (coord.), RECIO GAYO, Miguel (coord.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos,* Madrid, Reus, pp. 115-134.

BENNETT, Colin J., RAAB, Charles D. (2006): *The governance of privacy, Policy Instruments in Global Perspective*, Massachusetts, The MIT Press.

BUQUICCHIO, Giovanni (1986): «Informática y libertades: Balance de quince años de actividad en el seno del Consejo de Europa», *Jornadas Internacionales sobre Informática y Administración Pública,* Oñati, Instituto Vasco de Administración Pública-Herri Arduralaritzaren Euskal Erakundea.

BYGRAVE, Lee A. (2010): «International agreements to protect personal data», en Rule, James B., Greenleaf, Graham (ed.), *Global Privacy Protection. The First Generation,* Cheltenham (Reino Unido), Edward Elgar Publishing.

CAMPUZANO TOMÉ, Herminia (2002): *Vida privada y datos personales,* Madrid, Tecnos.

CERDA SILVA, Alberto (2011): «El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea», *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso,* 36, pp. 327-356.

CONDE ORTIZ, Concepción (2005): *La protección de datos personales, Madrid, Dykinson.*

CORDERO ÁLVAREZ, Clara Isabel (2019): «La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: especial referencia al caso estadounidense y la Cloud Act», *Revista Española de Derecho Europeo,* 70, pp. 49-108.

COUDERT, Fanny (2005): «Transferencias internacionales de datos», en ALMUZARA ALMAIDA, Cristina (coord.), *Estudio práctico sobre la protección de datos de carácter personal,* Madrid, Lex Nova, pp. 385-417.

DAVARA RODRÍGUEZ, Miguel Ángel (2007): «La transferencia Internacional de Datos», *Revista Española de Protección de Datos,* 1, pp. 17-60.

EMBID IRUJO, José Miguel (1987): *Grupos de sociedades y accionistas minoritarios. La tutela de la minoría en situaciones de dependencia societaria y grupo,* Madrid, Ministerio de Justicia, Centro de Publicaciones.

— (2003): *Introducción al derecho de los grupos de sociedades,* Granada, Comares.

— (2008): «El significado jurídico de los grupos de sociedades. La corporate governance», *Ekonomiaz: Revista vasca de economía,* 68, pp. 84-101.

— (2012): «Ante la regulación de los grupos de sociedades en España», *Revista de derecho mercantil,* 284, pp. 25-52.

— (2013): «*Los grupos de sociedades en la propuesta de Código Mercantil», Revista de derecho mercantil,* 290, pp. 53-68.

Estadella Yuste, Olga (1995): *La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales,* Madrid, Tecnos.

Estadella Yuste, Olga (1996): *La transmisión internacional de datos personales y su control,* Madrid, Tecnos.

European Union Agency for Fundamental Rights and Council of Europe (2018): *Handbook on European data protection law*, Luxemburgo, Publications Office of the European Union. Accesible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.

Fatás Monforte, José Miguel, García Sanz, Javier (2008): «Título Primero. Disposiciones Generales (Arts. 1 a 7)», en Palomar Olmeda, Alberto (dir.), González-Espejo García, Pablo (dir.), Álvarez Rigaudias, Cecilia Irene (coord.), *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre),* Cizur Menor, Thomson-Civitas.

Fernández-Longoria, Paula, Fernández-Samaniego, Javier (2010): «Transferencias internacionales de datos personales. Título V. Movimiento Internacional de Datos. artículos 33 y 34», en Troncoso Reigada, Antonio (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Madrid, Civitas, pp. 1767-1800.

García del Poyo, Rafael, Gari, Francisco (2007): «Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales», *Revista Española de Protección de Datos,* 2, pp. 239-266.

García-Cuevas Roque, Elena (2012): «Las transferencias internacionales de datos y las libertades individuales: un acercamiento a las normas de protección de datos», *Estudios de Deusto,* 60, 2, pp. 171-194.

Gascón Marcén, Ana (2020): «La regulación del flujo de datos personales entre la Unión Europea y el Reino Unido tras el Brexit», *Cuadernos de Derecho Transnacional,* 12, 1, pp. 231-246.

Gonzalo Doménech, Juan José (2019): «Las decisiones de adecuación en el derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros», *Cuadernos de Derecho Transnacional,* 11, 1, pp. 350-371.

Guasch Portas, Vicente (2012): «La transferencia internacional de datos de carácter personal», *RDUNED. Revista de Derecho UNED,* 11, pp. 413-454.

— (2017): «La computación en nube y las transferencias internacionales de datos en el nuevo reglamento de la UE», *RDUNED. Revista de derecho UNED,* 20, pp. 333-350.

HELGUERO SAINZ, José (2010): «Objeto y naturaleza de los códigos tipo», en TRONCOSO REIGADA, Antonio (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Madrid, Civitas, pp. 1727-1747.

HEREDERO HIGUERAS, Manuel (1996): *La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentario y Textos,* Madrid, Tecnos.

— (1997): *La Directiva Comunitaria de Protección de los Datos de Carácter Personal,* Pamplona, Aranzadi.

HERRÁN ORTIZ, Ana Isabel (2002): *El Derecho a la Intimidad en la nueva Ley Orgánica de Protección de Datos Personales,* Madrid, Dykinson.

HOWARD, Philip N., JONES, Steve (ed.) (2005): *Sociedad on-line: Internet en contexto, Barcelona,* Editorial UDOC.

MADEC, Alain (1984): *El mercado internacional de la información. Los flujos transfronteras de informaciones y datos,* Madrid, Fundesco/Tecnos.

MENDOZA LOSANA, Ana Isabel (2015): «Transferencias Internacionales de Datos Personales: Estados Unidos no es un Puerto Seguro, pero tampoco una isla inalcanzable», *Revista CESCO de Derecho de Consumo*, 15, pp. 212-227.

ORTEGA GIMÉNEZ, Alfonso (2015): *La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita,* Madrid, AEPD.

— (2016): *Transferencias internacionales de datos de carácter personal ilícitas,* Cizur Menor, Thomson Reuters-Aranzadi.

OSTER, Jan (2017): E*uropean and International Media Law,* Cambridge (Reino Unido), Cambridge University Press.

PIÑAR MAÑAS, José Luis (2010): «Concepto de datos de carácter personal: Título I. Disposiciones Generales. Artículo 3», en TRONCOSO REIGADA, Antonio (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Madrid, Civitas, pp. 183-213.

— (2017): «Capítulo septuagésimo. Las transferencias internacionales en el nuevo reglamento europeo de protección de datos», en PAREJO ALFONSO, Luciano José (coord.), VIDA FERNÁNDEZ, José (coord.), *Los retos del Estado y la Administración en el siglo XXI: libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo,* Vol. II, Valencia, Tirant lo Blanch, pp. 2063-2098.

— (2016): «Transferencias de datos personales a terceros países u organizaciones internacionales», en PIÑAR MAÑAS, José Luis (dir.), ÁLVAREZ CARO, María

(coord.), Recio Gayo, Miguel (coord.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos,* Madrid, Reus, pp. 427-460.

Piñol i Rull, Joan, Estadella Yuste, Olga (1993): «La regulación de la transmisión internacional de datos en la L.O. 5/1992 de 29 de octubre», en Ripoll I Carulla, Santiago (coord.), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática,* Barcelona, Universitat Pompeu Fabra.

Pulido Quecedo, Manuel (2003): «La catequista y los riesgos de Internet», *Actualidad Jurídica Aranzadi,* XIII, 602.

Rallo Lombarte, Artemi (2012): «Hacia un nuevo sistema europeo de protección de datos las claves de la reforma», *Revista de derecho político,* 85, pp. 13-56.

Recio Gayo, Miguel (2019): «Nivel adecuado para transferencias internacionales de datos», Derecho PUCP: *Revista de la Facultad de Derecho,* 83 (Ejemplar dedicado a: Nuevas tecnologías: El futuro del Derecho en la era digital), pp. 207-240.

Recuero Linares, Mikel (2019): «Transferencias internacionales de datos genéticos y datos de salud con fines de investigación», *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada = Law and the human genome review: genetics, biotechnology and advanced medicine,* Extra 1, pp. 413-433.

Ripoll Carulla, Santiago (1994): «El movimiento internacional de datos. Legislación española y derecho internacional», *TELOS,* 37.

Sancho Villa, Diana (2010): *Negocios Internacionales de Tratamiento de Datos Personales,* Cizur Menor, Civitas-Thomson Reuters.

Serrano de Pablo Valdenebro, Luis (2008): «XI. Las transferencias internacionales de datos (arts. 65 a 70)», en Zabía de la Mata, Juan (coord.), *Protección de Datos. Comentarios al Reglamento,* Valladolid, Lex Nova.

Serrano Pérez, María Mercedes (2005): «El derecho fundamental a la Protección de Datos. Su contenido esencial», *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas,* 1, pp. 245-265.

— (2021): «Algunos elementos de los códigos de conducta: la autorregulación regulada», *AC, Asuntos Constitucionales,* 0, 151-168.

Solar Calvo, Pedro (2012): «La doble vía europeo de protección de datos», *Diario La Ley,* 7832, XXXIII.

Stoffel Vallotton, Nicole (2003): «El espacio económico europeo: un ejemplo de integración diferenciada en las relaciones exteriores de la Unión Euro-

pea. La aplicación del acervo comunitario a terceros estados», *Revista de Derecho Comunitario Europeo, 7*, 15, pp. 573-625.

SUÑÉ LLINÁS, Emilio (1999): «Marco jurídico del tratamiento de datos personales en la Unión Europea y en España», en VV. AA., *La armonización legislativa de la Unión Europea,* Madrid, Dykinson-Universidad Rey Juan Carlos (URJC), pp. 245-274.

TUDORICA, Melania, MULDER, Trix (2019): «The GDPR Transfer Regime and Modern Technologies», VV. AA., *Proceedings of ITU Kaldeioscope: ICT for Health: Networks, standards and innovation,* Atlanta (Georgia), International Telecommunication Union (ITU).

ULL PONT, Eugenio (2000): *Derecho Público de la Informática (Protección de datos de carácter personal),* Madrid, UNED.

VERDAGUER LÓPEZ, Jordi, BERGAS JANÉ, Mª Antonia (2012): *TODO Protección de Datos,* Valencia, CISS.

YAKOVLEVA, Svetlana (2020): «Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'», *The Journal of World Investment & Trade,* 21, 6, pp. 881-919.