

ANULACIÓN DEL PRIVACY SHIELD EN LAS TRANSFERENCIAS
INTERNACIONALES DE DATOS: ¿PRESENCIAMOS UN
DESPLAZAMIENTO FÁCTICO DE LA RESPONSABILIDAD?

*CANCELLATION OF THE PRIVACY SHIELD IN INTERNATIONAL
DATA TRANSFERS: ARE WE WITNESSING A FACTUAL SHIFT IN
RESPONSIBILITY?*

Rev. Boliv. de Derecho N° 31, enero 2021, ISSN: 2070-8157, pp. 476-503



Juan Francisco
RODRÍGUEZ
AYUSO

ARTÍCULO RECIBIDO: 9 de septiembre de 2020

ARTÍCULO APROBADO: 13 de noviembre de 2020

RESUMEN: El presente estudio ofrece un análisis exhaustivo de las transferencias internacionales de datos personales a terceros países u organizaciones internacionales merced a la nueva normativa en materia de privacidad. Más concretamente, analiza los efectos que, sobre este esquema normativo, trae consigo la anulación del Escudo de privacidad en los movimientos transatlánticos de información entre la Unión Europea y Estados Unidos y cómo ello supone, de facto, una traslación de la responsabilidad hacia el responsable del tratamiento.

PALABRAS CLAVE: Dato personal; transferencias internacionales; RGPD; UE; EE. UU.

ABSTRACT: *This study provides a comprehensive analysis of international transfers of personal data to third countries or international organizations due to new privacy regulation. More specifically, it analyzes the effects on this regulatory scheme of the annulment of the Privacy Shield in the transatlantic information movements between the European Union and the United States and how this implies, in fact, a transfer of responsibility to the controller.*

KEY WORDS: *Privacy; international transfers; GDPR; EU; US.*

SUMARIO.- I. INTRODUCCIÓN.- II. CONCEPTO DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES Y MEDIOS PARA SU REALIZACIÓN LEGÍTIMA.- 1. Transferencias basadas en una decisión de adecuación por parte de la Comisión.- 2. Transferencias efectuadas mediante la prestación de garantías adecuadas.- 3. Transferencias específicas y excepcionales.- III. TRANSFERENCIAS INTERNACIONALES DE DATOS A ESTADOS UNIDOS TRAS LA ANULACIÓN DEL ESCUDO DE PRIVACIDAD: INTERROGANTES Y ALTERNATIVAS.

I. INTRODUCCIÓN.

El Capítulo V del 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/CE¹ (en adelante, Reglamento general de protección de datos o RGPD) abarca los arts. 44 y 50 y, en ellos, se disciplinan las conocidas como “Transferencias de datos personales a terceros países u organizaciones internacionales”. Mucho más escueta era, al respecto, 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 datos² (en adelante, DPDP), que dedicaba a esta cuestión tan sólo los preceptos 25 y 26, es decir, dos artículos frente a los seis de la nueva normativa comunitaria. Únicamente teniendo en cuenta este aspecto, podemos observar que el legislador europeo ha adquirido conciencia de la relevancia que supone la realización de transferencias internacionales de datos personales en un panorama globalizado como el actual, pretendiendo contribuir con una mayor clarificación y detalle normativo a esta cuestión.

A nivel interno español, los preceptos del Reglamento general de protección de datos se verán desarrollados y completados por el Título VI (que comprende los arts. 40 a 43) de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales³ (en adelante, LOPDGDD). De este modo, se produce un desplazamiento de las medidas contenidas en los

1 Diario Oficial de la Unión Europea (en adelante, DOUE) L 119/1, de 4 de mayo de 2016.

2 Diario Oficial de las Comunidades Europeas (en adelante, DOCE) L 281/31, de 23 de noviembre de 1995.

3 Boletín Oficial del Estado (en adelante, BOE) núm. 294, de 6 de diciembre de 2018.

• Juan Francisco Rodríguez Ayuso

Profesor Ayudante Doctor acreditado por ANECA y Coordinador Académico del Máster Universitario en Protección de Datos, Universidad Internacional de La Rioja (UNIR), Av. de la Paz, 137 26006 Logroño, La Rioja, España. ORCID ID: <https://orcid.org/0000-0003-4721-1465>. E-mail: juanfrancisco.rodriguez@unir.es.

arts. 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD) y de aquellas previstas en los arts. 65 a 70 y 137 a 144 del 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 (en adelante, RDLOPD).

Sin embargo, no se contempla en la nueva regulación una definición que nos permita entender qué es una transferencia internacional de datos personales, siguiendo, en este punto, la línea marcada por la DPDP. Tampoco se incluye definición alguna que haga posible conocer qué se entiende por tercer país. Pese a ello, conviene aclarar que, a efectos de la nueva (también de la anterior) normativa en materia de protección de datos personales, no tendrán la consideración de transferencia internacional aquellas transmisiones de datos personales que se produzcan en el interior del territorio comunitario. Es por ello por lo que el art. 4.23) RGPD conceptualiza los tratamientos transfronterizos de la siguiente manera: a) bien como 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; b) bien como el tratamiento de datos personales realizado en el contexto de las actividades de un único 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. En otras palabras, los tratamientos transfronterizos no serán, en sentido estricto, transferencias internacionales, ya que tienen lugar en el interior de la Unión Europea, cuyo territorio proporciona el mismo nivel de protección en materia de protección de datos. De este modo, las transferencias internacionales comportan un tratamiento de datos personales en el que confluyen, como mínimo, un Estado comunitario y un tercer país u organización internacional situado fuera de la Unión Europea.

A la vista de lo anterior, la nueva regulación, nacional y comunitaria, sobre protección de datos personales pone de manifiesto, de un lado, la clara convicción de que la realización de transferencias de datos personales a terceros países u organizaciones internacionales constituyen una realidad fundamental en la actualidad, y, de otro, la evidencia (a la que procura dar respuesta) de los riesgos que tales transferencias internacionales pueden conllevar para los derechos y libertades de las personas físicas titulares de los datos personales. Merced a ello, se configura un escenario que, siguiendo la herencia marcada por la normativa ya derogada, introduce novedades relevantes que veremos a largo de los siguientes apartados.

II. CONCEPTO DE TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES Y MEDIOS PARA SU REALIZACIÓN LEGÍTIMA.

Como ya hemos anticipado en líneas anteriores, ni la regulación precedente ni la actual proporcionan una definición que permita comprender qué constituye una transferencia internacional de datos personales. Pese a ello, y siendo conscientes de la dificultad que entraña reducir a un concepto la figura, especialmente en un mundo globalizado como en el que vivimos actualmente, parece imprescindible establecer los elementos cuya concurrencia nos permitan afirmar que estamos en presencia de la misma:

En primer lugar, parece evidente, hemos de estar ante un tratamiento de datos personales, es decir, ante un tratamiento de cualquier tipo de información que afecte a una persona física identificada o identificable [art. 4.1) RGPD], que no es sino el interesado, siempre y cuando dicho tratamiento y dicho sujeto se encuentren sometidos al ámbito de aplicación establecido en los arts. 2 y 3 RGPD y 2 LOPDGDD⁴.

En segundo lugar, en tratamiento de estos datos personales habrá de ser considerado, además, como transferencia internacional. Pese a lo que pueda parecer, con esta afirmación no se incurre en afirmaciones absurdas o en reiteraciones innecesarias, ya que, como ha quedado puesto de manifiesto, la nueva normativa en materia de protección de datos no proporciona definición alguna de transferencia internacional de datos personales⁵.

Así las cosas, ¿podríamos entender que el concepto de transferencia internacional de datos personales abarcaría también aquellos supuestos en los que el tratamiento de los mismos persiga, de un modo claro, su puesta a disposición de terceros? En este sentido, la letra g) del art. 49.1 RGPD permite aportar claridad al respecto, ya que entiende adecuada a Derecho aquella transferencia de datos que tenga lugar desde un registro público que, al amparo del ordenamiento jurídico interno de los Estados miembros o de conformidad con el Derecho comunitario, persiga proporcionar información al público y esté abierta a la consulta del público en general o, más específicamente, de cualquier sujeto que pueda llegar a acreditar un interés legítimo, si bien únicamente en la medida en que, en cada supuesto específico, se satisfagan las condiciones que impone el Derecho comunitario o el Derecho interno de los países comunitarios.

4 EUROPEAN DATA PROTECTION BOARD: "The transfer of personal data to third countries and international organisations by EU institution and bodies", *Position paper*, 2014, pp. 5-6.

5 LÓPEZ CALVO, J.: "Transferencia de Datos Personales a terceros países y organizaciones internacionales (Arts. 44-50 RGPD. Arts. 40-43 y Disposición adicional quinta y decimotercera LOPDGDD)", en AA.VV.: *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (coord. por J. LÓPEZ CALVO), Wolters Kluwer, Madrid, 2019, pp. 572-573.

A continuación, se describen cada una de las vías que, llegado el caso, podrían permitir la realización de transferencias de datos personales a terceros países u organizaciones internacionales. Tales alternativas se encuentran recogidas en los arts. 45 a 49 RGPD y 41 a 43 LOPDGDD.

I. Transferencias basadas en una decisión de adecuación por parte de la Comisión.

La regulación en materia de protección de datos personales pivota en torno a un modelo amparado en la existencia de decisiones de adecuación como elemento primario para la realización satisfactoria y jurídicamente adecuada de transferencias internacionales de datos personales.

En cuanto a la competencia para poder adoptar esta decisión de adecuación, la regulación precedente establecía los cimientos que permitieron que no sólo fuera la Comisión, sino también cada uno de los Estados miembros, quienes tuvieran la facultad de disponer si un determinado país, situado fuera de las fronteras comunitarias, ofrecía un nivel adecuado de protección de los datos personales de los interesados⁶. Empero, la nueva normativa encomendará esta decisión de adecuación únicamente a la Comisión, excluyendo a los Estados miembros; de acuerdo con el apartado primero del art. 45 y con el considerando 103, ambos del Reglamento general de protección de datos, la razón que justifica esta asignación única y exclusiva a la Comisión parece justificarse por la necesidad de aportar, a nivel de toda la Unión Europea, seguridad y uniformidad jurídica en lo que atañe a ese país tercero u organización internacional que deba ofrecer, llegado el caso, el nivel adecuado de protección.

Además, se ha ampliado de manera expresa el ámbito subjetivo de quienes pueden ser objeto de esta decisión de adecuación. En este sentido, podrán serlo los terceros países o un territorio concreto o uno o varios sectores de manera específica dentro de ese tercer país, así como una organización internacional (art. 45.1 RGPD). Pese a ello, la nueva normativa no establece definición alguna de territorio o sector específico, de manera tal que esta concreción en cuanto al alcance de sendos términos habrá de ser desarrollada en las decisiones de adecuación que, en su caso, sean adoptadas.

En cuanto al procedimiento, el Reglamento general de protección de datos asigna a la Comisión la competencia necesaria para poder llevar a cabo la adopción de un acto de ejecución en virtud del cual se establezca la conformidad. Este acto será adoptado de acuerdo con el procedimiento de examen a que alude el art.

6 RECIO GAYO, M.: "Nivel adecuado para transferencias internacionales de datos", *Derecho PUCP: Revista de la Facultad de Derecho*, núm. 83, 2019, p. 213.

93.2 RGPD, precepto este que, a su vez, hace referencia al artículo quinto del Reglamento (UE) n° 182/2011 del Parlamento Europeo y del Consejo de 16 de febrero de 2011 por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión⁷.

Ahora bien, además de la Comisión, el Comité Europeo de Protección de Datos (en adelante, CEPD o, en inglés, *European Data Protection Board* -EDPB-) asumirá, como en su momento hiciera el Grupo de Trabajo del Artículo 29, un papel esencial en este proceso. Tanto es así que la letra s) del art. 70.1 del Reglamento general de protección de datos establece que el CEPD habrá de facilitar a la Comisión un dictamen para que esta pueda realizar la evaluación de la adecuación en relación con el nivel de protección que ha de presentar el tercer país u organización internacional, en especial con la finalidad de poder realizar la evaluación de si este tercer país, un territorio o uno o varios sectores específicos del mismo, así como una organización internacional, llegado el momento, ya no pueden garantizar este nivel satisfactorio de protección. En este sentido, la Comisión deberá proporcionar al citado Comité toda la información y documentación que resulte preceptiva, donde se incluya la correspondencia mantenida con el gobierno del tercer país, que se refiera al territorio afectado.

Desde un punto de vista práctico, estos dictámenes han sido decisivos en el desarrollo de procedimientos para reconocer el nivel de adecuación, ya que son imprescindibles dada la perspectiva estrictamente jurídica y técnica que asume el CEPD, garantizando, así, un estudio imparcial de cada supuesto⁸. Este dictamen, conviene advertir, será preceptivo, si bien no vinculará a la Comisión para que esta adopte las decisiones que estime oportunas.

Nada se detalla en el Reglamento general de protección de datos en cuanto a la manera en que el proceso ha de ser iniciado. Cabría la posibilidad de que el inicio fuera llevado a cabo por la Comisión de oficio o, incluso, a iniciativa del EDPB. De igual modo, podría surgir como resultado de un acuerdo internacional anterior celebrado por la Comisión. No obstante, lo más normal es que sean los países, sus territorios o las organizaciones internacionales que tengan interés en el resultado de la decisión de adecuación, los que tomen la iniciativa de presentar su solicitud ante la Unión Europea, originando el análisis de los aspectos a que alude el art. 45.2 RGPD.

7 DOUE L 55/13, de 28 de febrero de 2011.

8 CERVERA NAVAS, L.: "El Comité Europeo de Protección de Datos", en AA.VV.: *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (coord. A. RALLO LOMBARTE), Tirant lo Blanch, Valencia, 2019, p. 667.

Este análisis abarca los distintos aspectos a que alude dicho precepto. En este sentido, el considerando 104 RGPD establece el marco general en que se ha de sustentar este análisis, como son los valores fundamentales en que se fundamenta la Unión Europea, especialmente la protección de los derechos humanos⁹. En este contexto, la Comisión habrá de valorar obligatoriamente determinados elementos que han de perseguir esta protección eficaz, no únicamente formal, de la protección de los datos personales del interesado. Conviene poner de manifiesto, no obstante, que algunos de estos aspectos son de difícil evaluación en relación con las organizaciones internacionales; tanto es así que, si advertimos, en el considerando 104 RGPD no se hace alusión alguna a las mismas.

Así las cosas, los aspectos que se deberán considerar al respecto pueden ser agrupados en tres categorías:

a) El marco jurídico general, en sentido amplio [letra a) del art. 45.2 RGPD]. Se tendrá en cuenta, aquí, que se trate de un Estado de Derecho, que respete los derechos y libertades, que cuente con una legislación adecuada, con jurisprudencia, con el reconocimiento de derechos, entre otras cuestiones. Además, se incorpora una alusión específica al acceso de las autoridades públicas a los datos personales y a la obligación de proteger las transferencias internacionales de datos que se realicen posteriormente.

Ello nos recuerda, en parte, a la enumeración establecida por el Tribunal de Justicia de la Unión Europea (en adelante, TJUE) en la sentencia de 6 de octubre del año 2015, asunto C-362/14, en virtud de la cual se declaraba la invalidez de la Decisión 2000/520/CE de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América¹⁰, de gran relevancia en la conformación que, en la actualidad, presenta el modelo de adecuación.

b) Que existan y funcionen de manera eficaz una o varias autoridades de control en el tercer país, territorio u organización internacional de que se trate [letra b) del art. 45.2 RGPD]. Estas autoridades de control tendrán la obligación de cooperar con las autoridades de la Unión Europea y de los Estados miembros. En este sentido, el considerando 104 RGPD establece la obligación de que el control

9 CORDERO ÁLVAREZ, C. I.: "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*, núm. 70, 2019, pp. 58-62; EDUARDO USTARAN, P. G.: "Transferencias internacionales de datos", en AA.VV.: *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (coord. por A. RALLO LOMBARTE), Tirant lo Blanch, Valencia, 2019, pp. 473-475.

10 DOCE L 215/7, de 25 de agosto de 2000.

ejercido por estas autoridades se produzca de manera eficaz e independiente, destacando la importancia que la nueva normativa en materia de protección de datos personales atribuye a este aspecto, como bien se ha puesto de relieve de forma reiterada en distintas decisiones de adecuación aprobadas y en los dictámenes del Grupo de Trabajo del Artículo 29¹¹. Ello está alineado, de manera clara, con lo dispuesto en el art. 8.3 de la Carta de los Derechos Fundamentales de la Unión Europea¹², que establece la obligación de que exista una autoridad de control independiente que pueda garantizar de manera eficaz el derecho fundamental a la protección de datos, haciendo que el principio de control independiente se erija como uno de los más importantes en la configuración de este derecho fundamental.

c) Concurrencia de compromisos que, a nivel internacional, sean asumidos por el tercer país, territorio u organización internacional, especialmente en materia de protección de datos personales [letra c) del art. 45.2 RGPD]. Especial importancia adquiere, entre estos compromisos internacionales, la adhesión al Convenio del Consejo de Europa, de 28 de enero de 1981¹³, como bien pone de manifiesto el considerando 105 RGPD.

Una vez remitido el dictamen por parte del CEPD y del Parlamento Europeo, la Comisión procederá a la adopción de una decisión de adecuación, de conformidad con lo dispuesto por el art. 45.3 RGPD. Este acto de ejecución deberá establecer un mecanismo de revisión regular, como mínimo cada cuatro años, que considere todos aquellos acontecimientos importantes sucedidos a lo largo de ese intervalo de tiempo en el territorio de que se trate, especificando su ámbito de aplicación territorial y sectorial y determinando, en su caso, la autoridad de control o autoridades de control a que alude la letra b) del art. 45.2 RGPD. Por su parte, el art. 97 del Reglamento general de protección de datos establece que, a más tardar el 25 de mayo del año 2020 y, con posterioridad, cada cuatro años, la Comisión deberá presentar al Parlamento Europeo y al Consejo un informe relativo a la evaluación y revisión del RGPD, incluyendo un examen de esta aplicación y del funcionamiento del capítulo V, en especial en relación con las decisiones de adecuación llevadas a cabo en virtud del art. 45.3 RGPD.

Por último, el apartado octavo del art. 45 RGPD establece la obligación de la Comisión de publicar, en el DOUE y en su página web, una enumeración de aquellos terceros países, territorios o sectores específicos en relación con los cuales se haya adoptado una decisión de adecuación, afirmando que los mismos ofrecen, o ya no, el nivel de protección adecuado requerido.

11 Entre otras, Guidelines on Article 49 of Regulation 2016/679, de 06 de febrero de 2018.

12 DOCE C 364/I, de 18 de diciembre de 2000.

13 En nuestro país, BOE núm. 274, de 15 de noviembre de 1985.

Una vez obtenida la decisión de ejecución, uno de los aspectos más relevantes radica en que la transferencia internacional de datos personales que se realice no conllevará la necesidad de obtener ninguna autorización específica, tal y como establece el art. 45.1 RGPD. En este sentido, las transferencias internacionales de datos personales se asemejan a los tratamientos transfronterizos, cuya definición se contiene en el art. 4.23) RGPD.

Por lo demás, a pesar de que la finalidad de la decisión de adecuación adoptada por la Comisión es aportar seguridad y uniformidad jurídicas en todo el territorio de la Unión Europea, la realidad es que las autoridades de control de los Estados miembros cuentan con la habilitación necesaria para poder realizar tareas de investigación en orden a determinar si una transferencia realizada con base en una decisión de adecuación es, o no, conforme con la normativa en materia de protección de datos. La razón se encuentra en la sentencia del TJUE de 6 de octubre de 2015, en virtud de la cual se establece la invalidez de la decisión sobre puerto seguro. Esta capacidad investigadora no abarcará, sin embargo, la facultad de no aplicar una decisión de adecuación que resulte puesta en entredicho.

Por otro lado, la decisión de adecuación exige a la Comisión la supervisión constante de aquellas circunstancias que puedan condicionar una aplicación eficaz de dicha decisión (art. 45.4 RGPD)¹⁴. Esta norma únicamente alude a los países terceros y a las organizaciones internacionales, si bien parece obvio que este análisis habrá de abarcar también aquellas áreas concretas en relación con las cuales se haya reconocido la adecuación en cuestión¹⁵.

14 RECUERO LINARES, M.: "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*, núm. Extra I, 2019, pp. 424-427.

15 Para concluir, resulta importante aludir a un hecho, cual es que, tras la sentencia del TJUE de 6 de octubre del año 2015, la Comisión ha procedido a aprobar la Decisión de Ejecución (UE) 2016/2295 de la Comisión de 16 de diciembre de 2016 en virtud de la cual se produce la modificación de las Decisiones 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/C, 2010/146/UE, 2010/625/UE, 2011/61/UE y las Decisiones de Ejecución 2012/484/UE y 2013/65/UE, relativas a la protección adecuada de los datos personales por determinados países, en aplicación del art. 25, apartado 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo (DOUE L 344/83, de 17 de diciembre de 2016), sobre la protección adecuada de los datos personales por parte de determinados países, en aplicación del apartado sexto del art. 25 DPDP. Esta Decisión establece, con carácter fundamental, dos aspectos relacionados con las decisiones de adecuación que han sido objeto de aprobación: a) de una parte, han de precisar con claridad que, teniendo en cuenta que las mismas establecen un límite de las facultades que corresponden a las autoridades nacionales de supervisión equiparable a la establecida en la decisión de Puerto Seguro, anulada posteriormente por el Tribunal, ha de procederse a una modificación dirigida a eliminar estas limitaciones; b) de otra, como consecuencia de la precitada sentencia del TJUE, la Comisión habrá de realizar un seguimiento constante, tanto legislativamente como en la práctica, de aquellas modificaciones que pudieran influir en el correcto funcionamiento de las decisiones de adecuación, en especial de la evolución de aquellas normas que disciplinan el acceso a los datos personales por parte de las autoridades públicas.

2. Transferencias efectuadas mediante la prestación de garantías adecuadas.

La normativa precedente pivotaba sobre la base de la existencia de una decisión de adecuación como presupuesto legal jurídicamente habilitante para poder realizar transferencias internacionales de datos personales. La regulación actual sobre protección de datos refuerza estas transferencias internacionales por medio de la introducción de una nueva vía que, en defecto de la decisión de adecuación antes aludida, permitiría a responsables y encargados del tratamiento transferir datos personales a terceros países u organizaciones internacionales por medio de la prestación de garantías adecuadas que, en esa normativa anterior, tan sólo eran consideradas como una excepción a la regla general, dentro del apartado segundo del art. 26 DPDP.

Así las cosas, y de acuerdo con el art. 46.I RGPD, a falta de una decisión de adecuación por parte de la Comisión, el responsable o el encargado del tratamiento únicamente podrán realizar transferencias internacionales de datos personales en el supuesto de que hayan ofrecido determinadas garantías que resulten suficientes y siempre que las personas físicas titulares de los datos personales cuenten con derechos exigibles y acciones legales efectivas¹⁶. En este sentido, la existencia de garantías adecuadas se erige en el único presupuesto general que, juntamente con la existencia de decisiones de adecuación, ampara la realización de transferencias de datos personales a terceros países u organizaciones internacionales, de modo que el resto de los supuestos constituirían ya excepciones a ambas reglas generales. Además, con independencia de qué garantías sean prestadas, se exige que estas sean eficaces y efectivas para los interesados, ya que estos han de verse respaldados, en todo momento, repetimos, por derechos exigibles y acciones legales efectivas.

Por lo demás, el art. 15.2, al igual que los art. 13.1.f) y 14.1.f), todos ellos del RGPD, al regular el derecho de acceso y el derecho de información con que cuenta el interesado, respectivamente, establecen la necesidad de que, en el supuesto de que se realicen transferencias internacionales de datos personales, el interesado que ejercite este derecho o que tenga derecho a ser informado, respectivamente, tendrá que ser informado de todas aquellas garantías que resulten adecuadas, al amparo del precitado art. 46 del Reglamento general de protección de datos.

En definitiva, las garantías adecuadas permiten hacer lícita la realización de transferencias internacionales cuando no exista una decisión de adecuación por parte de la Comisión (incluidas las aprobadas con base en la DPDP) o en aquellos

16 ÁLVAREZ RIGAUDIAS, C.: "Condiciones para las transferencias internacionales de datos personales en servicios de cloud", en AA. VV. *Derecho y cloud computing* (dir. por R. MARTÍNEZ MARTÍNEZ), Aranzadi, Cizur Menor, 2017, pp. 130-133.

supuestos en que no concurra ninguna de las excepciones previstas en el art. 49 RGPD.

La nueva normativa comunitaria distingue dos grupos claramente diferenciados de garantías que pudieran resultar adecuadas: a) aquellas que no exigen de autorización y b) aquellas que sí la requieren. En concreto, el art. 46.2 RGPD establece que las garantías adecuadas podrán ser susceptibles de aportación, sin necesidad de requerir autorización específica alguna por parte de la autoridad de control, a través de alguno de los siguientes medios:

a) Instrumentos que sean jurídicamente vinculantes y que puedan exigirse entre autoridades u organismos de naturaleza pública. En este sentido, las transferencias internacionales de datos entre autoridades u organismos públicos pueden ser lícitas sin la autorización de la autoridad de control sobre la base de la existencia de disposiciones que se incorporen a acuerdos de carácter administrativo, tales como un memorando de entendimiento, y que establezcan el reconocimiento de derechos exigibles y eficaces a las personas físicas titulares de los datos personales. Si estas garantías adecuadas se incorporan en acuerdos de carácter administrativo que no son jurídicamente vinculantes, se habrá de obtener una autorización por parte de la autoridad de control competente (considerando 108 RGPD), que aplicará el mecanismo de coherencia al amparo de lo dispuesto por el art. 46.4 RGPD (art. 46.3 RGPD).

b) Normas corporativas vinculantes, que, por su relevancia, desarrollaremos de manera detallada más adelante.

c) Cláusulas tipo en materia de protección de datos personales que sean adoptadas por la Comisión. Las cláusulas tipo pretenden tener una importancia ciertamente relevante con la nueva normativa en materia de protección de datos, equiparable a la que han tenido en el pasado. Estas cláusulas podrán ser adoptadas por parte de la Comisión o, como veremos en el siguiente supuesto, por una autoridad de control, o incorporadas por las partes y, con carácter posterior, autorizadas por una autoridad de control (aplicando, en este último supuesto, el mecanismo de coherencia del art. 46.4 RGPD).

Estas garantías apropiadas habrán de garantizar el cumplimiento y la satisfacción de las exigencias en materia de protección de datos personales y de los derechos que corresponden a los interesados, lo que supone la inclusión del derecho a obtener una reparación de carácter administrativo o judicial eficaz y a ejercer la reclamación de una indemnización, dentro de la Unión Europea o en

un país tercero¹⁷. En especial, habrán de aludir a la satisfacción de los principios generales relativos al tratamiento de los datos personales y a aquellos principios de protección de los datos desde el diseño y por defecto, recogidos en los arts. 5 y 25 RGPD, respectivamente (considerando 108 RGPD).

d) Cláusulas tipo en materia de protección de datos adoptadas, en este caso, por parte de una autoridad de control, siendo aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere el art. 93.2 RGPD.

e) Códigos de conducta, juntamente con compromisos de carácter vinculante y exigible por el responsable o por el encargado del tratamiento, en el tercer país, de aplicar garantías adecuadas, incluyendo aquí aquellas que se refieren a los derechos que corresponden a los interesados.

f) Mecanismos de certificación, además de compromisos vinculantes y exigibles, del mismo modo que los códigos de conducta establecidos en la letra anterior.

Por otro lado, el art. 46.3 RGPD establece que, siempre que se cuente con la autorización emitida por la autoridad de control competente, las garantías adecuadas también podrán ser aportadas, en su caso, por medio de:

a) Cláusulas contractuales celebradas entre el responsable o el encargado del tratamiento y el responsable del tratamiento, el encargado del tratamiento o el destinatario de los datos personales establecidos en un tercer país u organización internacional.

b) Disposiciones que sean incorporadas en acuerdos de carácter administrativo, suscritas entre las autoridades u organismos de naturaleza pública que reconozcan derechos efectivos y exigibles para las personas físicas titulares de los datos.

Un aspecto fundamental dentro de estas garantías viene constituido, como anticipábamos, por las normas corporativas vinculantes (también conocidas, en inglés, como *Binding Corporate Rules* -BCR-), que constituyen una de las más relevantes novedades aportadas por la regulación actual sobre protección de datos y que quedan recogidas dentro del art. 47 RGPD.

En este sentido, el art. 4.20) RGPD entiende por normas corporativas vinculantes aquellas 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 conjunto de transferencias de datos

17 SÁNCHEZ DOMINGO, M. B.: "La transferencia de datos personales a terceros países y organizaciones internacionales según la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016", en AA.VV.: *Los avances del espacio de Libertad, Seguridad y Justicia de la UE en 2017: II Anuario ReDPE* (coord. por M. Á. GUTIÉRREZ ZARZA), Wolters Kluwer, Madrid, 2018, p. 171.

personales a un responsable o encargado del tratamiento en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta. La definición proporcionada por el art. 4 RGPD y la configuración de su regulación son el resultado de un proceso evolutivo a que se han visto expuestas estas normas corporativas vinculantes desde hace, aproximadamente, quince años, momento en el que comenzó a abordarse esta cuestión, especialmente por parte del Grupo de Trabajo del Artículo 29, cuya gran labor ha sido puesta de manifiesto en una serie de documentos de gran interés para un examen pormenorizado de esta cuestión¹⁸. Así las cosas, la normativa actual sobre protección de datos recoge el resultado de un intento por regular de forma eficaz aquellas transferencias internacionales realizadas en el contexto de grandes multinacionales o de grupos de empresas [entendido este, de acuerdo con el art. 4.19) RGPD, como aquel grupo constituido por una empresa que ejerce el control y sus empresas controladas], facilitando su articulación, siempre con la garantía del respeto del derecho fundamental a la protección de datos personales¹⁹.

En este sentido, conviene recordar la regulación proporcionada por el derogado RDLOPD, que ya incorporó una primera alusión específica a las normas corporativas vinculantes dentro de su art. 70.4. En cualquier caso, resulta evidente que estas normas corporativas vinculantes constituyen, en la actualidad, una herramienta cada vez más empleada, aspecto este que está llamado a consolidarse en el futuro.

Dada la configuración de las normas corporativas vinculantes como fuente de obligaciones para los responsables y encargados del tratamiento, se analiza su carácter vinculante en cuanto declaración unilateral de voluntad²⁰. En este sentido, las posibles dudas que pudieran suscitarse, teniendo en cuenta el sistema configurado por el Código Civil²¹, han de considerarse eliminadas en la actualidad, por cuanto que las normas corporativas vinculantes encuentran regulación específica en una norma jurídica de aplicación directa en los Estados miembros, como es el Reglamento general de protección de datos; ello pone de manifiesto, una vez más, el alcance que presenta la normativa actual en materia de protección de datos personales en nuestro ordenamiento jurídico.

18 En especial, ARTICLE 29 DATA PROTECTION WORKING PARTY: *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, de 28 de noviembre de 2017.

19 GUASH PORTAS, V.: "La computación en nube y las transferencias internacionales de datos en el nuevo reglamento de la UE", *RDUNED. Revista de derecho UNED*, núm. 20, 2017, pp. 340-342.

20 ORTEGA GIMÉNEZ, A.: "El impacto del Reglamento General de Protección de Datos de la Unión Europea y de la LOPDGD en el régimen jurídico de las transferencias internacionales de datos de carácter personal", en AA.VV.: *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (dir. por R. GARCÍA MAHAMUT y B. TOMÁS MALLÉN), Tirant lo Blanch, Valencia, 2019, p. 401; PIÑAR MAÑAS, J. L.: "Transferencias de datos personales a terceros países u organizaciones internacionales", en AA.VV.: *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (dir. por J. L. PIÑAR MAÑAS), Reus, Madrid, 2016, pp. 446-448.

21 Gaceta de Madrid núm. 206, de 25 de julio de 1889.

No obstante, teniendo en cuenta la controversia que estas normas corporativas vinculantes pueden suponer en los sistemas jurídicos continentales, la nueva normativa sobre la materia establece una regulación pormenorizada con la finalidad principal de proteger el carácter vinculante y garantista de los BCR. En esta línea, el art. 47.I RGPD parte de los requisitos que habrán de reunir estas normas corporativas vinculantes; así, dispone, la autoridad de control competente deberá aprobar estas normas de acuerdo con el mecanismo de coherencia regulado en el art. 63 RGPD, siempre que las mismas:

1) Sean jurídicamente vinculantes y cumplidas por parte de todos los que integran el grupo empresarial o la unión de empresas que se dedican a una actividad económica conjunta, incluyendo también a sus empleados.

2) Confieran a los interesados, de modo expreso, derechos exigibles en relación con el tratamiento que se realice de sus datos personales.

3) Satisfagan las exigencias comprendidas en el art. 47.2 RGPD.

Este apartado segundo del art. 47 RGPD establece el contenido mínimo que habrán de incluir los *Binding Corporate Rules*. Es este un apartado extenso que viene a integrar aquello que el Grupo de Trabajo del Artículo 29 venía reivindicando desde el año 2003. Como en otros casos, se advierte la intención del legislador comunitario de poner de manifiesto que las normas corporativas vinculantes son, en esencia, herramientas que permiten proteger el derecho fundamental a la protección de datos personales en un contexto complejo, como es el propio en el que estas han de ser aplicadas, con multitud de transferencias de datos personales a terceros países y/u organizaciones internacionales de naturaleza muy heterogénea y de distintos territorios. Así las cosas, el art. 47.2 RGPD incluye el contenido mínimo que habrá de ser especificado en las normas corporativas vinculantes que resulten afectadas:

a) La descripción de la estructura presentada por el grupo empresarial o unión de empresas que se dediquen a una actividad económica conjunta, así como los datos de contacto de cada uno de sus integrantes.

b) Las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus finalidades, el tipo de interesados que resulten afectados por dicho tratamiento y el nombre del tercer país o de los terceros países de que se trate.

c) El carácter jurídicamente vinculante de las normas corporativas vinculantes, tanto a nivel interno como externo.

d) El cumplimiento de los principios rectores del tratamiento de los datos personales, tales como el principio de limitación de la finalidad, el de minimización de datos, el de limitación de los plazos de conservación, el de calidad de los datos, el de protección de datos desde el diseño y por defecto, la base jurídica del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos personales y las exigencias en relación con la realización de transferencias internacionales de datos realizadas con posterioridad a organismos no vinculados por los BCR.

e) Los derechos que corresponden a los interesados en relación con el tratamiento realizado por responsables o encargados del tratamiento y los medios de que disponen para poder ejercerlos, en especial el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles, de acuerdo con lo establecido por el art. 22 RGPD, el derecho a presentar una reclamación ante la autoridad de control competente y ante los Tribunales competentes de los Estados miembros de acuerdo con el art. 79 RGPD y el derecho a obtener una reparación y, cuando proceda, una indemnización derivada de una violación de las normas corporativas vinculantes.

f) La aceptación, por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro, de la responsabilidad en el caso de cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión Europea. En este caso, el responsable o el encargado del tratamiento únicamente se verán exonerados de dicha responsabilidad, de un modo total o parcial, si demuestran que el acto que motivó los daños y perjuicios no resulta imputable a ese miembro.

g) El modo en que se proporciona a los interesados una adecuada información en relación con las normas corporativas vinculantes, en especial en lo relativo a las disposiciones contempladas en las letras d), e) y f) del presente art. 47.2 RGPD, amén de los preceptos 13 y 14 de la misma norma.

h) Las funciones a desempeñar por el delegado de protección de datos que sea nombrado de acuerdo con el art. 37 RGPD (y, en nuestro país, además, de conformidad con el art. 34 LOPDGDD) o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones.

i) Los procedimientos elaborados para el ejercicio de reclamaciones.

j) Los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos deberán incluir la realización de auditorías de protección de datos y métodos para garantizar acciones correctivas con el fin de proteger los derechos de los interesados. Los resultados de esta verificación habrán de ser comunicados a la persona o entidad a que se refiere la letra h) anterior y al Consejo de Administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite.

k) Los mecanismos establecidos para poder realizar la comunicación y registro de las modificaciones introducidas en las normas, así como para la notificación de cada una de esas modificaciones a la autoridad de control.

l) El mecanismo de cooperación con la autoridad de control, con el fin de garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en especial poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j) anteriormente descrita.

m) Los mecanismos para poder informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un tercer país o a un miembro del grupo empresarial o de la unión de empresas, que, con probabilidad, tengan un efecto adverso en relación con las garantías que se hayan establecido en las normas corporativas vinculantes.

n) La formación en materia de protección de datos personales necesaria para el personal que tenga acceso permanente o habitual a los datos personales.

3. Transferencias específicas y excepcionales.

Por último, el art. 49 RGPD regula aquellas excepciones que, plasmadas en situaciones específicas, permiten la realización de transferencias de datos personales a terceros países u organizaciones internacionales²². Estas excepciones han sido objeto de interpretación por parte del Grupo de Trabajo del Artículo 29 en dos documentos relevantes: en primer lugar, el documento de trabajo sobre “Transferencias de datos personales a terceros países: aplicación de los arts. 25 y 26 de la directiva sobre protección de datos en la UE” (WP 12), objeto de adopción con fecha de 24 de julio de 1998; en segundo lugar, el “Documento de trabajo relativo a una interpretación común del artículo 26, apartado uno, de

22 Para un mayor entendimiento de esta última vía contemplada por el RGPD, *vid.* Directrices 2/2018 del CEPD sobre las excepciones a lo dispuesto en el art. 49 del Reglamento (UE) 2016/679.

la Directiva 95/46/CE de 24 de octubre de 1995" (WP 114), adoptado el 25 de noviembre de 2005.

Estas excepciones hacen posible la realización de transferencias internacionales de datos personales sin la necesidad de obtener autorización alguna por parte de la autoridad de control. No obstante, el responsable o el encargado del tratamiento habrán de configurar determinadas soluciones que hagan posible a los interesados el ejercicio de derechos exigibles y efectivos en relación con el tratamiento de sus datos personales dentro del territorio comunitario y una vez tenga lugar la transferencia, de tal modo que, como bien establece el considerando 114 RGPD, puedan seguir contando en todo momento con derechos fundamentales y garantías efectivas.

En este sentido, y atendiendo al art. 49.1.1º RGPD, podemos subrayar las siguientes modificaciones que, en este contexto, se han producido respecto de la normativa inmediatamente precedente:

a) Por lo que respecta al consentimiento del interesado, se exige que este sea específico y no sólo inequívoco. También que el interesado sea debidamente informado de todos aquellos riesgos que, con probabilidad, puedan afectarle en el caso de realización de estas transferencias internacionales de sus datos personales en ausencia de una decisión de adecuación y de garantías adecuadas, establecidas en los arts. 45 y 46 RGPD, respectivamente [letra a) del art. 49.1 RGPD].

b) En aquellos casos en que la realización de la transferencia internacional de datos personales venga impuesta por razones importantes de interés público, este interés habrá de ser reconocido por la normativa comunitaria o por el Derecho interno de los Estados miembros que resulte de aplicación al responsable del tratamiento (art. 49.4 RGPD).

c) A la excepción consistente en la existencia de un interés vital del interesado, se incluye aquella otra excepción basada en la existencia de un interés vital en relación con otras personas, si bien se establece la necesidad de que el interesado esté física o jurídicamente incapacitado para prestar su consentimiento²³ [letra f) del art. 49.1 RGPD].

d) En el caso de que la realización de la transferencia internacional se produzca desde un registro público, se especifica, en la actualidad, que dicha transferencia no comprenderá todos los datos personales ni categorías enteras de datos personales contenidos en dicho registro. Además, si la finalidad del registro consiste en la consulta por parte de personas que tengan un interés legítimo, la transferencia

23 Sobre esta cuestión, y para más detalle con motivo de la crisis sanitaria actual derivada del COVID-19, *vid.* RODRÍGUEZ AYUSO, J. F.: *Privacidad y Coronavirus*, Dykinson, Madrid, 2020, pp. 59-60.

internacional sólo podrá efectuarse con la solicitud de estas personas o si las mismas hubieran de ser las destinatarias (art. 49.2 RGPD).

e) El responsable o el encargado del tratamiento deberán documentar en los registros de actividades de tratamiento del art. 30 RGPD la evaluación y las garantías adecuadas a que alude, como veremos a continuación, el art. 49.1.2° RGPD (art. 49.6 RGPD).

En principio, el conjunto de excepciones contempladas en el art. 49 RGPD es cerrado o *numerus clausus*, de modo que no será posible la aplicación de cualquier otra excepción adicional mediante aplicación analógica. Ahora bien, sucede que algunas de estas excepciones son, en exceso, amplias, y que el art. 49.1, *in fine*, RGPD permite la realización de transferencias internacionales cuando no resulte de aplicación ninguna de las excepciones contenidas en dicho apartado, bajo la condición de que estas transferencias se realicen dentro de los límites y bajo las condiciones que el art. 49.1.2° RGPD contempla:

- a) Que no sean repetitivas,
- b) Que afecten únicamente a un número reducido de interesados.
- c) Que sean imprescindibles a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses, derechos y libertades del interesado.
- d) Que el responsable del tratamiento haya realizado una evaluación previa de todas las circunstancias que concurran en esta transferencia internacional de datos y, con base en este análisis, ofrezca garantías adecuadas con respecto a la protección de los datos personales de los interesados.

Por lo demás, el responsable del tratamiento deberá informar a la autoridad de control de la transferencia internacional, así como al interesado (a este último no sólo de la transferencia, sino también de los intereses legítimos imperiosos perseguidos).

Para concluir, pese a que el art. 49 RGPD alude, en general, a las excepciones que legitimarían la realización de transferencias internacionales de datos personales aun cuando no contarán con una decisión de adecuación o, en su defecto, con la existencia de garantías adecuadas, su apartado quinto comprende una situación que resulta ser la contraria: cuando no exista una decisión en virtud de la cual se constate la adecuación de la protección de los datos personales, el Derecho comunitario o el Derecho interno de los Estados miembros podrá, basándose en la existencia de razones importantes de interés público, establecer, de modo

expreso, limitaciones a la realización de transferencias internacionales de categorías especiales de datos personales a un tercer país u organización internacional. Además, en estos casos, los Estados miembros deberán notificar a la Comisión estas disposiciones.

Al hilo de cuanto se ha expuesto, y por lo que respecta a la situación existente dentro del ordenamiento jurídico español, el art. 43 LOPDGDD regula los supuestos sometidos a información previa a la autoridad de protección de datos competente. En este caso, dispone el precepto, los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos por ellos perseguidos y la concurrencia del resto de los requisitos previstos en el art. 49.1.2º RGPD; asimismo, deberán informar a los afectados, tanto de la transferencia como de los intereses legítimos imperiosos perseguidos. Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

III. TRANSFERENCIAS INTERNACIONALES DE DATOS A ESTADOS UNIDOS TRAS LA ANULACIÓN DEL ESCUDO DE PRIVACIDAD: INTERROGANTES Y ALTERNATIVAS.

Con fecha de 16 de julio del presente año, el TJUE ha publicado una Sentencia²⁴ por la cual invalida la Decisión de Ejecución 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.²⁵

Merced a esta Decisión, se habilitaba la realización de transferencias internacionales procedentes de cualquier Estado miembro del EEE a Estados Unidos, siempre que la entidad receptora (importadora de los datos personales) estuviera adherida a un sistema de control denominado “Escudo de privacidad” (también conocido, en inglés, como *Privacy Shield*), considerando esta adhesión suficiente como para establecer la presunción de que garantizaba un nivel de protección adecuado y acorde al exigido en el territorio de la Unión Europea. Dotado de más amplias garantías en relación con la información personal de los individuos en el ámbito de las relaciones transatlánticas que el sistema precedente²⁶, se subsanaba el problema, originado años atrás, cuando el TJUE, al

24 Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020. Asunto C-311/18, Data Protection Commissioner contra Facebook Ireland Ltd y Maximilian Schrems.

25 DOUE L 207/I, de 1 de agosto de 2016.

26 LÓPEZ AGUILAR, J. F.: “La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del Derecho europeo, y su impacto en la relación

igual que sucede ahora, anuló el esquema de transferencias internacionales hasta entonces vigente, conocido como “Puerto Seguro”²⁷ (o, lo que es lo mismo, *Safe Harbor*), una vez interpuesta la reclamación del ciudadano austríaco Maximilian Schrems frente a Facebook, sobre la base de que los datos transferidos desde la Unión Europea a Norteamérica carecían de la seguridad necesaria por ser accesibles al gobierno y a las agencias de seguridad de este país sin respetar las garantías y los derechos fundamentales reconocidos por la normativa comunitaria a sus ciudadanos, como es, en esencia, el derecho a la privacidad y a la protección de sus datos personales²⁸; de hecho, la motivación de esta última anulación reside en una nueva reclamación del Sr. Schrems (de ahí el nombre de esta sentencia, conocida como “Schrems II”), argumentando que tampoco con la nueva fórmula emanada del Escudo de privacidad se respetaban sus derechos fundamentales, lo que provocó que Irlanda volviera a plantear una cuestión prejudicial al TJUE y que desembocó en el resultado ya conocido.

Al igual que sucedió entonces, la nueva situación propiciada por la anulación del Escudo de privacidad obliga a la búsqueda de alternativas que permitan la realización de transferencias internacionales a Estados Unidos de forma acorde con las salvaguardas impuestas por el Reglamento general de protección de datos. A priori, la solución más factible reside en el empleo de las ya conocidas cláusulas contractuales tipo (CCT) elaboradas por la Comisión Europea; más

transatlántica UE-EEUU”, en AA.VV.: *Teoría y realidad constitucional*, UNED, Madrid, 2017, p. 563.

27 En concreto, en su sentencia de fecha 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), el TJUE invalidó la Decisión 2000/520/CE, en la que la Comisión había declarado que ese país tercero garantizaba un nivel adecuado de protección.

A raíz de esta sentencia, y como bien indica la Sentencia de 16 de julio de 2000 (p. 19), la Comisión adoptó la Decisión, «[...] tras haber procedido, a efectos de su adopción, a una evaluación de la normativa de los Estados Unidos, como se precisa en el considerando 65 de la antedicha Decisión:

“La Comisión ha evaluado las limitaciones y salvaguardias existentes en el Derecho de los Estados Unidos con respecto al acceso a los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. y la utilización de los mismos por los poderes públicos estadounidenses a efectos de seguridad nacional, aplicación de la ley y otros fines de interés público. Asimismo, el Gobierno estadounidense, a través de su Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) [...], ha proporcionado a la Comisión una serie de declaraciones y compromisos detallados que se exponen en el anexo VI de la presente Decisión. Mediante carta firmada por el secretario de Estado y adjunta como anexo III a la presente Decisión, el Gobierno de los Estados Unidos se ha comprometido asimismo a crear un nuevo mecanismo de supervisión de las injerencias con fines de seguridad nacional, a saber, el Defensor del Pueblo en el ámbito del Escudo de la privacidad, que será independiente de los servicios de inteligencia. Por último, la declaración del Departamento de Justicia de los Estados Unidos contenida en el anexo VII de la presente Decisión describe las limitaciones y salvaguardias aplicables al acceso a los datos y a su utilización por parte de los poderes públicos a efectos de aplicación de la ley y otros fines de interés público. Con vistas a mejorar la transparencia y reflejar la naturaleza jurídica de estos compromisos, cada uno de los documentos enumerados y adjuntos a la presente Decisión se publicará en el Registro Federal de los Estados Unidos”».

28 Sobre esta cuestión, vid. BIURRUN ABAD, F. J.: “Primera evaluación a la vista del ‘Privacy Shield’”, *Actualidad jurídica Aranzadi*, núm. 932, 2017, p. 28; GÓMEZ SANTOS, M.: “Del puerto seguro al ‘privacy shield’: las transferencias de datos de carácter personal entre la Unión Europea y los Estados Unidos a examen”, en AA.VV.: *Reflexiones sobre Derecho privado patrimonial* (dir. por A. ÁVILA DE LA TORRE), Ratio Legis, Salamanca, 2017, pp. 252-255; LÓPEZ-LAPUENTE GUTIÉRREZ, L.: “La transferencia de datos a EEUU: la transición del Safe Harbor al Privacy Shield y un paso más allá”, *Actualidad jurídica Uriá Menéndez*, núm. 45, 2017, pp. 36-38; ORTEGA GIMÉNEZ, A.: “Transferencia internacional de datos personales: del Safe Harbor al Privacy Shield”, *Revista Lex Mercatoria*, núm. 4, 2016, pp. 85-90.

concretamente, de aquellas recogidas en la Decisión de la Comisión 2010/87/UE 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 Consejo²⁹, cuya validez ha sido ratificada, eso sí, por la reciente STJUE. Todo ello sin obviar la posibilidad de acudir, dentro también de la segunda vía habilitada por el RGPD, a la utilización de normas corporativas vinculantes cuando el exportador y el importador de los datos objeto de protección formen parte de lo que se conoce como “grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta”.

Empero, cualquiera de los escenarios presentes plantea una serie de dificultades en nada desdeñables. En efecto, la sencillez y fluidez en que consiste la habilitación legal prevista en el art. 45 RGPD, una vez superados los análisis previos y procedentes por parte de la Comisión para efectuar la declaración de adecuación o la presunción *iuris tantum* en que se traducía la incorporación de una entidad en el listado del *Privacy Shield*, en nada es comparable con la ardua tarea de elaborar, adaptar y revisar de forma periódica tales cláusulas contractuales tipo en relación con cada uno de los importadores que hayan de recibir tales datos. Y todo ello por no mencionar el desplazamiento de la responsabilidad que se produce con la irrupción, en este nuevo contexto, del art. 46 RGPD hacia el responsable del tratamiento o exportador de los datos, quien deberá (adicionado, además, con el reforzamiento del prisma de la *accountability* al amparo de la nueva regulación en materia de privacidad) establecer las garantías adecuadas para que las transferencias no supongan menoscabo alguno de los derechos que corresponden al interesado en cuanto titular de los datos personales tratados, como bien señala el TJUE y reitera el CEPD, estableciendo que es necesario³⁰:

«[...] incluir mecanismos eficaces que permitan garantizar en la práctica que el nivel de protección exigido por el Derecho de la Unión sea respetado y que las transferencias de datos personales basadas en estas cláusulas sean suspendidas o prohibidas en caso de que se incumplan dichas cláusulas o de que resulte imposible cumplirlas»,

de forma que,

«[...] la posibilidad de transferir datos personales [...] dependerá del resultado de su evaluación, teniendo en cuenta las circunstancias de las transferencias y las medidas complementarias que haya podido aplicar. Las medidas complementarias,

29 DOUE L 39/5, de 12 de febrero de 2010.

30 Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 — Comisaria de Protección de Datos vs Facebook Irlanda y Maximilian Schrems. Adoptada el 23 de julio de 2020 (pp. 1 y 3).

junto con las CCT, tras un análisis caso por caso de las circunstancias de la transferencia, tendrían que garantizar que la legislación estadounidense no afecte al nivel de protección adecuado que garantizan».

Si, tras esta labor, llega a la conclusión de que, considerando las circunstancias propias y singulares de la transferencia y las posibles medidas complementarias, no se aplicarían las garantías adecuadas, el exportador de los datos deberá proceder a la suspensión o finalización de la transferencia de datos personales. Ahora bien, si, pese a este resultado, desea seguir transfiriendo datos, deberá notificarlo a la autoridad de control³¹ que resulte competente al respecto³².

Una tercera posibilidad de las previstas legalmente, bien es cierto que subsidiaria respecto de las dos *supra* indicadas, vendrá proporcionada por el art. 49 RGPD, si bien, como ya se indicó en párrafos anteriores, deberán cumplir una serie de exigencias ciertamente singulares, de entre las cuales el CEPD destaca, por su relevancia y en términos literales, las que se siguen³³:

«[...] cuando las transferencias se basen en el consentimiento del titular de los datos, deberán ser:

- explícitas;

- específicas para la transferencia o conjunto de transferencias de datos concreta (lo que significa que el exportador de los datos debe asegurarse de obtener una autorización específica antes de que se ponga en marcha la transferencia, incluso si esto ocurre después de efectuarse la recogida de los datos); e

31 Para un estudio pormenorizado de las funciones, poderes y competencias de la autoridad de control, *vid.* RODRÍGUEZ AYUSO, J. F.: *Control externo de los obligados por el tratamiento de datos personales*, Barcelona, Ed. Bosch, 2020.

32 Al respecto, y en relación con las cláusulas contractuales tipo, *vid.*, en primer lugar, el considerando 145 STUE de 16 de julio; en segundo lugar, la cláusula 4, letra g), de la Decisión 2010/87/UE de la Comisión; en tercer lugar, la cláusula 5, letra a), de la 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 (DOCE L 181/19, de 4 de julio de 2001), y, en cuarto y último lugar, la letra c) del Anexo II de la Decisión 2004/915/CE de la Comisión de 27 de diciembre de 2004 o la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países (DOUE L 385/74, de 29 de diciembre de 2004).

Por su parte, y relacionados con las normas corporativas vinculantes, *vid.*, en primer lugar, el considerando 145 STUE de 16 de julio; en segundo lugar, la cláusula 4, letra g), de la Decisión 2010/87/UE; en tercer lugar, la sección 6.3 del WP256, rev. 01 (Grupo de Trabajo del artículo 29, documento de trabajo que establece un cuadro con los elementos y principios que se recogen en las NCV, refrendado por el CEPD, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109), y, en cuarto y último lugar, la sección 6.3 del WP257, rev.01 (Grupo de trabajo del artículo 29, documento de trabajo que establece un cuadro con los elementos y principios que se recogen en las NCV, refrendado por el CEPD, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

33 Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 — Comisaría de Protección de Datos vs Facebook Irlanda y Maximilian Schrems. Adoptada el 23 de julio de 2020 (p. 4).

- informadas, en particular sobre los posibles riesgos de la transferencia (es decir, que el titular de los datos también debería informar de los riesgos específicos derivados del hecho de que sus datos serán transferidos a un país que no ofrece una protección adecuada y que no se aplican garantías adecuadas destinadas a garantizar la protección de los datos).

Con respecto a las transferencias necesarias para la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento, debe tenerse en cuenta que los datos personales solo podrán transferirse cuando la transferencia sea ocasional. Deberá establecerse caso por caso si las transferencias de datos se determinarían como "ocasionales" o "no ocasionales". En cualquier caso, esta excepción solo podrá invocarse cuando la transferencia sea objetivamente necesaria para la ejecución del contrato.

En relación con las transferencias necesarias por razones importantes de interés público (que deben reconocerse en la legislación de la UE o de los Estados miembros, el CEPD recuerda que el requisito sustancial para la aplicabilidad de esta excepción es la constatación de un interés público importante y no la naturaleza de la organización, y que, aunque esta excepción no se limita a las transferencias de datos que son «ocasionales», esto no significa que las transferencias de datos sobre la base de la excepción por razones importantes de interés público puedan tener lugar a gran escala y de manera sistemática. Por el contrario, debe respetarse el principio general según el cual las excepciones establecidas en el art. 49 del RGPD no deben convertirse en "norma" en la práctica, sino que deben limitarse a situaciones específicas y cada exportador de datos debe garantizar que la transferencia cumpla la prueba de necesidad estricta».

Por último, tampoco se podrá descartar, hasta tanto se proceda (algo que parece probable por el impacto que su ausencia podría conllevar para el sistema económico internacional) a un nuevo acuerdo entre la Unión Europea y Estados Unidos, la suspensión o anulación de los acuerdos actualmente vigentes de prestación de servicios con importadores situados en territorio Norteamericano y su sustitución por otros, igualmente fiables y eficaces, que estén ubicados en el EEE o en países que ofrezcan un nivel de protección adecuado³⁴.

34 Hasta la fecha, los países y territorios que están declarados como adecuados son los siguientes: a) Suiza, merced a la 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 (DOCE L 215/1, de 25 de agosto de 2000); b) Canadá, merced a la 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* (DOCE L 2/13, de 4 de enero de 2002), respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos; c) Argentina, merced a la 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 (DOUE L 168/19, de 5 de julio de 2003); d) Guernsey, merced a la Decisión 2003/821/CE de la Comisión de 21 de noviembre de 2003 relativa al carácter adecuado de la protección de los datos

BIBLIOGRAFÍA

ÁLVAREZ RIGAUDIAS, C.: “Condiciones para las transferencias internacionales de datos personales en servicios de cloud”, en AA. VV. *Derecho y cloud computing* (dir. por R. MARTÍNEZ MARTÍNEZ), Aranzadi, Cizur Menor, 2017.

ARTICLE 29 DATA PROTECTION WORKING PARTY: *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, de 28/11/2017.

BIURRUN ABAD, F. J.: “Primera evaluación a la vista del ‘Privacy Shield’”, *Actualidad jurídica Aranzadi*, núm. 932, 2017.

CERVERA NAVAS, L.: “El Comité Europeo de Protección de Datos”, en AA.VV.: *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (coord. A. RALLO LOMBARTE), Tirant lo Blanch, Valencia, 2019.

CORDERO ÁLVAREZ, C. I.: “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*, núm. 70, 2019.

EDUARDO USTARAN, P. G.: “Transferencias internacionales de datos”, en AA.VV.: *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (coord. por A. RALLO LOMBARTE), Tirant lo Blanch, Valencia, 2019.

personales en Guernsey (DOUE L 308/27, de 25 de noviembre de 2003); e) Isla de Man, merced a la 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 (DOUE L 151/52, de 30 de abril de 2004); f) Jersey, merced a la Decisión 2008/393/CE de la Comisión de 8 de mayo 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 (DOUE L 138/21, de 28 de mayo de 2008); g) Islas Feroe, merced a la 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 (DOUE L 58/17, de 9 de marzo de 2010); h) Andorra, merced a la 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 (DOUE L 277/27, de 21 de octubre de 2010); i) Israel, merced a la 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 (DOUE L 27/39, 1 de febrero de 2011); j) Uruguay, merced a la Decisión 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 (DOUE L 227/11, de 23 de agosto de 2012); k) Nueva Zelanda, merced a la Decisión 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 (DOUE L 28/12, de 30 de enero de 2013), y l) Japón, merced a la Decisión de 23 de enero de 2019.

EUROPEAN DATA PROTECTION BOARD: "The transfer of personal data to third countries and international organisations by EU institution and bodies", *Position paper*, 2014.

GÓMEZ SANTOS, M.: "Del puerto seguro al 'privacy shield': las transferencias de datos de carácter personal entre la Unión Europea y los Estados Unidos a examen", en AA.VV.: *Reflexiones sobre Derecho privado patrimonial* (dir. por A. ÁVILA DE LA TORRE), Ratio Legis, Salamanca, 2017.

GUASH PORTAS, V.: "La computación en nube y las transferencias internacionales de datos en el nuevo reglamento de la UE", *RDUNED. Revista de derecho UNED*, núm. 20, 2017.

LÓPEZ AGUILAR, J. F.: "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del Derecho europeo, y su impacto en la relación transatlántica UE-EEUU", en AA.VV.: *Teoría y realidad constitucional*, UNED, Madrid, 2017.

LÓPEZ CALVO, J.: "Transferencia de Datos Personales a terceros países y organizaciones internacionales (Arts. 44-50 RGPD. Arts. 40-43 y Disposición adicional quinta y decimotercera LOPDGDD)", en AA.VV.: *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (coord. por J. LÓPEZ CALVO), Wolters Kluwer, Madrid, 2019.

LÓPEZ-LAPUENTE GUTIÉRREZ, L.: "La transferencia de datos a EEUU: la transición del Safe Harbor al Privacy Shield y un paso más allá", *Actualidad jurídica Uría Menéndez*, núm. 45, 2017.

ORTEGA GIMÉNEZ, A.: "El impacto del Reglamento General de Protección de Datos de la Unión Europea y de la LOPDGDD en el régimen jurídico de las transferencias internacionales de datos de carácter personal", en AA.VV.: *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales* (dir. por R. GARCÍA MAHAMUT y B. TOMÁS MALLÉN), Tirant lo Blanch, Valencia, 2019.

ORTEGA GIMÉNEZ, A.: "Transferencia internacional de datos personales: del Safe Harbor al Privacy Shield", *Revista Lex Mercatoria*, núm. 4, 2016.

PIÑAR MAÑAS, J. L.: "Transferencias de datos personales a terceros países u organizaciones internacionales", en AA.VV.: *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad* (dir. por J. L. PIÑAR MAÑAS), Reus, Madrid, 2016.

RECIO GAYO, M.: "Nivel adecuado para transferencias internacionales de datos", *Derecho PUCP: Revista de la Facultad de Derecho*, núm. 83, 2019.

SÁNCHEZ DOMINGO, M. B.: "La transferencia de datos personales a terceros países y organizaciones internacionales según la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016", en AA.VV.: *Los avances del espacio de Libertad, Seguridad y Justicia de la UE en 2017: II Anuario ReDPE* (coord. por M. Á. GUTIÉRREZ ZARZA), Wolters Kluwer, Madrid, 2018.

RECUERO LINARES, M.: "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*, núm. extra 1, 2019.

RODRÍGUEZ AYUSO, J. F.: *Control externo de los obligados por el tratamiento de datos personales*, Barcelona, Ed. Bosch, 2020.

RODRÍGUEZ AYUSO, J. F.: *Privacidad y Coronavirus*, Dykinson, Madrid, 2020.

