LA TRANSFERENCIA INTERNACIONAL DE DATOS CON TERCEROS ESTADOS EN EL NUEVO REGLAMENTO EUROPEO: ESPECIAL REFERENCIA AL CASO ESTADOUNIDENSE Y LA CLOUD ACT[1]

CLARA ISABEL CORDERO ÁLVAREZ

Profesora contratada Doctor de Derecho Internacional privado en la Universidad Complutense de Madrid. Vicedecana de Innovación y Calidad de la Facultad de Derecho (UCM)

Revista Española de Derecho Europeo 70
Abril – Junio 2019
Págs. 49–108

SUMARIO: I. PLANTEAMIENTO. II. CUESTIONES CONCEPTUALES PREVIAS. III. PRECEDENTES DEL REGLAMENTO: DE LA ARMONIZACIÓN A LA UNIFICACIÓN DEL DERECHO EUROPEO. 1. *La transferencia de datos a terceros Estados con nivel adecuado de protección: evaluación institucional y Agencias Nacionales de Control*. 2. *Países sin nivel de protección suficiente*. 2.1. Las cláusulas contractuales como mecanismo de garantía. 2.2. Reglas corporativas vinculantes para grupos de empresas multinacionales. IV. EL NUEVO RÉGIMEN UNIFICADO DE LAS TRANSFERENCIAS INTERNACIONALES. 1. *Transferencias basadas en una decisión institucional de adecuación*. 2. *Garantías adecuadas como mecanismo de transferencia*. 3. *El consentimiento del interesado como piedra angular*. 3.1. El consentimiento como condición del tratamiento. 3.2. Trasferencias internacionales basadas en el consentimiento. V. TRANSFERENCIAS DE DATOS DESDE EUROPA A ESTADOS UNIDOS. 1. *De los principios "Safe Harbour" al acuerdo "Privacy Shield"*. 2. *El futuro de las transferencias de datos transatlánticas tras la "Cloud Act"*. VI. CONCLUSIONES. 1. *Bibliografía*.

1. Esta contribución se ha realizado en el marco del proyecto de investigación MINECO-FEDER: "Protección transfronteriza de la transmisión de datos personales a la luz del nuevo Reglamento europeo: problemas prácticos de aplicación" (código PGC2018-096456-B–I00).

RESUMEN: El nuevo Reglamento de protección de datos unifica la normativa europea (y su interpretación) en esta materia, estableciéndose un único sistema para todo el Espacio Económico Europeo; lo que sin duda revierte en una mayor seguridad jurídica. Además, con la ampliación del alcance espacial se asegura que se apliquen las mismas reglas tanto a las empresas europeas como aquellas domiciliadas en terceros Estados, si suministran bienes y servicios o vigilan la conducta de los ciudadanos europeos. Es evidente que el nuevo instrumento supone un significativo avance legislativo respecto de la anterior normativa, donde las transferencias internacionales de datos son la pieza clave. Ahora bien, cabe plantearse si este marco normativo es suficiente para asegurar que este tipo de operaciones se realice con las máximas garantías cuando tengan por destino un tercer Estado. En particular, pese a los avances conseguidos, el futuro de las transferencias desde la UE a EEUU se manifiesta incierto con los mecanismos existentes; más aún con la aprobación de la conocida como Cloud Act.

PALABRAS CLAVE: Datos personales– Transferencias internacionales– Unión Europea– Terceros países– Reglamento General Protección de datos (RGPD)– Consentimiento– Puerto Seguro– Escudo de privacidad– EEUU– Cloud Act

ABSTRACT: The General Data Protection Regulation unifies European law (and its interpretation) in this field, due to it establishes a unique system for the whole European Economic Area. Consequently, this instrument reverts in a greater legal security. In addition, the expansion of its territorial scope ensures that the same rules will be applied both to European companies and those ones domiciled in third countries when their goods or services are offered in the Union or monitors European citizens´ behavior. It is evident that the new instrument supposes a significant advance in comparison with the previous legislation. The Regulation´s approach is more appropriate for regulating a globalized and digitized world where international data transfers are the key element. However, it could be considered whether this legal framework is enough to ensure data transfers to third countries adapted to the new Regulation. In particular, despite the progresses already made, the future of transfers from the EU to the U.S are unknown; even more after getting into force the Cloud Act

KEYWORDS: Personal data– Cross-border data transfer– European Union– Third countries– General Data Protection Regulation (GDPR)– Consent– Safe Harbor– Privacy Shield– U– S– Cloud Act

Fecha de recepción: 30-1-2019
Fecha de aceptación: 13-3-2019

I. PLANTEAMIENTO

1. La importancia que en Europa se otorga a la protección de datos personales dada su naturaleza de derecho fundamental, tal y como se reconoce en el CEDH[2] como parte integrante del derecho a la intimidad recogido en su artículo 8 [3] y en la Unión Europea de conformidad con los artículos 7 y 8 de la Carta de Derechos Fundamentales[4], se traduce en la existencia de una reglamentación comunitaria imperativa sobre el uso de este tipo de información sensible. El carácter imperativo de esta normativa (previamente la Directiva

2. Convenio para la protección de los derechos humanos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 195 (BOE núm. 243, de 10.X.79).
3. De conformidad con los límites que el TEDH ha sentado con su jurisprudencia sobre el alcance e interpretación de los derechos garantizados en este precepto Respecto de los posibles contenidos del derecho a la vida privada, con un análisis pormenorizado de las sentencias del TEDH, véase REBOLLO DELGADO, L.: *El derecho fundamental a la intimidad,* Ed. Dikynson, 2ª ed. Madrid, 2005; pp. 366-377, en esp. pp. 374-377.
4. Carta de Derechos fundamentales de la Unión Europea (CDFUE), DOCE 18.12.2000, C 364/3 (2000/C 364/01).

sobre protección de datos y actualmente el Reglamento General) conduce a su aplicación necesaria para aquellas operaciones que afecten al tráfico de datos personales en el mercado interior. En particular, dentro del amplio ámbito de la protección del datos las transferencias internacionales de datos personales tienen una importancia muy significativa por su incidencia en las operaciones transfronterizas, por lo que el análisis de su reglamentación en el Derecho europeo resulta esencial y justifica el objeto del presente estudio.

2. Es evidente que, en un contexto como el actual, las transferencias internacionales de datos personales resultan esenciales para el desarrollo de los intercambios comerciales y para la prestación de los servicios en línea (como por ejemplo la conocida como *Cloud Computing*[5] o las redes sociales). A esto ha de añadirse que generalmente los proveedores de servicios de la Sociedad de la Información, que desarrollan o dirigen su actividad a consumidores/usuarios europeos, tienen su sede o establecimiento fuera de la Unión Europea –típicamente en EEUU–, mientras que los servidores donde se localizan los centros de almacenamiento de los datos se encuentran en otro u otros Estados distintos. Todo ello, unido a los avances informáticos y todas las herramientas que operan en la nube, conduce necesariamente a considerar que resulta imprescindible contar con una reglamentación adecuada de la protección de los datos personales[6] que permitan garantizar un tratamiento adecuado de los mismos más allá de la Unión Europea[7]. Así pues, podría decirse que la trans-

5. La computación en la nube puede definirse como: "Utilización de las instalaciones propias de un servidor web albergadas por un proveedor de Internet para almacenar, desplegar y ejecutar aplicaciones a petición de los usuarios demandantes de las mismas". Fuente: *Diccionario Español de Ingeniería. Real Academia de Ingeniería de España.* 1.0 edición, 2014, *http://diccionario.raing.es/es/lema/computaci%C3%B3n-en-la-nube* (visto el 11.01.2019). Sobre la computación en la nube, clasificación de modelos, intervinientes y tipos de servicios, puede verse GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas contractuales y reglas corporativas vinculantes", *RDUNED*, Nº. 14, 2014, pp. 247-270, en esp. pp. 248 a 252.
6. Sobre los riesgos y retos que para la privacidad en general supone este tipo de actividades comprendidas dentro de la computación de la nube y las posibles soluciones técnicas y jurídicas para afrontarlo –existentes y futuras–, véase GHORBEL, A.; GHORBEL, M. y JMAIEL, M., "Privacy in cloud computing environments: a survey and research challenges", *The Journal of Supercomputing*, June 2017, Volume 73, Issue 6, pp 2763-2800. Donde se concluye que no existe una solución única y general que englobe todas las cuestiones y riesgos respecto de la privacidad que se pueden plantear en este contexto y las posibles. De hecho, la gran variedad de datos personales que pueden encontrarse en la nube (fotos, documentos, bases de datos, etc.) y la diversidad de ámbitos y servicios de procesamiento y ejecución existentes hace prácticamente imposible encontrar una única solución genérica, por lo que debe de articularse soluciones flexibles.
7. Resulta evidente que la normativa europea de protección de datos debe enfrentarse a cuestiones transfronterizas, en la medida que dentro de su ámbito de aplicación están las posibles disputas sobre tratamiento de datos relacionadas con supuestos transnacionales en línea. En este sentido, resulta esencial el estudio de la jurisprudencia del Tribunal de Justicia resolviendo sobre su aplicación extraterritorial y las transferencias transfronterizas de datos. En este contexto, puede verse, BU-PASHA, S. "Cross-border issues under EU

ferencia internacional de datos es uno de los elementos más importantes en esta materia concreta –y previsiblemente sea el más relevante en el futuro–; lo que pone de manifiesto la relevancia y necesidad de tratamiento del objeto de estudio en una sociedad globalizada como la actual.

3. En contraposición a la alta exigencia para los responsables del tratamiento de datos personales que se deriva del Derecho europeo, fuera del Espacio Económico Europeo hay Estados cuya regulación puede calificarse como poco exigente –como es el caso de EEUU, que se caracteriza por su laxitud y por ser principalmente normas autorreguladoras[8] –o incluso caracterizarse por la ausencia de cualquier tipo de reglamentación en la materia–[9]. La dispar reglamentación existente en este ámbito puede conducir en la práctica a que quede sin efectos la buscada protección de este tipo de datos por el Derecho europeo cuando aquellos se localicen en países con un nivel de protección inferior o simplemente inexistente. Corresponde, consecuentemente, analizar la regulación actual de este tipo de transferencias desde la perspectiva europea, atendiendo a los distintos elementos que configuran su marco jurídico. Por un lado, a luz del nuevo Reglamento General de protección de datos (en adelante, el Reglamento)[10], por el que se deroga la Directiva 95/46/CE (en adelante, la Directiva[11]). En segundo lugar, de conformidad con los todavía vigentes acuerdos con terceros Estados, en particular del denominado acuerdo *Privacy Shield o Escudo de privacidad*[12] entre EEUU y la UE (sobre transferencias de datos tanto de carácter comercial como el acceso de las autoridades públicas

---

data protection law with regards to personal data protection", *Information & Communications Technology Law*, 24.05.2017, pp. 213-228 (*https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740*).

8. Un estudio comparado de la normativa de protección de datos en Australia, Canadá, EEUU, la Unión Europea, India, Japón, Hong Kong, Malasia y Singapur, puede verse en BHASIN, M., "Challenge of guarding online privacy: role of privacy seals, government regulations and technological solutions", *Socìal no-ekonomičnì Problemì ì Deržava*, 2016, nº 15 (2), pp. 85-104 (*https://core.ac.uk/download/pdf/131446056.pdf*).
9. Aunque parece que existe una tendencia favorable a la reglamentación de esta materia. En este sentido, en el año 2015 se constató que un creciente número de países de todo el mundo ya habían adoptado o estaban en vías de elaboración de nuevas leyes en materia de protección de datos y privacidad. *Vid.* GREENLEAF, G., "Global data privacy laws 2015: 109 countries, with European laws now in a minority", informe publicado en *Privacy Laws & Business International*, n.º 133, febrero de 2015, pp. 14-17 (*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529*).
10. 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. DOUE L 119/1, 4.5.2016.
11. 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE, 23.11.95, Nº.1.281/31).
12. Acuerdo aprobado la Comisión Europea el 12 de julio de 2016 que configura el marco de privacidad de transferencia de datos personales por motivos comerciales desde Europa hacia Estados Unidos (*http://collections.internetmemory.org/haeu/20171122154227/ http:/*

de EEUU a los datos personales transferidos desde la UE, incluso por motivos de seguridad nacional) y, por último, paralelamente, según la preexistente doctrina jurisprudencial del Tribunal de Justicia en esta materia.

Particular referencia merecen en este trabajo el análisis de las consecuencias prácticas que suponen los cambios introducidos por el Reglamento en torno a los aspectos del consentimiento como excepción para transferir los datos personales a terceros Estados que no tienen en su ordenamiento un tratamiento equivalente al europeo y si esta aproximación resulta suficiente para conseguir la protección que por las instituciones europeas se perseguía con esta reglamentación.

4. En el marco jurídico actual de la protección de datos, el nuevo Reglamento se configura como la base del sistema europeo, y por lo tanto se trata de norma de fundamento para las transferencias internacionales. En la medida que el Reglamento tiene carácter de derecho material imperativo –relativo–[13], lo que unido al alcance espacial del instrumento (artículo 2), su aplicación está garantizada por los tribunales y Autoridades nacionales de control los Estados de la Unión en los litigios que sobre el tratamiento de datos o posibles responsabilidades por su tratamiento inadecuado –bien cuando conozcan de este tipo de demandas, bien cuando tengan que resolver sobre el eventual reconocimiento y ejecución de resoluciones extranjeras o medidas cautelares sobre esta materia–. Ahora bien, es posible que esto no sea suficiente para asegurar en la práctica un tratamiento adecuado de estos datos cuando el que tiene que resolver/decidir es un tercer Estado fuera del Espacio Económico Europeo. En este sentido, resulta reveladora la última iniciativa legislativa de Estados Unidos, donde se tramita una ley para permitir el acceso de sus autoridades a datos alojados en servidores situados en el extranjero –incluida la UE–, la *Clarifying Lawful Overseas Use of Data Act*[14], conocida como la *Cloud Act* (que en los términos actuales deja sin objeto parte del acuerdo *Privacy Shield*[15]).

5. En lo que respecta en particular a las transferencias internacionales de datos, el nuevo instrumento ha introducido importantes novedades en relación con la Directiva. La primera novedad que debe referirse en este ámbito,

---

ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf). Este acuerdo vino a sustituir al antiguo *Safe Harbor*, utilizado desde el año 2000.

13. En términos similares a su predecesora la Directiva y la legislación nacional de transposición de los Estados Miembros.
14. H.R.4943 –*CLOUD Act*, 115th Congress (2017-2018). Texto íntegro disponible en *https://www.congress.gov/bill/115th-congress/house-bill/4943*.
15. Sin perjuicio de que la vigencia de tal acuerdo está en entredicho en la medida que actualmente existe un recurso de anulación presentado frente a la Decisión 2016/1250, por ser contraria a los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (Recurso interpuesto el 25 de octubre de 2016, *La Quadrature du Net y otros c. Comisión*, Asunto T-738/16).

es que con el Reglamento el exportador de los datos podrá ser tanto el responsable como el encargado del tratamiento[16]. Esta apreciación específica supone que ya no resulta aplicable la condición que algunos Estados Miembros habían impuesto para este tipo de operación y que consistía en que el exportador debía ser siempre el responsable del tratamiento (lo que condicionaba también las partes de las posibles soluciones contractuales para alcanzar las garantías adecuadas exigidas por el Derecho europeo para las transferencias internacionales). Asimismo, la delimitación del ámbito espacial (art. 3 [17]) y material (art. 2) [18] de aplicación del Reglamento conduce a que casi la totalidad de tratamientos de datos personales estarán sujetos a este instrumento; y por cuanto a las transferencias de datos internacionales se refiere, las nuevas reglas abarcan tanto las transferencias con fines comerciales como las derivadas del cumplimiento de la ley o tratados internacionales –fundamentalmente de asistencia judicial mutua[19]–. Por tanto, el Reglamento busca una protección de datos con vocación de universalidad –en términos similares a cómo el legislador español transpuso la Directiva en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD)[20]–. La diferencia por tanto entre la anterior regulación –la Directiva y normativa nacional de los Estados miembros de transposición– y el actual Reglamento/nueva LOPD de 2018 radica, esencialmente, en el régimen de funcionamiento de la transferencia de datos a terceros Estados –fuera del Espacio Económico Europeo–.

En este sentido, se incorporan nuevas reglas detalladas y claras para todos los supuestos de transferencia internacional con el objeto de dotar de transparencia a este tipo de operaciones. Si bien el Reglamento se mantiene en la línea marcada por la Directiva respecto de adecuación de las decisiones sobre

16. Esto supone que el que resulte ser el exportador, el responsable o el encargado, deberá adoptar las medidas necesarias para compensar la falta de protección de datos de país de destino, mediante garantías adecuadas para el interesado (Considerando 108). No obstante, el responsable del tratamiento sigue siendo la figura principal en el Reglamento, y como tal es el que principal obligado en última instancia a adoptar las medidas y previsiones necesarias para asegurar las garantías exigidas por este instrumento en el tratamiento de datos en estos supuestos (Considerando 11).
17. *Vid*. RIPOLL CARULLA, S., "Aplicación territorial del reglamento", en *Reglamento general de protección de datos: Hacia un nuevo modelo europeo de privacidad*, VVAA (Dir. J. L. Piñar Mañas), Ed. Reus, 2016, pp. 77-186.
18. Sobre el ámbito material de aplicación del nuevo Reglamento *vid*. URIARTE LANDA, I., "Ámbito de aplicación material", en *Reglamento general..., ob. cit.,* pp. 63-76.
19. *Vid*. considerando 115 y art. 48 del Reglamento.
20. *BOE* núm. 298, de 14/12/1999, páginas 43088 a 43099. Norma derogada, con efectos de 7 de diciembre de 2018, por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, sin perjuicio de lo previsto en las disposiciones adicional 14 y transitoria 4 de la, según su disposición derogatoria única (BOE núm. 294, de 06/12/2018); en adelante, nueva LOPD. Con esta nueva Ley Orgánica el legislador español trata de adaptar el ordenamiento jurídico español al nuevo Reglamento y completar sus disposiciones; así como garantizar los derechos digitales del artículo 18.4 de la Constitución.

el nivel de protección del país de destino, las cláusulas contractuales tipo, las normas corporativas vinculantes o las excepciones a la prohibición general de realizar transferencias de datos fuera del Espacio Económico Europeo, se clarifican reglas y se introducen nuevas herramientas para las transferencias[21]. También desde el punto de vista burocrático el Reglamento supone una mejora desde la perspectiva de los exportadores de datos, en la medida que la simplifica en ciertos supuestos. En términos generales, desde la perspectiva española, puede referirse un cambio relevante respecto de la tramitación administrativa que estas operaciones requerían con la Directiva-LOPD, esto es, solicitud de previa autorización administrativa (artículo 33.1 LOPD) –y aprobación de la AEPD– salvo las excepciones del artículo 34 LOPD. El Reglamento en este sentido da un giro total dejando la autorización administrativa a casos realmente excepcionales, de tal manera que la autorización administrativa pasa de ser la norma general a ser una excepción muy concreta (en este sentido se recoge en el art. 42 de la nueva LOPD de 2018). Pese a esto la Autoridades nacionales de control no pierden relevancia, sino todo lo contrario, pues en la nueva reglamentación se amplía su poder y se regula más detalladamente su independencia, funciones y facultades[22], llegando incluso a hacer una referencia explícita a su facultad para suspender el flujo de datos a un tercer Estado o a una determinada organización internacional (art. 58) –lo que ya estaba previsto en ciertas legislaciones nacionales de transposición, como en el caso español[23]–. Asimismo, la reforma practicada por el Reglamento faculta a la Comisión para crear mecanismos de cooperación internacional que faciliten la aplicación de la normativa de protección de datos, incluso mediante la celebración de acuerdos internacionales de asistencia mutua (art. 50)[24].

6. Finalmente, cabe referir el recientemente constituido Comité Europeo de Protección de Datos (en adelante, CEPD)[25], que se configura como máximo

21. Estableciendo un "renovado y diversificado conjunto de instrumentos de transferencia internacional", *Cf. Comunicación de la Comisión al Parlamento europeo y al Consejo, sobre el Intercambio y protección de los datos personales en un mundo globalizado*, COM(2017) 7 final/2 de 17.02.2017, ap. 2.2, (*https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52017DC0007R%2801%29#footnoteref45*).
22. *Vid*. Capítulo VI del Reglamento y Título VII de la nueva LOPD de 2018.
23. En ejercicio de la facultad que le concede al Director de la AEPD el art. 37.1.f) de la LOPD, y previa audiencia del exportador, éste podrá suspender temporalmente la transferencia de datos a un determinado Estado, aunque la Comisión hubiera constatado la existencia en aquel de un nivel adecuado de protección si se daban alguna de las condiciones del art. 69 del RLOPD.
24. Complementado por el Considerando 102.
25. Fundado el 25 de mayo de 2018, es un organismo europeo independiente cuya función principal es conseguir la aplicación coherente de las normas de protección de datos en toda la Unión Europea (del Reglamento General de Protección de Datos y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 sobre protección de datos en el ámbito policial) y promover la cooperación entre las autoridades de protección de datos de la UE (fuente: *https://edpb.europa.eu/about-edpb/about-edpb_es*).

órgano de coordinación de las políticas de privacidad en el ámbito de la UE –y que viene a sustituir al Grupo de Trabajo de artículo 29–, en la medida que está llamado a tener una intensa actividad para conseguir los propósitos marcados por el nuevo instrumento. En lo que respecta a la transferencia internacional de datos, este organismo ha publicado sus nuevas Directrices sobre las excepciones previstas en el artículo 49 del Reglamento[26] basados en el anterior documento del Grupo de Trabajo del artículo 29[27] (en adelante, GT29) en interpretación del art. 26 (1) de la Directiva[28]. Esta Directrices resultan esenciales en la práctica, dado que determinan las condiciones y requisitos para que se pueda cumplir el principio general de que los datos personales solo pueden transferirse a terceros países si en estos se proporciona un nivel de protección adecuado o si se han aportado garantías adecuadas y los interesados disfrutan de derechos exigibles y efectivos.

II. CUESTIONES CONCEPTUALES PREVIAS

7. Debe delimitarse necesariamente lo que se entiende por transferencia internacional de datos en el contexto de la normativa europea, por dos razones fundamentales. En primer lugar, para poder centrar así el objeto de estudio, en la medida que tal consideración determina la aplicación del régimen especial del Capítulo V del Reglamento; y en segundo lugar, para poder entender la problemática práctica que este tipo de actividades pueden generar en lo que respecta a la tutela efectiva de los datos personales.

8. No existe una definición expresa en la reglamentación europea sobre protección de datos de lo que se entiende por transferencia internacional a terceros países (dado que entre las definiciones del art. 4 del actual Reglamento sólo encontramos, en su numeral 23, la referencia al tratamiento transfronterizo de datos en relación con los Estados miembros). Consecuentemente, para suplir esta laguna conceptual, podemos recurrir a la normativa española donde podemos encontrar una definición concreta de transferencia internacional de datos en el artículo 5.1.s) del Real Decreto 1720/2007, de 21 de diciembre[29]

26. *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018* (*https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf*).
27. Este Grupo de trabajo es un órgano consultivo independiente sobre la protección de datos y la intimidad, que se creó en virtud del artículo 29 de la Directiva 95/46/CE y está integrado dentro de las Autoridades de Protección de Datos de todos los países miembros. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.
28. *Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, adoptado el 25 de noviembre de 2005 (2093/05/EN, WP114). *https://www.pdpjournals.com/docs/88080.pdf*.
29. BOE núm. 17, de 19 de enero de 2008. Norma que no ha sido expresamente derogada con la nueva LOPD de 2018, ni por el Reglamento, de conformidad con la disposición derogatoria única de la LO 3/2018, en aquellos que no sea contrario a la nueva normativa. En

(en adelante, RLOPD[30]), por el que se aprobaba el Reglamento de desarrollo de la LOPD, que sigue vigente: *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.* Según esta definición, las transferencias internacionales suponen un flujo de datos desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (en adelante EEE, integrado por los países de la Unión Europea más Liechtenstein, Islandia y Noruega). En este contexto, el exportador de datos personales será la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una transferencia internacional de datos; y el importador aquella persona física o jurídica, pública o privada, u órgano administrativo que reciba la transferencia como responsable del tratamiento, encargada del mismo o tercero[31]. Lo que aplicado al contexto del Reglamento supone que el flujo de datos tiene origen en un Estado del EEE y como destino un tercer Estado. Así, existirá transferencia internacional cuando ésta constituya una cesión o comunicación de datos o cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable, produciéndose una salida física de datos fuera del EEE. Quedan excluidos de tal definición los supuestos de acceso a los datos por cuenta de un encargado del tratamiento establecido dentro del EEE, dado que no se produce una salida jurídica de los datos.

9. Ahora bien, la delimitación de que una determinada actividad constituye una transferencia de datos a tercer país a tales efectos no es una cuestión tan sencilla como pareciera en una primera aproximación. La variada y amplia casuística que puede producirse en el ámbito de las actividades desarrolladas en la nube puede plantear numerosas dudas en este sentido, como da muestra la nutrida jurisprudencia del Tribunal de Justicia resolviendo las cuestiones prejudiciales planteadas en relación con la Directiva[32] (doctrina extensible al vigente Reglamento). Cabe destacar la Sentencia de 6 de noviembre de 2003 (TJCE 2003, 368), *Lindqvist*[33], donde el Tribunal da respuesta a la cuestión prejudicial planteada sobre si existe transferencia de datos a un tercer país, en

---

consecuencia, la definición referida sigue plenamente vigente y viene a suplir una laguna que sigue existiendo en la normativa europea.

30. Un análisis en profundidad sobre el Reglamento de desarrollo de la LOPD puede verse en VV.AA., *Protección de datos: Comentarios al Reglamento* (Coord. ZABÍA DE LA MATA, J.) Ed. Lex Nova, 2008.
31. *Cf.* letras j y ñ) del art. 5.1 del RLOPD.
32. Un análisis de la principal jurisprudencia del Tribunal de Justicia en este sentido puede verse en el apartado 4.5 "Concepto de transferencia internacional" en PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Ed. Wolters Kluwer, 2018, pp. 156-160.
33. STJCE de 6 de noviembre de 2003 (TJCE 2003, 368), *Bodil Lindqvist*, asunto C-101/01 (I-12992).

el sentido del art. 25 de la Directiva (que se corresponde con los artículos 44 y ss. del Reglamento), cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por persona física o jurídica que gestiona el sitio en el que está alojada dicha página (proveedor de servicios de alojamiento de páginas web) y que tiene su domicilio en el mismo Estado u otro Estado miembro, de manera que dichos datos son accesibles a cualquier persona que se conecte a Internet, incluyendo aquellas situadas en terceros países. A mayor abundamiento, específicamente se plantea si la respuesta a esta cuestión seguiría siendo la misma si se acreditaba que ningún nacional de un país tercero ha accedido efectivamente a dichos datos o si el servidor en el que está almacenada la página se encuentre físicamente situado en un tercer país.

La posición institucional y de los distintos Gobiernos que intervinieron en el proceso resulta muy ilustrativo de la problemática ante la que nos encontramos. Por un lado, la Comisión y el Gobierno sueco consideraron que la introducción de los datos personales en una página web a través de un ordenador, cuando dichos datos resultan accesibles a nacionales de terceros países, constituía una transferencia internacional de datos a estos efectos; incluso aunque ningún nacional de tercer Estado haya accedido efectivamente a dichos datos o aun cuando el servidor en el que estuvieran almacenados los datos estuviera físicamente situado fuera de la UE (ap. 53, *Lindqvist*). Por el contrario, los Gobiernos holandés y del Reino Unido mostraron una posición totalmente contraria. Por cuanto se refiere al Gobierno holandés (partiendo de la premisa de que no se define en la Directiva el concepto de transferencia[34]) consideraba que, por un lado, ha de entenderse que dicho concepto se refiere a un acto dirigido intencionadamente a transferir datos personales del territorio de un Estado miembro a un tercer país y, por otro, que no era posible distinguir entre las diferentes formas en los que los datos se ponen al alcance de terceros; concluyendo que la introducción de datos personales en una página web por medio de un ordenador no puede considerarse transferencia internacional de datos personales a los efectos del art. 25 de la Directiva. Por lo que respecta al Reino Unido, consideró que el supuesto analizado no estaba cubierto por este artículo. Así, alegó que este precepto reglamentaba supuestos de transferencias de datos personales a terceros Estados y no la posibilidad de acceder a dichos datos desde fuera de la UE; concretando que el concepto de transferencia implica que una persona situada en un determinado lugar transmite un dato a una tercera persona situada en otro lugar, lo que en el supuesto de referencia no se verificaba en estos términos (aps. 54 y 55, *Lindqvist*).

El Tribunal de Justicia para resolver parte de la misma premisa que el Gobier-

34. Esta laguna conceptual se mantiene con la entrada en vigor del nuevo instrumento, en la medida que entre las definiciones que el Reglamento recoge en su artículo 4 no se encuentra la "transferencia", ni tampoco en ninguno de los preceptos del Capítulo V de este instrumento dedicado a la reglamentación de las transferencias internacionales de datos, a terceros países u Organizaciones internacionales (arts. 44 a 50).

no holandés, esto es, la ausencia de definición de transferencia internacional (a país tercero) en la norma institucional. En este contexto, la respuesta del Tribunal se argumenta en dos consideraciones esenciales. Por un lado, la naturaleza técnica de las operaciones objeto de análisis y, por otro, el objetivo y la organización sistemática del Capítulo IV de la Directiva (que se corresponde en esencia con el actual Capítulo V del vigente Reglamento).

Desde el punto de vista de la naturaleza técnica de las operaciones efectuadas, el Tribunal de Justicia señala, que la naturaleza propia de Internet y el carácter público de la información que se publica en este medio hace que ésta pueda ser consultada en cualquier momento por un "número indeterminado de personas que residen en múltiples lugares" (aps. 58 a 61). Los medios técnicos empleados para acceder a Internet determinan la ubicuidad de la información que encuentra en la red. En este contexto, los particulares cuentan a su disposición con modalidades de uso de Internet con significativa relevancia práctica en el ámbito de la protección de datos. Como, por ejemplo, en el caso de análisis, la gestión de una página web –que transmite los datos al proveedor de servicios de alojamiento de páginas web, que es quien gestiona la infraestructura informática necesaria para garantizar el almacenamiento de dichos datos y la conexión del servidor que aloja el sitio web–, permite la transmisión posterior de dichos datos a cualquier persona que tenga conexión a Internet y los solicite –con independencia del lugar físico en el que esté ubicado el solicitante[35]–. Los ordenadores que forman parte de esa infraestructura necesaria pueden encontrarse –y esa es la realidad habitual– en uno o varios países distintos de aquél en el que se encuentra domiciliado el proveedor de servicios de alojamiento de páginas web, "sin que los clientes (el titular/gestor de la página web) tengan o puedan tener conocimiento de ello". Todo ello, en relación con el caso concreto analizado, supone para el Tribunal que "las páginas web de la Sra. Lindqvist no contenían los mecanismos técnicos que permiten el envío automático de la información a personas que no hayan buscado deliberadamente acceder a dichas páginas". Por lo que concluye que, para el caso de referencia, "los datos personales que llegan al ordenador de una persona que se encuentra en un país tercero y que proceden de una persona que los ha publicado en un sitio Internet, no han sido objeto de una transferencia directa entre estas dos personas, sino que se han transmitido con la ayuda de la infraestructura informática del proveedor de servicios de alojamiento de páginas web donde está almacenada la página".

La segunda consideración es el análisis sistemático de la reglamentación de la transferencia internacionales (Capítulo IV de la Directiva[36]), para determinar si

35. Salvo que dicha información esté vetada a un determinado territorio o limitada a ciertos países, a través del uso de herramienta de geolocalización, lo que se denomina como Geo-bloqueo.
36. El equivalente al actual Capítulo V del Reglamento, que introduce como novedad en la reglamentación de las transferencias internacionales de datos no solo aquellas realizadas a terceros países sino también a Organizaciones internacionales.

los comportamientos a los que se circunscribe la cuestión prejudicial están o no cubiertas por este régimen especial[37]. La aproximación operada por el Tribunal en este sentido parte de la realización previa de una serie de consideraciones de tipo general[38]. Primero, sobre el carácter especial del régimen establecido para este tipo de operaciones, integrado por reglas específicas y que se diferencia y complementa al régimen general contenido en el Capítulo II (licitud de los tratamientos de datos personales). En segundo lugar, sobre la finalidad que se persigue con este régimen específico[39]: impedir transferencias a terceros Estados que no tengan o garanticen un nivel de protección equiparable al de la UE (aps. 62 a 64), y las obligaciones impuestas por este régimen a los Estados miembros y la Comisión para el control de las transferencias de datos a terceros Estados teniendo en cuenta el nivel de protección dispensado por aquellos países (aps. 65 y 66). Establecido el contexto, el Tribunal analiza cómo ha de considerarse el uso de Internet en el marco de las transferencias internacionales (aps. 67 a 69). La Directiva no recogía disposición alguna relativa al uso de Internet en su Capítulo IV –y en los mismos términos se repite esta aproximación en el correlativo Capítulo V del Reglamento–. La normativa europea no precisa los criterios que permitan determinar si, para las operaciones realizadas a través de proveedores de servicios de alojamiento de páginas web, debe tomarse en consideración el lugar de establecimiento del proveedor, su domicilio profesional o el lugar donde se encuentran físicamente los ordenadores que integran la infraestructura informática del proveedor (ap. 67). Contextualizando el desarrollo de Internet existente en el momento en el que la Directiva fue elaborada y la ausencia de dichos criterios, para el Tribunal resulta evidente que el legislador europeo no podía tener en mente que un supuesto con el de referencia esté incluido dentro del concepto de transferencia de datos a tercer país. Una aproximación en sentido contrario conduciría a que, a los efectos de la normativa europea, cada vez que se publican datos personales en una página web sería considerada forzosamente como una transferencia internacional de datos a todos los terceros países en los existan medios técnicos necesarios para acceder Internet. De esta forma el régimen especial se convertiría en un régimen general, con significativas consecuencias prácticas (en la medida que la Comisión constatara que

37. Aclarando el Tribunal que sus consideraciones en este sentido no se refieren a las operaciones que realizan los proveedores de servicios de páginas web, al no estar incluidas por el órgano jurisdiccional remitente en su cuestión prejudicial, sino únicamente a las actividades realizadas por la Sra. Lindqvist (ap. 62).
38. Las consideraciones que a este respecto el Tribunal de Justicia realizó en esta resolución, son extrapolables al actual Reglamento, en la medida que éste que parte de la misma sistemática que su predecesora. Si bien, con un mayor detalle y exhaustividad en los términos, condiciones y regímenes aplicables, en particular, en lo que respecta a las transferencias internacionales con terceros países u Organizaciones internacionales (Capítulo V), como se deduce del presente estudio.
39. Objetivo definido en los Considerandos 56 a 60 de la Directiva (sintetizado en el considerando 101 del actual Reglamento, y especificado en los considerandos números 102 a 116).

uno solo de los terceros países no garantizara un nivel de protección adecuado, se impediría cualquier difusión de datos personales en Internet[40]).

Por todo ello, el Tribunal de Justicia concluye que las operaciones realizadas por la Sr. Lindqvist (subir datos a una página web), no constituyen por sí mismas "una transferencia a un país tercero de datos", con independencia de si alguna persona de un tercer Estado ha tenido acceso a la página web de que se trata o si el servidor del proveedor se encuentra físicamente fuera de la UE. En consecuencia, no existe transferencia internacional a los efectos del art. 25 de la Directiva (extrapolable al actual art. 44 y ss. del Reglamento) cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el sitio Internet en el que se puede consultar la página que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros[41].

10. En definitiva, la determinación de la operación como de transferencia de datos internacional (fuera del EEE) resulta esencial (durante la vigencia de la Directiva y ahora en aplicación del Reglamento), por los controles que establece el Derecho Europeo en este sentido para garantizar el adecuado tratamiento. Así pues, del carácter internacional de la transferencia dependerá si es necesario o no tramitar autorización administrativa previa y específica o de declaración de mediante Decisión de adecuación (al margen de las excepciones tasadas), salvo supuestos de países con nivel de protección adecuado o transferencias en las que se han asegurado garantías adecuadas efectivas y exigibles por los interesados, o supuestos de normas corporativas vinculantes (también conocidas como *Binding corporate rules*)[42] para transferencias entre grupos de empresas multinacionales[43].

---

40. De conformidad con el art. 25.4 Directiva, serían los Estados miembros los obligados a impedir tal difusión. Mientras que en el art. 44 del Reglamento el protagonismo se centra en las Decisiones de la Comisión sobre el nivel de adecuación del tercer Estado, un territorio o un sector específico de ese tercer país o una organización internacional, y los actos de ejecución para garantizar dichas transferencias –por los que derogará, modificará o suspenderá la Decisión en caso de que ya no se garantice el nivel de protección requerido, según el art. 44.5 Reglamento–.
41. Apartados 70-71 y punto 4 del Fallo.
42. Definidas en el Reglamento 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" (art. 4 núm. 20).
43. Al margen de las excepciones previstas en las que en determinados supuestos se podrán mover los datos personales de forma internacional sin cumplir ninguna de las previsiones anteriores (art. 34 LOPD y actual artículo 49 Reglamento).

11. Una vez delimitados en términos generales aquellos comportamientos que pueden constituir transferencias internacionales de datos a los efectos del objeto de estudio, procede analizar el régimen especial previsto en el Derecho europeo. En primer lugar, mediante un examen comparativo de los dos instrumentos fundamentales en este ámbito, esto es, la Directiva ya derogada y el ya vigente Reglamento; todo ello junto con la referencia a la principal doctrina jurisprudencial asentada por el Tribunal de Justicia para su interpretación y aplicación. Por otro lado, y con especial mención a las operaciones de transferencia de datos personales desde Europa a Estados Unidos, se analizará el alcance y operatividad de los convenios con terceros Estados a los efectos de garantizar las transferencias internacionales: situación actual y su posible futuro en atención a los ya plateados recursos de anulación, y los que eventualmente puedan instarse respecto de las vigentes Decisiones de ejecución de la Comisión[44], y las recientes iniciativas legislativas extranjeras –como por ejemplo la ya aprobada *Cloud Act* estadounidense–. Todo ello con el fin de poder determinar los efectos prácticos de este cambio legislativo en el nuevo entorno internacional.

III. PRECEDENTES DEL REGLAMENTO: DE LA ARMONIZACIÓN A LA UNIFICACIÓN DEL DERECHO EUROPEO

12. En este apartado va a analizarse la evolución del Derecho europeo en la regulación de la transferencia internacional de datos personales a terceros Estados, partiendo de la armonización realizada a través de la Directiva, cumplimentada por la doctrina jurisprudencial del Tribunal de Justicia[45], hasta llegar al *status quo* vigente desde el pasado 25 de mayo de 2018, con la entrada en vigor del Reglamento general, por el que se unifica esta materia para todos los Estados Miembros estableciendo un único sistema en todo el EEE[46].

---

44. *Vid*. Recurso interpuesto el 16 de septiembre de 2016, *Digital Rights Ireland/Comisión* (Asunto T-670/16), ya resuelto mediante Auto del Tribunal General de 22 de noviembre de 2017 desestimando el Recurso basado en el artículo 263 TFUE por el que se solicitaba la anulación de la 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. Actualmente sigue pendiente de resolver el Recurso interpuesto el 25 de octubre de 2016, *La Quadrature du Net y otros c. Comisión* (Asunto T-738/16), por el que se solicita que se declare que la misma Decisión sobre el Escudo de la privacidad UE-EE. UU es contraria a los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea y, en consecuencia, anule la citada Decisión.
45. *Vid*. PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos...*, *ob.cit.*, pp. 156-160.
46. Un análisis pormenorizado de las claves esenciales del cámbio de régimen europeo de protección de datos por el paso de la Directiva al Reglamento puede verse en RALLO LOMBARTE, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de derecho político*, Nº 85, 2012, pp. 13-56.

1. LA TRANSFERENCIA DE DATOS A TERCEROS ESTADOS CON NIVEL ADECUADO DE PROTECCIÓN: EVALUACIÓN INSTITUCIONAL Y AGENCIAS NACIONALES DE CONTROL

13. La Directiva abordaba la transferencia de datos personales a terceros países en su Capítulo IV, integrado únicamente por dos artículos: el 25 (principios) y 26 (excepciones)[47]. Se permitía la libre circulación de datos personales a países situados fuera del EEE si el país de destino garantizaba un nivel adecuado de protección y el mismo principio de base rige en el nuevo instrumento. Consecuentemente, el responsable del tratamiento y sus corresponsables o encargados debían –y deben– establecer garantías específicas. La interpretación de estos dos artículos venía determinada por el propósito de aquella norma, esto es, armonizar la legislación nacional en materia de protección de datos y asegurar el más alto nivel de protección dentro de la Unión, partiendo del carácter de derecho fundamental que el respeto a la vida privada y familiar y a la protección de los datos personales otorga la Constitución europea a la luz de los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea[48].

En este sentido, las autoridades nacionales de control cumplían una labor fundamental (dentro de su jurisdicción) en la aplicación de la Directiva. Por lo que respecta a España, la Agencia Española de Protección de Datos (AEPD) ostentaba las competencias para evaluar la aplicación de las disposiciones adoptadas con base en la Directiva (la LOPD y el RLOPD)[49] respecto del tratamiento de datos personales realizado en el marco de las actividades de un responsable del tratamiento con establecimiento en el territorio español o, aun cuando no lo tuviera, recurriera para el tratamiento de los datos a medios (automatizados o no) situados en territorio español, salvo si solo los utiliza con fines de tránsito (art. 4.1 de la Directiva)[50]. Por lo que respecta en particular a la transferencia de datos personales a terceros Estados, el responsable

47. Un estudio concreto de la transferencia de datos internacionales en el contexto de la Directiva puede verse en GRANDE SANZ, M., "La transferencia internacional de datos personales: presente y futuro", *Diario La Ley*, Nº 8808, Sección Tribuna, 21 de Julio de 2016, Ref. D-293.
48. DOCE 2000/C 364/01.
49. La transferencia internacional de datos se encontraba regulada en los arts. 33 y 34 de la LOPD –art. 43 de la nueva LOPD de 2018– y artículos 65 a 70 y 137 a 140 del RLOPD.
50. En este sentido se ha pronunciado reiterada jurisprudencia del Tribunal de Justicia. Entre otras, la STJUE de 13 de mayo de 2014, asunto *Google Spain*, C-131/12 (ECLI:EU:C:2014:317), sobre el alcance del ámbito de aplicación espacial del Derecho comunitario en materia de protección de datos (Directiva); y la STJUE de 1 octubre de 2015 (JUR 2015, 234820), asunto *Weltimmo,* C-230/14 (ECLI:EU:C:2015:639) sobre la determinación de la ley nacional aplicable y la autoridad nacional competente para sancionar, en un supuesto donde el responsable del tratamiento estaba establecido formalmente en un Estado miembro pero la vulneración del derecho a la protección de los datos personales se concreta en otro Estado miembro. Esta aproximación se supera con el nuevo ámbito territorial de aplicación del Reglamento (art. 3).

del tratamiento debía informar a la AEPD –obligación que se mantiene en la nueva LOPD de 2018 en su art. 43 en relación con el art. 49.1 del Reglamento– para su inscripción en el Registro General de Protección de Datos (art. 65.3 del RLOPD); al margen de la posible declaración por la Agencia del nivel adecuado de protección del Estado de destino para evitar, en su caso, la necesaria previa autorización para la transferencia.

14. A la luz de la Directiva –y disposiciones nacionales de transposición– las transferencias internacionales de datos contaban con distinto tratamiento en función de si gozaba o no (según la Comisión Europea o una Autoridad Nacional de Control) el Estado de destino de un nivel adecuado de protección. En el caso de que el importador de datos se encontrara en un Estado sin un nivel adecuado de protección de datos personales podría requerirse autorización previa a la transferencia –salvo ciertas excepciones–.

15. Para realizar su labor de evaluación, la Comisión tomaba en consideración todas las circunstancias concurrentes en la transferencia concreta o categoría de transferencias (obligación que se mantiene en el ámbito del nuevo Reglamento, por cuanto que recae en esta institución dicha tarea con carácter exclusivo, si bien, concretándose en otros los factores de evaluación). En particular, debía de analizarse la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final y las normas de Derecho (generales o sectoriales) así como las de carácter profesional y las medidas de seguridad vigentes en aquel país (art. 25.2 Directiva). El estándar de referencia para la valoración del nivel de protección del Estado es el marcado por el Derecho Europeo; si bien no es necesario un nivel idéntico sí debe ser equiparable. En este contexto, el GT29 ha referido en varios Documentos la necesidad de analizar la posible equiparación entre los principios inspiradores del régimen de protección de datos personales del ordenamiento jurídico del Estado que se está evaluando y los del Derecho Europeo y verificar su nivel de efectividad en la práctica[51]. Esta aproximación ha sido reforzada por la jurisprudencia del Tribunal de Justicia, en la medida que este "control", mediante declaración de idoneidad del régimen jurídico de protección de datos personales del Estado de importación, es la forma de evitar que se eluda el elevado nivel de protección que se garantiza

51. *Vid*. Documento WP12 sobre "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea", aprobado por el Grupo de trabajo el 24 de julio de 1998 (DG XV D/5025/98), donde se establece una serie de principios que constituyen el núcleo" de principios de contenido" de protección de datos y de requisitos de procedimiento/de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección; y Documento WP114 de trabajo "relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995" (2093/05/ES) adoptado el 25 de noviembre de 2005.

por la Directiva en el tratamiento de datos en caso de transferencias internacionales a terceros Estados (Sentencia *Schrems*[52]).

Actualmente, la lista de países que la Comisión ha decidido que tienen un nivel de protección adecuado son: Japón (Decisión de Ejecución 2019/419/UE de la Comisión de 23 de enero de 2019)[53], Andorra (Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010), Argentina (Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003), Suiza (Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000), Islas Feroe (Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010), Guernsey (Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003), Israel (Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011), Isla de Man (Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004), Jersey (Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008), Nueva Zelanda (Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012), Uruguay y Canadá (Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos: *Personal Information and Electronic Document Act*– sector privado). Respecto de EEUU previamente fue excluido en la medida que la Decisión 2000/520/CE sobre transferencia internacional de datos personales a empresas de EEUU (conocida como la Decisión *Safe Harbor* o de Puerto Seguro) fue declarada inválida por el Tribunal de Justicia en su ya referida Sentencia *Schrems* (TJCE 2015, 324)[54]. No obstante, posteriormente, dicha idoneidad ha sido determinada de manera limitada por la Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, aplicable a las entidades certificadas en el marco del

52. *Cf.* STJUE de 6 de octubre de 2015 (TJCE 2015, 324), asunto *Schrems*, C-362/2014, ap. 73, (EU:C:2015:650). Un análisis pormenorizado de esta sentencia y de las consecuencias en la aplicación del nuevo Reglamento para la protección privada del derecho fundamental a la autodeterminación informativa, puede verse en REQUEJO ISIDRO, M. "La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el 9Reglamento (UE) 2016/67", *La Ley Mercantil*, nº 42, diciembre 2017, pp. 1-25.
53. Esta es la primera de las Decisiones de Ejecución que la Comisión adopta en el marco del nuevo RGPD al amparo de su art. 45 apartado 3 tras su entrada en vigor. Las consecuencia principal de esta Decisión es que las transferencias internacionales de datos de la UE-EEE a Japón puede realizarse sin necesidad de obtener ninguna otra autorización, de conformidad con lo dispuesto en el artículo 45, apartado 1, y en el considerando 103 del Reglamento.
54. La anulación de dicha Decisión por el TJUE abrió el debate entre la doctrina y los profesionales de la privacidad sobre el futuro de las transferencias internacionales de datos. A modo de ejemplo, dentro del ámbito nacional profesional puede referirse *Monográfico de la Asociación Profesional Española de Privacidad (APEP) sobre sentencia del TJUE que anula el acuerdo para la transferencia de datos personales UE – EEUU "Safe Harbor"*, disponible en *https://www.apep.es/monografico-safe-harbor/?v=04c19fa1e772*. Entre la doctrina internacional véase, entre otros, CRESPI, S, "The Applicability of Schrems Principles to the Member States: National Security and Data Protection within the EU Context", *European Law Review*, Nº 5, 2018, pp. 669-686; KUNER, C. "Reality and Illusion in EU Data Transfer Regulation Post Schrems", *German Law Journal*, vol. 18, n1 4, 2017, pp. 881-918.

Escudo de Privacidad UE-EEUU (conocida como Decisión *Privacy Shield* o de Escudo de Privacidad).

16. En cualquier caso, aunque exista una decisión de la Comisión declarando la adecuación del nivel de protección de un país eso no impide que el titular, cuyos los datos personales hayan sido o pudieran ser objeto de transferencia internacional a dicho Estado, pueda alegar lo contrario, puesto que las Decisiones no solo declaran la adecuación del nivel de protección de la normativa del tercer Estado de importación sino las condiciones y requisitos para que mantenga dicha equiparación con el Derecho Europeo. En este sentido, las Decisiones de la Comisión obligan a los Estados miembros y a todos sus órganos –Agencias nacionales de control y órganos jurisdiccionales, incluidos– a adoptar todas las medidas que resulten necesarias para su cumplimiento y resulten eficaces. Y es en este contexto en el que si una Agencia Nacional de Control tienen conocimiento de que el país de destino no cumple con el nivel de protección exigido en la UE, por solicitud presentada por el titular de los datos personales objeto de transferencia internacional – ya realizada o que pudieran ser objeto de aquella–, pese a que exista declaración de la Comisión al efecto (mediante Decisión) tiene dos únicas posible opciones: 1º) considerar fundada la solicitud del particular y comparecer ante los tribunales nacionales para que, en su caso, planteen una cuestión prejudicial al TJUE sobre la validez de la decisión de la Comisión; lo que por otro lado no impedirá que la Agencia investigue por su cuenta los hechos y, si así lo considera, en ejercicio de sus facultades, pueda suspender temporalmente la transferencia internacional dirigida a ese Estado en cuestión. 2º) desestimar la solicitud por considerarla infundada y que sea personalmente el interesado quien ejercite acción judicial ante los tribunales nacionales[55] para que sean ellos, si así procede, quienes planteen la cuestión prejudicial ante el Tribunal de Justicia. En cualquiera de los dos supuestos, será el Tribunal de Luxemburgo el que deba resolver sobre la posible invalidez de la Decisión de la Comisión sobre el nivel de protección adecuado del tercer Estado de destino en cuestión.

17. Finalmente debe indicarse que la Directiva permitía que el nivel de adecuación de protección del país de destino fuera declarado por la Agencia Nacional de Control de residencia/establecimiento del titular de los datos, evitando así el requisito de autorización previa[56]; posibilidad que ahora ha des-

55. Ese fue el supuesto en el caso *Schrems (TJCE 2015, 324) (loc. cit.)*. Asunto en el que Sr. *Schrems* presentó ante el comisario una reclamación por la que solicitaba que se prohibiera a Facebook Ireland transferir sus datos personales a EEUU. Fundamenta su reclamación en la falta de tutela de los datos personales en EEUU, en particular al no garantizar una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas. En este sentido, Sr. *Schrems* se refiere a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de EEUU, en particular, las de la *National Security Agency*.

56. El nivel de protección adecuado del Estado de destino que haya sido declarado por la

aparecido en el nuevo Reglamento dado que esta declaración corresponde en exclusiva a la Comisión[57].

2. PAÍSES SIN NIVEL DE PROTECCIÓN SUFICIENTE

18. Como regla general, cuando los datos personales se transfieran a un país que no garantice un nivel adecuado de protección de tratamiento, el artículo 26 de la Directiva exigía que el exportador obtuviera previamente una autorización específica para realizar dicha transferencia. No obstante, esta regla tenía ciertas excepciones que eximían de la tramitación de tal autorización, como cuando las transferencias se encontraran dentro alguno de los supuestos previstos en el número primero de esta disposición (que en términos generales se mantienen en el Reglamento en el art. 49).

19. No era necesario solicitar una autorización previa y específica para la transferencia o grupo de transferencias cuando se encuadrara dentro de alguno de los supuestos tasados del art. 26 1 de la Directiva –y apartados de las letras a) a la j) del artículo 34 de la LOPD–. Esto es, supuestos en los que la transferencia internacional: 1) ha sido consentida de forma inequívoca por el interesado –titular de los datos–; 2) cuando sea imprescindible para ejecutar el contrato entre el interesado y el responsable del tratamiento o las medidas precontractuales adoptadas a petición del interesado; 3) cuando resulta necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en favor del interesado, entre el responsable del tratamiento y un tercero; 4) cuando sea indispensable o sea legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; 5) cuando se requiera para la salvaguardia del interés vital del interesado; 6) cuando tenga lugar desde un registro público concebido para facilitar información al público; 7) cuando la misma resulte de la aplicación de tratados o convenios internacionales en los que sea parte España; 8) aquella se realice a los efectos de prestar o solicitar auxilio judicial internacional; 9) sea necesaria para la prevención o diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios; o finalmente, 10) se trate de una transferencia dineraria conforme a la legislación específica del país de destino.

A sensu contrario, para aquellas transferencias que no encajen en los anteriores supuestos (y el país de destino no goza de un nivel adecuado de protección), el exportador requiere de autorización previa y específica (arts.

AEPD, no requiere una autorización específica (*ex ante* art. 34.k) de la LOPD, y arts. 66.2, 67.1 y 68 del RLOPD).

57. Y así se recoge en la nueva LOPD de 2018, en su artículo 42.1 con remisión al art. 46.2 del Reglamento; al reglamentar los supuestos de transferencias que requieren de previa autorización de la AEPD.

26.2 de la Directiva y 70.2 del RLOPD). La tramitación de esta autorización exige que el solicitante preste las garantías suficientes sobre la protección de la vida, de los derechos y libertades fundamentales de las personas y del ejercicio de los respectivos derechos. Estas garantías pueden realizarse a través de dos posibles vías[58]: a) mediante la incorporación en el contrato celebrado con el importador de los datos de determinadas cláusulas contractuales –ya sean cláusulas contractuales tipo o cláusulas *ad hoc*–; o b) mediante la adopción de reglas corporativas vinculantes por el grupo multinacional de empresas donde se desarrollará la transferencia internacional.

2.1. Las cláusulas contractuales como mecanismo de garantía

20. La incorporación de ciertas cláusulas contractuales en el contrato que vincula al exportador e importador de los datos puede ser suficiente en ciertos casos para que se asegure el nivel de garantía necesario para autorizar la transferencia o grupo de transferencias. En este sentido, el artículo 26.4 facultaba a la Comisión para declarar que determinadas cláusulas contractuales tipo ofrecían garantías suficientes a estos efectos (lo que se mantiene en el Reglamento[59]). En este contexto la Comisión europea ha adoptado cláusulas contractuales tipo para dos posibles supuestos: transferencias internacionales de datos entre responsables del tratamiento o entre un responsable y un encargado del tratamiento[60], y que con la entrada en vigor del Reglamento siguen siendo válidas[61] (al igual que las adoptadas, en su caso, por las Autoridades nacionales de control[62], como son las cláusulas contractuales de la AEPD). Las cláusulas

58. En particular, sobre las diferentes herramientas que se pueden emplear para que las transferencias internacionales se realice de acuerdo a la normativa de protección de datos europea durante la vigencia de la Directiva –y en particular desde la perspectiva de la legislación española–, véase, GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas...", *loc. cit.*, pp. 255 y ss. Trabajo en que se analizan las cláusulas contractuales tipo de la Unión Europea de la Decisión 2010/87/UE, las cláusulas contractuales de la AEPD (encargado a subencargado) y las reglas corporativas vinculantes para los encargados del tratamiento.
59. Art. 46.2 letras c y d.
60. Sobre la diferencia entre ambas figuras véase el Dictamen 1/2010 de 16 de febrero de 2010 del Grupo de Trabajo del Artículo 29 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169), p. 17-24, disponible en *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf*.
61. Un estudio sobre la evolución de las cláusulas tipo en la UE, adoptadas por la Comisión durante la vigencia de la Directiva puede verse en GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas...", *loc. cit.*, apartado V, pp. 257-260.
62. El Grupo de Trabajo del artículo 29 ya apunto esta posibilidad en su Dictamen 3/2009, sobre el principio de responsabilidad, adoptado el 13 de julio de 2010 (00062/10/ES, GT 173), ap. 57. Posibilidad que por otra parte la Comisión reiteró en el Considerando 23 de la Decisión 2010/87/UE, de 5 de febrero de 2010, también conocida como Decisión CCT (DOUE L 39 de 12 de febrero de 2010), que otorga a las autoridades nacionales en materia de protección de datos, la posibilidad de dar mayor flexibilidad en la subcontratación que puedan llevar a cabo encargados nacionales con subencargados que operan en terceros países.

contractuales tipo entre responsables de tratamiento cubren los supuestos de la transferencia de datos personales por responsables/exportadores del tratamiento establecidos en la UE a destinatarios/importadores establecidos fuera del territorio del EEE que actúen también como responsables del tratamiento[63]. Mientras que las cláusulas contractuales tipo entre un responsable y un encargado del tratamiento cubren aquellas transferencias de datos personales por responsables del tratamiento establecidos en la UE/EEE a destinatarios establecidos fuera del EEE que actúen solamente como encargados del tratamiento[64]. Para este tipo de transferencias no se exigen las mismas garantías, porque el encargado del tratamiento actúa exclusivamente en nombre del responsable.

Cabe señalar en este sentido la labor realizada por la AEPD en 2012 cuando elaboró un conjunto de cláusulas contractuales aplicables a contratos de subcontratación de servicios entre encargados establecidos en España y subencargados radicados en terceros Estados, que hasta el momento estaban excluidas de las normas reguladoras de las transferencias internacionales de datos[65] (limitándose a supuestos en los que los que la transferencia se realizara por un responsable del tratamiento, bien a otro responsable, bien a un encargado)[66]. A la luz de este conjunto de cláusulas contractuales, se permite que el solicitante de la autorización de la transferencia internacional sea directamente el encargado del tratamiento y no el responsable del tratamiento (como se exigía hasta ese momento). En este modelo de cláusulas contractuales el responsable debía autorizar previamente al encargado la posterior subcontratación a un subencargado importador y, si es el caso, a posteriores subencargados. Para ello es necesario un marco jurídico básico: el contrato marco responsable-encargado[67], que garantice que por parte del responsable y del encargado se asegure que los tratamientos de datos han sido efectuados y seguirán efectuándose de conformidad con la normativa. Asimismo, en el contrato deberán constar las autorizaciones a la subcontratación y a las transferencias internacionales de

63. *Vid*. las Decisiones 2001/497/CE, de 15 de junio de 2001 (DOCE L 181 de 4 de julio de 2001) y 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la anterior (DOUE L 385 de 29 de diciembre de 2004),.
64. Respecto de las transferencias entre responsable de datos y un encargado del tratamiento –aunque también aplicable entre encargado y subencargado de tratamiento establecidos en un tercer Estados–, puede verse la Decisión CCT que deroga la Decisión 2002/16/CE, de 27 de diciembre de 2001 (DOCE L 51 de 22 de febrero de 2002).
65. 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 (*BOE* de 16-12-2000).
66. En este sentido se manifestó la AEPD en su Informe 582/2004, "Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección. Necesidad de intervención del responsable. Informe 582/2004" (Disponible en la web de la AEPD).
67. Regulado en el artículo 12 de la LOPD y en los artículos 20 a 22 del RLOPD.

datos, debiendo identificarse los ficheros y con previa notificación al Registro General de Protección de Datos[68].

21. Si bien el contenido de este tipo de cláusulas puede ser diverso en la práctica, lo cierto es que por lo general suelen recoger determinadas cuestiones que determinan el carácter favorable de la autorización, a saber: a) una cláusula a favor de tercero para que el afectado pueda hacer valer el contrato en cuestión en caso de vulneración en el tratamiento de sus datos; b) una cláusula de responsabilidad solidaria entre las partes contratantes (responsable/exportador-responsable/importador) o basada en *culpa in eligendo* o *in vigilando* o subsidiaria (responsable/importador-encargado); c) la restricción de transferencias posteriores; d) una estipulación sobre seguridad y control del cumplimiento de las garantías y de los compromisos establecidos en las cláusulas contractuales (tipo o *ad hoc*); y e) una disposición impidiendo la modificación de las cláusulas a favor de tercero[69].

El GT29, en su ya referido informe WP12, analizó cuál debe ser el objetivo de una solución contractual en este sentido. Así, en el contexto de las transferencias de datos a terceros Estados el contrato es un medio que permite al responsable del tratamiento ofrecer garantías adecuadas al transmitir datos fuera de la Unión Europea/ EEE a un país en el que el nivel general de protección no sea suficiente. Por lo tanto, para que una cláusula contractual pueda cumplir esta función, debe compensar satisfactoriamente la ausencia de una protección general adecuada en el ordenamiento jurídico de importación mediante inclusión de los elementos esenciales para garantizar aquella en la situación de referencia. Para evaluar si la solución contractual es adecuada, el punto de partida es delimitar qué se entiende por "garantías suficientes" que exigía el art. 26.2 de la Directiva (art. 46.2 del Reglamento) para integrar el concepto de "protección adecuada". Esta noción integra una serie de principios básicos para la protección de datos, además de ciertas condiciones esenciales para asegurar su eficacia.

El primer requisito es que la solución contractual obligue a las partes a garantizar que se aplique en su integridad el conjunto de principios básicos de protección de datos al tratamiento de los datos transferidos al tercer Estado; esto es: el principio de limitación de objetivos; el principio de proporcionalidad y de calidad de los datos; principio de transparencia; el principio de seguridad; derecho de acceso, rectificación y oposición; restricciones respecto a transferencias sucesivas a personas ajenas al contrato. A estos principios generales ha de añadirse, en su caso, los principios complementarios relativos a los

68. A mayor abundamiento sobre la tramitación para este tipo de operaciones a la luz del modelo de cláusulas contractuales de la AEPD de 2012 véase GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas...", *loc. cit.*, apartado VI, pp. 261-264.
69. *Cf.* GRANDE SANZ, M., "La transferencia internacional...", *loc. cit.*, p. 6.

datos sensibles, a la mercadotecnia directa y a las decisiones automatizadas. Es necesario que el contrato establezca de forma pormenorizada la manera en que el receptor de los datos (importador) debe aplicar estos principios[70], dado que no se cuenta con otros mecanismos adicionales a tales efectos –por ejemplo, del sistema jurídico del Estado de destino[71]–. En lo que respecta a la efectividad de la solución contractual para establecer un sistema de protección de datos suficiente, el GT29 ha concretado tres criterios para evaluar la capacidad del sistema para: 1) ofrecer un nivel satisfactorio de cumplimiento de las normas; 2) facilitar apoyo y asistencia a los interesados en el ejercicio de sus derechos y 3) proporcionar vías adecuadas de recurso a los interesados quienes resulten perjudicados en el caso de que no se observen las normas.

2.2. Reglas corporativas vinculantes para grupos de empresas multinacionales

22. En el ámbito de vigencia de la Directiva, la adopción de reglas corporativas vinculantes resultaba efectiva a los efectos de conseguir la autorización previa a la transferencia cuando aquella se realizase entre empresas de un mismo grupo multinacional. En este sentido, el exportador –el grupo empresarial en cuyo ámbito se pretendía realizar la transferencia–, podía basar su solitud de autorización en la existencia de estas reglas, siempre y cuando fueran vinculantes para todas las empresas del grupo y exigibles por la Autoridad Nacional de Control y por los interesados –para el caso de España, exigibles por la AEPD y por los titulares de los datos que sean objeto de tratamiento en dicha operación de conformidad con el Derecho español (art. 70.4 del RLOPD)–. Mientras que en el sistema anterior eran los ordenamientos jurídicos nacionales los que determinaban si era o no necesario tramitar la autorización específica para realizar las transferencias entre las empresas del grupo empresarial, una vez adoptadas las reglas corporativas vinculantes (para el caso español sí resultaba necesario obtener la autorización previa del Director de la AEPD), esto cambia radicalmente con la entrada en vigor del Reglamento. Con el nuevo Reglamento la adopción de reglas corporativas vinculantes permite que dentro del grupo empresarial multinacional puedan transmitirse datos entre sí sin tener que tramitar autorización previa. Así, el artículo 47 del Reglamento establece que la autoridad de control aprobará normas corporativas de carácter vinculante a las que se podrán unir los grupos de empresas, permitiendo salvaguardar la transferencia de datos. El hecho de que sea el propio Reglamento el que recoja esta posibilidad directamente supone que, por primera vez en materia de protección de datos, las "*Binding corporate rules*" o normas

70. Esto es, el contrato debe especificar los fines de la transferencia de datos, las categorías de los datos transferidos, el plazo límite para su conservación, las medidas de seguridad, etc.
71. Como pudieran ser los códigos de conducta, o las resoluciones de las Autoridades nacionales supervisoras o de control en ejercicio de su función consultiva.

corporativas vinculantes tienen rango legal –al margen de su adopción y actualización por el GT29 durante la vigencia de la Directiva[72]–.

23. La finalidad de la adopción de este tipo de reglas en el marco de la Directiva era doble. Por un lado, facilitar las transferencias de datos dentro del mismo grupo empresarial, estableciendo unos estándares comunes de protección de datos personales y procedimientos uniformes que garanticen su cumplimiento dentro y fuera de la empresa[73] (incluso frente a los titulares de los datos que se consideren afectados por el tratamiento); y, por otro, evitar la posibilidad de que cada Autoridad Nacional de Control donde operen –que suponga tratamiento de datos– las empresas del grupo resuelvan de forma diversa sobre la autorización[74], en relación con las transferencias o grupo de transferencias entre las empresas de ese grupo empresarial multinacional vinculado por las Reglas Corporativas uniformes. Así, era la Autoridad Nacional de Control que se considere líder la que resolvía sobre la idoneidad del conjunto de reglas corporativas vinculantes presentadas. Con el nuevo Reglamento, al eliminarse la necesidad de autorización administrativa previa para las transferencias dentro del grupo de empresas vinculadas por las normas corporativas aprobadas por la Autoridad de Control, ya no existe esa segunda función.

En el nuevo instrumento, también será la Autoridad de Control competente la que aprobará normas corporativas vinculantes –de conformidad con el mecanismo de coherencia del art. 63 –, siempre y cuando cumplan con los requisitos esenciales determinados en el artículo 47; por lo que su contenido resulta esencial para conseguir dicha aprobación[75]. En este contexto, la Comisión tiene asignadas competencias específicas, y podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes (art. 47.3) [76].

---

72. El Grupo de Trabajo del artículo 29 distingue en este sentido entre las reglas corporativas vinculantes dirigidas a los responsables (documentos WP74, WP107, WP108, WP133, WP153, WP154 y WP155) y las reglas dirigidas para los encargados del tratamiento (documentos WP195, WP195a y WP204).
73. La forma de conseguir ese cumplimiento puede ser bien por el cumplimiento de las reglas corporativas vinculantes de forma unilateral por la empresa o mediante su inclusión vía contractual.
74. En particular, para los supuestos en los que no se trate de un procedimiento de reconocimiento conjunto.
75. Al igual que con la Directiva a la luz de los distintos documentos que al efecto fueron adoptados por el GT29 y que han servido de base para esta disposición (*loc.cit.*, nota a pie nº 50).
76. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2, que remite al art. 5 del Reglamento (UE) no 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 Comisión.

24. El contenido específico de las reglas corporativas vinculantes determinará la aprobación o no de las mismas por la Autoridad competente. En este sentido, se específica de forma pormenorizada las formalidades que deben este conjunto de reglas cumplir para alcanzar tal aprobación en el art. 47 del Reglamento. Las futuras normas corporativas vinculantes adoptadas al amparo de esta disposición tendrán que cumplir tres requisitos esenciales para conseguir su aprobación. El primero de ellos exige que este conjunto de reglas sea jurídicamente vinculantes y deban ser cumplidas por todos los miembros del grupo empresarial o unión de empresas. En segundo lugar, deben conferir a los interesados derechos exigibles y, en tercer y último lugar, deben cumplir unas formalidades tasadas en el artículo 47.2 RGPD. Respecto de los elementos esenciales que recoge el número 2 de esta disposición, éstos recuerdan –aunque de manera más profusa y detallada– a los ya referidos por el GT29 en sus diferentes Documentos de Trabajo sobre las reglas corporativas vinculantes –y posteriores adaptaciones– dirigidas a los responsables y a los encargados del tratamiento de datos[77].

IV. EL NUEVO RÉGIMEN UNIFICADO DE LAS TRANSFERENCIAS INTERNACIONALES[78]

25. La aplicación del Reglamento va a suponer significativas diferencias prácticas en el ámbito de las transferencias internacionales en comparación con el régimen anterior. El nuevo instrumento europeo establece un régimen basado en tres grandes supuestos (al margen de las excepciones del art. 49), a saber: 1º transferencias internacionales basadas en una decisión de adecuación (artículo 45); 2º transferencias mediante garantías adecuadas (artículo 46) y 3º supuestos de normas corporativas vinculantes o "Binding corporate rules" (artículo 47). Se trata en realidad de un régimen similar al previsto en la Directiva, pero al unificarse el Derecho europeo en esta materia, se eliminan las posibles disparidades que entre los Estados miembros existían en su puesta en práctica al aplicarse una única normativa. Además, la creación del mecanismo de ventanilla única supone que corresponderá a una sola Autoridad controlar –y decidir– las operaciones transfronterizas de tratamiento de datos que las

77. El respeto a los principios de protección de datos del Derecho europeo y de los Estados miembros; la determinación de los flujos de información y de los fines del tratamiento; la posible limitación de las transferencias a entidades del grupo o de las transferencias posteriores bajo el esquema de garantías; la obligatoriedad interna y externa de las reglas; la posibilidad de obtener una reparación e indemnización por parte del afectado o de plantear, en su caso, recursos; los procedimientos para su ejecución; la cooperación con las autoridades de control; el procedimiento de actualización; y la jurisdicción competente. *Vid*. GRANDE SANZ, M., "Las Transferencias internacionales...", *loc. cit*., p. 7.

78. Un estudio detallado de la cuestión puede verse en *Vid.* PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales", en *Reglamento general..., ob.cit*., pp. 427-460.

empresas realicen en la UE. Con ello se garantizará una interpretación única de la nueva regulación, aunque intervengan varias autoridades nacionales de control en asuntos transfronterizos. Por otro lado, el ámbito de aplicación espacial del Reglamento genera una situación de igualdad de condiciones entre las empresas de la UE y de terceros Estados, en la medida que las empresas domiciliadas fuera de la Unión tendrán que aplicar el mismo régimen que las empresas europeas si suministran bienes y servicios o vigilan la conducta de los ciudadanos en la UE[79].

1. TRANSFERENCIAS BASADAS EN UNA DECISIÓN INSTITUCIONAL DE ADECUACIÓN

26. El artículo 45 determina que se podrá realizar una transferencia –o grupo de transferencias– a un tercer país u organización internacional, sin que sea necesario tramitar autorización administrativa previa, cuando el país de importación de los datos cuente con un nivel de protección adecuado (comparable o "sustancialmente equivalente"[80] al de la UE) declarado por la Comisión. En consecuencia, esta decisión tiene el efecto de permitir la libre circulación de datos personales hacia ese tercer país sin que el exportador de los datos tenga que aportar garantías adicionales ni obtener ningún tipo de autorización[81]. Esta previsión no es nueva, pues como ya se expuso, la Directiva también lo recogía en su art. 25.

27. En los mismos términos que en la Directiva, en el nuevo régimen la Comisión mantiene sus funciones de evaluación de los sistemas jurídicos de los terceros Estados de destino, para determinar si es o no necesaria autorización para la transferencia. A tales efectos, el Reglamento establece un catálogo preciso y detallado de los factores a considerar al evaluar el nivel de protección de un país u organización internacional. En los que se tiene en cuenta tanto el acceso de las autoridades públicas a los datos como la eficacia de los mecanismos de protección existentes y la posibilidad de ejecutarlos o de solicitar, de forma efectiva, una compensación administrativa y judicial (en consonancia con la doctrina *Schrems)*. Para poder adoptar una decisión de adecuación es preciso que existan en el país de destino normas de protección de datos comparables a las vigentes en la UE; lo que comprende tanto

79. Todo ello supone que estemos en un marco de protección de datos integral, unificado y simplificado dentro de la UE.

80. *Vid*. Sentencia *Schrems* (TJCE 2015, 324) (*loc. cit.*), apS. 73, 74 y 96; y considerando 104 del Reglamento.

81. Por consiguiente, las transferencias a dicho país se asimilarán a las transmisiones de datos dentro de la UE, lo que permitirá el acceso privilegiado de dicho Estado al mercado único europeo y la apertura de canales comerciales para los operadores de la UE. En este ámbito, la Comisión ha establecido una serie de criterios a la hora de determinar los terceros países con los que conviene entablar un diálogo sobre adecuación que pueden consultarse en el ap. 3.1 del Documento COM(2017) 7 final/2 (*loc. cit.*).

las medidas de protección sustantivas aplicables a los datos personales como los correspondientes mecanismos de supervisión y recurso disponibles en el tercer país de que se trate (art. 45.2). Igualmente, partiendo de las prácticas ya establecidas durante la eficacia del anterior régimen, el nuevo texto normativo permite expresamente la adopción de decisiones de adecuación con respecto a un determinado territorio, ámbito o sector industrial de un tercer país (lo que se denomina "adecuación parcial o sectorial")[82].

Respecto de las Decisiones adoptadas en este sentido por la Comisión durante la vigencia de la Directiva, éstas siguen vigentes (de conformidad con el artículo 45.9 del Reglamento). Por tanto, hasta sean modificadas, sustituidas o derogadas por nuevas Decisiones de la Comisión, se mantiene la lista de países declarados con nivel de protección adecuado[83].

28. La fundamental diferencia en este ámbito, entre el Reglamento y la Directiva, es que en el nuevo régimen la única autoridad que puede declarar la idoneidad del país de destino de la transferencia por ser adecuado su nivel de protección es la Comisión; sin que se refiera, ni si quiera por omisión, que tal posibilidad pudiera recaer en manos de los Estados Miembros, esto es, las Agencias Nacionales de Control del establecimiento o ubicación del exportador de datos (lo que sí se permitía en el art. 25 de la Directiva).

En cualquier caso, no es absoluto el alcance, ni definitivas las decisiones de la Comisión en este sentido –siendo una presunción *iuris tantum* la adecuación de las garantías–, como ya se manifestó el Tribunal de Justicia durante la vigencia del anterior sistema. De la doctrina *Schrems* se deriva que los actos adoptados por la Comisión en ejercicio de su competencia sobre la adecuación de terceros países de destino para permitir las transferencias, no obstan ni impiden el ejercicio de las facultades de las Autoridades nacionales de control para la protección de datos con fundamento en la normativa sobre derechos fundamentales en la UE (arts. 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea)[84]. Con esta base el Tribunal de Justicia consideró ilegal el acuerdo entre Europa y EEUU[85] de adhesión de entidades establecidas en aquel país a los Principios de Puerto Seguro conforme a un sistema de autocertificación[86]. Como consecuencia directa de esta Sentencia, la Comisión

82. *Vid*. art. 45.1 del Reglamento.
83. *Vid. supra*, ap. III.1, párrafo 13.
84. En concreto, en su nota de prensa de 6 de octubre de 2015 determinó que: "El Tribunal de Justicia estima que la existencia de una Decisión de la Comisión que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos, no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la Unión Europea" (*https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf*).
85. *Vid. Infra.* Ap. V. 1.
86. Entre ellos los principales prestadores de servicios de redes sociales, motores de búsqueda y correo electrónico.

Europea y los EEUU llegaron a un acuerdo –8 meses después– por el que se considera que aquellas organizaciones o entidades establecidas en EEUU que están adscritas al *Privacy Shield*[87] cumplen, *a prori,* con la adecuación exigida de protección y, por tanto, estarán exentas de autorización[88]. Esta aproximación no cambia con la entrada en vigor del Reglamento, como no puede ser de otra forma. A mayor abundamiento –y reforzando esta aproximación– la Comisión deberá revisar, al menos cada cuatro años, todas las decisiones sobre adecuación que emita (art. 45.3); lo que permitirá detectar fácilmente los posibles cambios que se produzcan con relación al nivel de protección ofrecido por cada uno de aquellos países.

2. GARANTÍAS ADECUADAS COMO MECANISMO DE TRANSFERENCIA

29. En defecto de una decisión de adecuación, las transferencias internacionales pueden basarse en instrumentos alternativos de transferencia que ofrezcan garantías adecuadas en materia de protección de datos (del art. 46), siempre que los interesados cuenten con derechos exigibles y acciones legales efectivas –incluso, sin necesidad de solicitar autorización expresa a la Autoridad de Control (art. 46.2)–. Así pues, la concurrencia de las concretas circunstancias o supuestos reglamentados en el artículo 46 genera una presunción favorable (*iuris tantum*) de que la transferencia cuenta con las garantías adecuadas, esto es, equivalentes a las exigidas dentro del EEE.

Por un lado, el número 2 se refiere a aquellos supuestos en los que no se requiere ninguna autorización expresa de una autoridad de control, presumiendo que de darse se cumplen con las garantías debidas: "a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; b) normas corporativas vinculantes de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2; e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas

87. Puede consultarse la lista de la organizaciones y entidades de EEUU adscritas al *Privacy Shield* en *https://www.privacyshield.gov/welcome*.
88. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU.

a los derechos de los interesados". Por otro lado, el número 3 de la disposición refiere a aquellos mecanismos para asegurar las garantías adecuadas que requieren autorización expresa de la Autoridad de Control competente[89]: a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario[90] de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

30. Si bien la posibilidad de recurrir a mecanismos alternativos de transferencia de datos no es una novedad en sí misma[91], sí lo es por cuanto que la reforma operada con el Reglamento formaliza y amplía las posibilidades de utilizar instrumentos existentes, como las cláusulas contractuales tipo[92] y las normas corporativas vinculantes. Además de incorporar nuevas herramientas alternativas de transferencia, como son los códigos de conducta y los mecanismos de certificación (junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de los interesados).

Así, por lo que respecta a las cláusulas contractuales tipo, con la reforma se posibilita su incorporación en los contratos celebrados entre encargados del tratamiento de la UE y encargados del tratamiento terceros país (las denominadas "cláusulas tipo de encargado a encargado"[93] que no existen en la actualidad[94]). Las normas corporativas vinculantes como mecanismos de adecuación también han sido actualizadas, flexibilizando su aplicación. Hasta la entrada en vigor del Reglamento, este tipo de normas se limitaban a los acuerdos entre entidades pertenecientes a un mismo grupo de empresas, si bien ahora pueden ser invocadas por uniones de empresas dedicadas a una actividad económica conjunta, sin que estas tengan que pertenecer necesariamente al mismo grupo empresarial[95]. Además, cuando las transferencias a terceros países estén basa-

89. En caso de España, las autorizaciones otorgadas por la AEPD previamente a la aplicación del Reglamento seguirán siendo válidas a estos efectos.
90. Como por ejemplo, subencargados de datos en el Estado de importación –tal y como se recogía ya por la AEPD desde 2012–.
91. A este respecto, véase, por ejemplo, la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE a raíz de la sentencia *Schrems*, COM(2015) 566 final de 6.11.2015.
92. Las cláusulas tipo de protección de datos adoptadas por la Comisión durante la vigencia de la Directiva siguen siendo válidas: Decisiones 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales entre responsables del tratamiento a un tercer país y la ya referida Decisión CCT.
93. *Vid*. el artículo 46.2, letras c) y d), y el considerando 168.
94. En este contexto, el Comité Europeo de Protección de Datos podría continuar con la labor iniciada por el Grupo de Trabajo del artículo 29 en la redacción de cláusulas contractuales tipo de encargado a encargado.
95. *Vid*. los artículos 46. 2, letra b), 47 y el considerando 110.

das en cláusulas contractuales tipo o en normas vinculantes corporativas se exime a los exportadores de datos de las obligaciones generales de notificación previa a las autoridades nacionales de control y de la autorización (art. 46.2) –lo que reduce significativamente los trámites burocráticos–.

31. El Reglamento introduce también nuevos instrumentos de transferencia internacional (art. 46.2 letras e y f). En este sentido, los responsables y encargados del tratamiento podrán utilizar, en determinadas condiciones[96], códigos de conducta o mecanismos de certificación aprobados (como sellos y marcas de privacidad) para proporcionar las garantías adecuadas exigidas[97]. Asimismo, se recoge la posibilidad de aportar garantías adecuadas para las transferencias de datos entre autoridades u organismos públicos sobre la base de acuerdos internacionales o administrativos (artículo 46, apartado 2, letra a), y apartado 3, letra b).

En este marco, la Comisión está llamada a colaborar con las partes interesadas para crear mecanismos alternativos de transferencia de datos personales adaptados a las necesidades o condiciones particulares de determinados sectores industriales, modelos de negocio u operadores.

3. EL CONSENTIMIENTO DEL INTERESADO COMO PIEDRA ANGULAR

32. No supone una novedad la previsión en el Reglamento de excepciones a la aplicación del régimen general para las transferencias internacionales (artículo 49); permitiendo al exportador –el responsable o el encargado– que pueda mover los datos fuera del espacio europeo sin cumplir con ninguna de las situaciones previstas para este tipo de operaciones en situaciones concretas. La nueva regulación sigue en este ámbito la línea marcada por la Directiva (art. 26.1), recogiendo condiciones ya previstas (como, por ejemplo, la prestación de consentimiento, la ejecución de un contrato o razones importantes de interés público, etc.), si bien de forma más amplia y específica; lo que va a tener significativas consecuencias prácticas para su apreciación como excepción. Además, se incorpora una nueva condición de excepción respecto a las transferencias que puedan tener lugar en aras de los intereses legítimos de una determinada empresa. Esta excepción tiene un alcance marcadamente limitado y exige la concurrencia acumulativa de determinadas condiciones para su consideración (art. 49.1. II): a) que la transferencia no sea repetitiva; b) que

96. Los responsables o encargados del tratamiento de terceros países podrán adherirse a un código de conducta o mecanismo de certificación de la UE mediante la asunción de compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar las garantías de protección de datos contenidas en dichos instrumentos (artículo 42.2).

97. Con estas nuevas herramientas se busca ofrecer soluciones que se adapten mejor a las exigencias de las transferencias internacionales en determinados ámbitos o sectores industriales o flujos de datos concretos, que tienen características y necesidades específicas.

afecte solo a un número limitado de interesados; c) que sea necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado; d) que el responsable del tratamiento evalué todas las circunstancias concurrentes en la transferencia de datos y, con base en esta evaluación, e) ofrezca garantías apropiadas con respecto a la protección de datos personales. En este supuesto el responsable del tratamiento deberá informar a la autoridad de control de la transferencia. Asimismo, además de la información a que hacen referencia los artículos 13 y 14 del Reglamento, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

33. Dada la relevancia práctica que la posible concurrencia de alguno de estos supuestos excepcionales supone, su delimitación resulta esencial. En este sentido, y para coadyuvar en este objetivo, fueron publicadas por el CEPD sus Directrices sobre las excepciones previstas en el artículo 49 del Reglamento[98], que viene completar la labor iniciada por el GT29 en este ámbito con el documento WP114[99]. En este contexto, muestra particular importancia la nueva reglamentación sobre la verificación consentimiento del interesado, por las evidentes consecuencias prácticas que van a derivarse de su aplicación en el ámbito de las transferencias internacionales de datos[100]; de lo que da cuenta los trabajos y documentos dedicados a esta cuestión por los organismos especializados, como son las Directrices del GT29 (documento en el que se analizan los requisitos para obtener y demostrar el consentimiento válido conforme al Reglamento[101]). Consecuentemente, este es un aspecto que merece especial análisis en este estudio.

3.1. El consentimiento como condición del tratamiento

34. Una de las diferencias sustanciales del nuevo sistema es la reglamentación del consentimiento del interesado como excepción al cumplimiento del régimen general de transferencias internacionales. De conformidad con el artículo 4 apartado 11 del Reglamento, cualquier consentimiento en el ámbito de este instrumento debe ser prestado de forma libre, específica, informada e inequívoca. Respecto de esta última condición, el artículo 49.1 letra a) se manifiesta más estricto para las transferencias internacionales de datos exigiendo que debe ser explícito. Se requiere una manifestación del consentimiento –in-

98. *Loc. cit.*, nota a pie nº 25.
99. *Loc. cit.*, nota a pie nº 27.
100. De conformidad con el art. 49.3, las autoridades públicas no pueden invocar esta excepción (art. 49.1 letra a) en el ejercicio de sus poderes públicos, al igual que ocurre con las excepciones contenidas en las letras b y c de este mismos apartado 1 de esta disposición.
101. Documento WP 259, *Guidelines on Consent under Regulation 2016/679*, adoptado el 28 de noviembre de 2017 (disponible en versión inglesa aquí: *file:///C:/Users/Usuario/Downloads/wp259_enpdf.pdf*)

formado– expresa e inequívoca (art. 49.1, letra a), frente al consentimiento inequívoco que exigía la Directiva –expreso o implícito– (art. 26.1 letra a). Esto supone que con la nueva redacción se prohíbe en la práctica el consentimiento tácito (que no se expresa o no se dice, pero se supone o se sobreentiende), que era una de las fórmulas más utilizadas por las empresas o instituciones responsables del tratamiento de acuerdo con el anterior régimen. En consecuencia, los consentimientos obtenidos con anterioridad a la entrada en vigor del Reglamento solo seguirán siendo válidos, en el ámbito de las transferencias internacionales, si se obtuvieron respetando los criterios establecidos por el art. 49: consentimiento expreso e inequívoco.

35. Resulta necesario delimitar los distintos tipos de consentimiento exigibles en materia de protección de datos, tras la reforma, en función del supuesto en cuestión[102]. El nuevo instrumento establece un alto estándar para el consentimiento, en la medida que éste garantiza a los interesados la elección y control legítimo sobre cómo usar sus datos personales. A tales efectos, se define en el artículo 4.11 lo que se entiende por consentimiento del interesado para que tenga efectos jurídicos en el ámbito del Reglamento, lo que junto al artículo 7, delimitan las condiciones para que el consentimiento sea considerado válido[103]. De esta definición se deduce que el consentimiento debe otorgarse mediante una clara acción afirmativa, que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado. Necesariamente esto supone que ciertas prácticas muy extendidas en este ámbito por las empresas responsables para recabar el consentimiento devienen inválidos en el nuevo marco legal.

Con la reforma, la licitud del tratamiento se hace depender de que el interesado haya prestado su consentimiento (válido) para el tratamiento de sus datos para uno o varios fines específicos[104]; por lo que en primer lugar ha de poder constatarse la existencia de tal consentimiento para que sea inequívoco. Ahora bien, el consentimiento puede ser inequívoco y otorgarse de forma implícita o de forma expresa. Como regla general, se va a exigir que el titular de los datos haya prestado su consentimiento sin mayor precisión en cuanto a la forma de prestarlo; por lo que cabría el consentimiento inequívoco e implícito. Así, para que el consentimiento sea válido bastaría una manifestación del

102. Sobre el requisito de consentimiento explícito y los demás requisitos aplicables necesarios para que el consentimiento se considere válido a la luz de este instrumento, pueden verse las Directrices sobre el consentimiento del Grupo de Trabajo del artículo 29, documento WP259 (*loc. cit.*), respaldadas por el CEPD. De hecho, En las directrices del CEPD expresamente se indica que la sección relativa a la interpretación del art. 49.1 a) del Reglamento, debe leerse junto con el documento WP29, en la medida que proporcionan un análisis más detallado sobre la interpretación de las condiciones generales y los criterios de consentimiento bajo el Reglamento.

103. También los artículos 32, 33, 42 y 43 dan una mayor orientación sobre el consentimiento.

104. *Vid*. art. 6.1 a) y Considerando 40.

interesado o una acción positiva del mismo, como por ejemplo el "seguir navegando por la web" para la aceptación de cookies (Considerando 32). El consentimiento inequívoco implícito puede considerarse como una actualización del consentimiento tácito. De tal forma que, de la acción implícita efectuada por el interesado, se deduzca que éste da su consentimiento sin lugar a dudas –lo que estaba admitido en el anterior régimen para transferencias de datos internacionales hasta la entrada en vigor de Reglamento[105]–. No es admisible –ni lo era durante la vigencia de la Directiva– la omisión del interesado como manifestación del consentimiento, es decir, éste tiene que hacer algo que solo puede ser interpretado como que acepta el tratamiento[106]. El término "acción afirmativa clara" de la definición de consentimiento (art. 4) supone que ciertos comportamientos anteriormente admisibles no lo sean en el nuevo marco. Así, por ejemplo, las casillas previamente marcadas por defecto[107], el silencio o inactividad del interesado, incluir el consentimiento como parte de los términos y condiciones generales o el uso de casillas de *opt out* no resultan ahora aceptables[108]. Este requisito de la acción afirmativa clara es operativo para el consentimiento normal, por lo que para los supuestos en los que se requiera el consentimiento explícito, el estándar de exigencia para su obtención será mayor. Para que considera que se trata de un consentimiento explícito éste no debe dejar lugar a la libre interpretación y debe ser recogido de forma clara y precisa –ya sea manifestado de manera escrita o hablada–. Consecuentemente, en aquellos supuestos en los que deba de recabarse por los responsables el consentimiento explícito del interesado, deberán asegurarse de su obtención de manera indiscutible. Como es el caso del tratamiento de datos sensibles, decisiones automatizadas y transferencias internacionales, para los que se exige que exista un consentimiento expreso e inequívoco del interesado. Finalmente, en la medida que el consentimiento puede prestarse para uno o varios fines específicos, una firma para autorizar varios consentimientos significa que los mismos son otorgados de forma positiva mediante un único acto jurídico, y el hecho de obtener varios consentimientos a la vez no significa que sean

105. En la medida que el art. 26.1 letra a) de la Directiva solo exigía que el interesado hubiera prestado su consentimiento inequívoco. Solo se hacía referencia en la Directiva al consentimiento explícito del interesado para legitimar, en su caso –y siempre que no lo prohibiera la legislación nacional del Estado Miembro–, el tratamiento datos que por su naturaleza pudieran atentar contra las libertades fundamentales o la intimidad por lo que no deben ser objeto de tratamiento alguno como son datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad (Considerando 33 y art. 8.2 letra a) de la Directiva).
106. Por ejemplo, el acceso a una zona con videovigilancia con un cartel que informa de la existencia de cámaras.
107. De esta forma se elimina cualquier eficacia del consentimiento pre-marcado de las ventanillas de diálogo que pueden aparecer mientras se navega por Internet.
108. En este sentido se ha manifestado el Grupo de Trabajo del artículo 29 en su documento WP259 (*loc. cit.)*.

otorgados por omisión. Asimismo, para que el consentimiento sea libremente prestado no se debe supeditar el consentimiento general a finalidades innecesarias, dentro de la ejecución de un contrato o de la prestación de un servicio.

3.2. Trasferencias internacionales basadas en el consentimiento

36. El nuevo régimen del consentimiento como base para las transferencias internacionales (art. 49.1 letra a) resulta mucho más restrictivo y específico que lo reglamentado en este sentido por la Directiva (art. 26.1 letra a). Son tres los requisitos concurrentes que se exigen ahora para que el consentimiento del interesado pueda constituirse como fundamento para la transferencia internacional de sus datos sin tener que someterse al régimen general: a) debe ser explícito; b) específico para esa transferencia de datos o conjunto de transferencias y c) informado previamente de los posibles riesgos de la transferencia para el interesado[109]. Habiéndose ya abordado anteriormente la cuestión de la naturaleza explícita del consentimiento, nos centraremos en los otros dos elementos que están estrechamente relacionados entre sí.

37. El carácter "específico" del consentimiento exigido para su consideración como válido en este contexto tiene la finalidad de "garantizar un grado de control y transparencia para el interesado". Para conseguir tal objetivo el GT29 ha identificado tres componentes que los responsables del tratamiento deben garantizar al recabar el consentimiento[110]: a) especificar la finalidad; b) granularidad en las solicitudes de consentimiento y c) separación clara de la información relacionada con la obtención de consentimiento para actividades de tratamiento de datos a partir de información sobre otros temas. En consecuencia, si el responsable quiere utilizar los datos para nuevas finalidades, será necesario que obtenga el consentimiento para tal finalidad.

Así pues, es necesario que el exportador en el momento de realizar la transferencia –o grupo de transferencias– haya recabado dicho consentimiento específico del interesado al efecto. Esta aproximación tiene relevantes consecuencias prácticas en las operaciones de las compañías que operan en la UE, por cuanto que en algunas ocasiones será imposible obtener el consentimiento del interesado para futuras transferencias al tiempo de la recopilación de los datos (si no se conoce la existencia y las circunstancias específicas de una transferencia en el momento en que se solicita el consentimiento, no se puede evaluar su impacto sobre el interesado). En consecuencia, el exportador de datos (responsable o encargado) debe asegurarse de obtener el consentimiento específico del interesado antes de que se realice la transferencia, incluso si esto se produce después de que se haya recopilado la información. Es posible recabar el consentimiento específico del interesado, antes de la transferencia y en

109. *Vid.* Documento WP259 (*loc. cit.*).
110. *Ibídem.*

el momento de la recopilación de los datos personales, siempre que esta transferencia concreta se le dé a conocer y las circunstancias de la transferencia no cambien después de que se haya prestado el consentimiento específico. Por lo tanto, el exportador de datos debe asegurarse de que se le facilita toda la información previamente al interesado para que su consentimiento sea informado. Parece claro que la aproximación por la que se optado en el Reglamento conduce necesariamente a que el elemento de especificidad está estrechamente relacionado con el requisito del consentimiento informado[111]. En este sentido, las Directrices del GT29 refuerzan la condición de que el consentimiento debe ser informado y el CEPD especifica aún más en los términos de esa información previa que obligatoriamente debe facilitarse al interesado antes de prestar su consentimiento específico.

38. Las Directrices establecen el contenido mínimo de la información que debe facilitarse al interesado para que se considere que el consentimiento prestado es válido:1) la identidad del responsable; 2) la finalidad de cada una de las operaciones de tratamiento; 3) el tipo de datos que se recopilarán; 4) el derecho a retirar el consentimiento; 5) detalles de cualquier tratamiento automatizado propuesto, incluido la creación de perfiles y, finalmente, cuando corresponda 6) los posibles riesgos de las transferencias de datos a terceros países a falta de una decisión de adecuación de la Comisión Europea y las salvaguardas apropiadas. Además de concretar ese contenido mínimo en cuanto al fondo, también se establecen los requisitos de forma para asegurar que tal información sea comprensible para el interesado. Así, el responsable debe garantizar la utilización de un lenguaje claro y sencillo; por lo que mensaje debe ser fácilmente comprensible para el usuario medio. Por consiguiente, los responsables no pueden usar largas políticas de privacidad ilegibles y el consentimiento debe ser claro y distinguible de otros asuntos y proporcionado de manera inteligible y forma accesible[112].

Para el CEDPD esta condición es especialmente importante, dado que reafirma y especifica en mayor medida el requisito general de consentimiento informado aplicable a cualquier consentimiento (art. 4.11). Por tanto, se trata de una exigencia que va más allá de la exigencia general para que el consentimiento se configure como base legal para el tratamiento legítimo de datos (art. 6.1 a), esto es, que el interesado esté debidamente informado con antelación

111. La necesidad de que el consentimiento sea informado, no solo en el ámbito de las transferencias internacionales sino en general en el contexto general del tratamiento de datos personales, se deriva del complimiento de las exigencias generales de transparencia recogidas en los artículos 13 y 14 del Reglamento. Sobre esta cuestión, en profundidad, véase el documento "Guidelines on transparency under Regulation 2016/679", adoptado el 25 de noviembre de 2017 y última revisión el 11 de abril de 2018 (documento, WP 260rev.01). Texto disponible en inglés: *file:///C:/Users/user/Downloads/20180413_Article29WPTransparencyGuidelinespdf.pdf*).

112. *Vid*. documento WP259, p. 13 y ss. (*loc. cit*.).

de los hechos específicos del tratamiento –que en caso de una transferencia de datos serían las circunstancias concretas de aquella[113]–. Pero cuando los datos personales se transfieren a un tercer Estado, el art. 49.1 a) requiere también que los interesados estén informados de los riesgos específicos derivados del hecho de que sus datos se transferirán a un país que no proporciona la protección adecuada y que no se están implementando las salvaguardas apropiadas para brindar protección a los datos –según los estándares de la UE–. También debe facilitarse toda la información referida a los destinatarios de los datos. El suministro de esta información es esencial para permitir que el interesado preste su consentimiento con pleno conocimiento de los específicos hechos y concretas circunstancias de la transferencia, en consecuencia, si ésta no es suministrada la excepción no se aplicará.

Por tanto, es necesario que se indique al interesado en el momento de recabar su consentimiento que éste es la base legal para la transferencia, debiendo especificar todos los destinatarios o categorías de destinatarios, todos los países a los que se transfieren los datos y que el tercer país al que se transferirán los datos no prevé un nivel adecuado de protección basado en una decisión de la Comisión Europea, ni tampoco existen medidas adoptadas para asegurar las garantías adecuadas o apropiadas[114]. Y respecto de este último requisito, se debe proporcionar información sobre los posibles riesgos para el interesado como consecuencia de esa falta de protección adecuada y de la ausencia de salvaguardias[115]. En aquellos casos en los las transferencia se realice después de que se haya recopilado la información personal del interesado, el exportador de datos debe informar a aquél previamente de la transferencia y de sus riesgos antes de que tenga lugar, con el fin de obtener su consentimiento explícito para legitimar la transferencia propuesta.

39. De todo este análisis realizado, cabe concluir que el Reglamento establece un umbral alto para el uso del consentimiento como excepción en el régimen de las transferencias internacionales de datos; en el que exportador deben demostrar que han obtenido un consentimiento válido para la transferencia –la carga de la prueba recae, por tanto, sobre el responsable o encargado[116]–, y debe asegurarse de mantenerlo[117]. Este estándar, combinado con el

113. Es decir, la identidad del controlador de datos, el propósito de la transferencia, el tipo de datos, la existencia del derecho a retirar el consentimiento, la identidad o las categorías de destinatarios.

114. Este último requisito también se deriva del deber de informar a los interesados (Artículos 13 (1) (f) y 14 (1) (e)).

115. Dicha notificación, que podría estar estandarizada, debería incluir, por ejemplo, que en el tercer país puede que no haya una autoridad de supervisión y/o principios de procesamiento de datos y/o los derechos de los interesados pueden no estar previstos en el tercer país (Guidelines 2/2018 del CEPD, p.8, *loc. cit)*.

116. El responsable también deberá poder demostrar que el interesado fue informado y que cumplió con todos los criterios relevantes para un consentimiento válido.

117. El fundamento de esta obligación es la rendición de cuentas que recae sobre el responsa-

hecho de que el consentimiento proporcionado por un interesado puede ser retirado en cualquier momento[118], podría conducir a la conclusión de que quizá el consentimiento podría no ser una solución viable y efectiva a largo plazo para legitimar las transferencias fuera de la UE[119].

V. TRANSFERENCIAS DE DATOS DESDE EUROPA A ESTADOS UNIDOS

40. Es evidente que los flujos de datos entre la UE y Estados Unidos son esenciales en las relaciones económicas entre ambos continentes, lo que repercute directamente en el desarrollo de la economía global. En un contexto como éste deviene esencial contar con un marco normativo estable que permita que el flujo transatlántico de este tipo de datos se realice con las máximas garantías, de manera que se respeten los derechos y libertades de los interesados (entre los que está el derecho fundamental al tratamiento de datos personales de los ciudadanos europeos). Actualmente este marco lo constituye el denominado acuerdo de *Privacy Shield* o Escudo de Privacidad. Si bien, al igual que ocurrió con su predecesor, el Acuerdo de Puerto Seguro[120] (declarado nulo tras la sentencia *Schrems* por el Tribunal de Justicia) su eficacia está en entredicho[121], y es posible que en un futuro próximo se vuelva a una situación de inseguridad jurídica en este sentido[122].

---

ble. Así, el responsable puede adoptar ciertas medidas para mantener el consentimiento del interesado. Por ejemplo, cuando el consentimiento se obtiene mediante una página web, la empresa responsable puede guardar la información sobre la sesión en la que se expresó el consentimiento. También puede mantener un registro de las declaraciones de consentimiento recibidas, para que pueda mostrar cómo y cuándo se obtuvo el consentimiento y la información proporcionada en el momento.

118. Asimismo, el reglamento no establece un límite de tiempo específico para la duración del consentimiento, que dependerá del contexto, el alcance del consentimiento original y las expectativas del individuo.

119. Precisamente en este sentido se ha manifestado el CEPD en sus Directrices sobre la interpretación del art. 49 del Reglamento. *Vid*. Guidelines 2/2018 del CEPD, *ibídem*.

120. Sobre los principios de Puerto Seguro, sus orígenes, evolución y su inadecuación para cumplir los objetivos perseguidos, lo que se ha verificado con su posterior anulación, véase, DE MIGUEL ASENSIO, P.A., "Transferencias de datos personales entre la UE y EEUU: el futuro de los Principios de Puerto Seguro", 4 de diciembre de 2013 (*http://pedrodemiguelasensio.blogspot.com/2013/12/transferencias-de-datos-personales.html*).

121. *Vid*. Asunto T-738/16, *loc. cit.*

122. Similar a la vivida tras la anulación del acuerdo de Puerto seguro (Decisión 2000/520/CE de la Comisión, *loc.cit.*). Un análisis de las consecuencias que supuso dicha anulación para las empresas europeas, *vid*. PIÑAR MAÑAS, J. L., "La mayoría de las transferencias de datos desde Europa a EEUU, en el aire", *Abogacía Española*, 26 octubre de 2015. Disponible en *https://www.abogacia.es/2015/10/26/la-mayoria-de-las-transferencias-de-datos-desde-europa-a–eeuu-en-el-aire/* (consultado el 19 de octubre de 2018); LÓPEZ LAPUENTE, L., "Las transferencias de datos a EEUU: la transición del Safe Harbor al Privacy Shield y un paso más allá", *Actualidad Jurídica Uría Menéndez, nº 45, año 2017, pp. 36-38. Disponible en https://www.uria.com/documentos/publicaciones/5315/documento/art 03.pdf?id=6965*; ORTEGA GIMÉNEZ, A., "Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield", *Revista Lex Mercatoria*, Nº. 4, 2016, pp. 85-90.

Dada la transcendencia práctica que ha tenido la anulación del Acuerdo de Puerto Seguro y la relevancia de la doctrina *Schrems* en régimen jurídico de las transferencias internacionales de datos, procede referir las líneas fundamentales esta resolución. De esta manera, podrá contextualizarse el marco jurídico actual y su eventual evolución en relación con el flujo de datos transatlántico.

1. DE LOS PRINCIPIOS "SAFE HARBOUR" AL ACUERDO "PRIVACY SHIELD"

41. En primer lugar, al margen de la evidente relevancia práctica que ha supuesto la sentencia *Schrems* en el ámbito de las transferencias internacionales de datos entre empresas y organizaciones de la UE y EEUU (en la medida que dejaba sin efectos el marco jurídico que hasta ese momento facultaba este tipo de operaciones), con esta resolución el Tribunal de Justicia pone la protección de datos en el lugar que le corresponde: entre los derechos fundamentales de los ciudadanos europeos[123]. Las revelaciones que quedaron al descubierto con ocasión de este caso, demostraron la existencia de programas de acceso masivo desde Estados Unidos a datos personales de ciudadanos europeos que resultaban incompatibles con el derecho fundamental a la protección de datos (inadmisible desde el punto de vista del Derecho europeo), lo que determinó el sentido de la sentencia. Con la posición que toma el Tribunal de Justicia en su resolución se refuerza la eficacia extraterritorial del derecho fundamental a la protección de los datos personales de los ciudadanos europeos.

El Tribunal de Justicia parte de la premisa de que el sistema establecido con el Acuerdo de Puerto Seguro no era contrario al art. 25.6 de la Directiva, ahora bien, su fiabilidad descansaba "en el establecimiento de mecanismos eficaces de detección y control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales y, en especial, del derecho al respeto de la vida privada y del derecho a la protección de los derechos personales" (ap. 81, *Schrems*). Quedando demostrado que no se cumplía¸ sino que al contrario este mecanismo facilitaba la vulneración sistemática de los estándares de protección de la legislación europea con respecto a datos personales transferidos de la UE a EEUU por empresas adheridas a este sistema[124].

Las cuestiones analizadas por el Tribunal (que causaron la anulación de

123. Un análisis pormenorizado de esta sentencia puede verse en el apartado "Transferencias de datos desde Europa a Estados Unidos", de PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos..., ob. cit.*, pp. 201-205. Sobre las principales consecuencias derivadas de la resolución, véase de MIGUEL ASENSIO, P.A., "Un par de reflexiones sobre la sentencia Schrems", *loc. cit.*

124. En este sentido se ha manifestado DE MIGUEL ASENSIO, P.A., "Un par de reflexiones sobre la sentencia Schrems", 16 de octubre de 2015 (*https://pedrodemiguelasensio.blogspot.com/2015/10/un-par-de-reflexiones-sobre-la.html*).

la Decisión) son esenciales para evaluar la validez de futuros acuerdos como marco regulador adecuado, para garantizar las transferencias de datos desde la UE a EEUU –y con terceros Estados en general–. Estas pueden concretarse en las siguientes[125]:

1) La existencia de una decisión de la Comisión declarando que un tercer Estado dispone de un nivel adecuado de protección de datos no puede dejar sin efecto ni limitar las facultades atribuidas a las Autoridades nacionales de control en virtud de la CDFUE y de la Directiva.

2) La Directiva no impedía a las Autoridades controlar este tipo de transferencias, lo que suponías que éstas pueden valorar, con total independencia, si se cumplen o no con el nivel de protección exigido por la Directiva. En consecuencia, para el Tribunal de Justicia la Comisión se excedió de sus competencias al privar en su Decisión 2000/520/CE a las Autoridades Nacionales[126] de sus facultades cuando una persona impugnara la compatibilidad de la Decisión con la protección a la vida privada y de las libertades y derechos fundamentales de las personas.

3) Para la adopción de la Decisión la Comisión se limitó a analizar el régimen de puerto seguro, cuando debería haber comprobado si EEUU ofrecía efectivamente, en razón de su legislación interna o de sus compromisos internacionales, un nivel de protección de los derechos fundamentales que fuera sustancialmente equivalente al garantizado dentro de la UE en virtud de la Directiva, interpretada a la luz de la CDFUE.

4) El acuerdo de Puerto Seguro resultaba aplicable a las entidades y empresas de EEUU adheridas al mismo, pero no a las autoridades públicas de EEUU. Además, las exigencias de seguridad nacional, interés público y cumplimiento de la ley de EEUU prevalecían sobre el régimen establecido por este Acuerdo y, por tanto, las entidades de EEUU estaban obligadas a dejar de aplicar, sin limitación, las reglas del Acuerdo cuando entraran en conflicto con tales exigencias. En consecuencia, el Acuerdo de puerto seguro permitía injerencias de las autoridades públicas de EEUU en los derechos fundamentales de los ciudadanos europeos sin que la Decisión hubiera contemplado la existencia en EEUU de reglas que las limiten o que establezcan una protección eficaz a los afectados ante este tipo de injerencias[127].

5) La legislación de EEUU autoriza la conservación generalizada de todos los datos personales transferidos desde la UE, sin que se establezca al efecto

125. *Vid.* GRANDE SANZ, M., "La transferencia internacional...", *loc. cit.,* pp. 14 y ss.

126. Cuestión distinta es que la competencia para declarar la invalidez de tal Decisión corresponda al Tribunal de Justicia.

127. La Comisión ya había señalado estas injerencias en sus Comunicaciones COM (2013)846 final y COM (2013)847 final, así como la necesidad de revisar y mejorar el Acuerdo de Puerto Seguro.

ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin que se reglamente ningún criterio objetivo que permita limitar el acceso de las autoridades públicas estadounidenses a los datos o su utilización posterior. Todo ello supone que no se respeta un nivel de protección equivalente al garantizado en la UE.

6) En la normativa EEUU no se prevé que el interesado (el ciudadano europeo titular de los datos transferidos) pueda ejercer ciertas acciones en Derecho que le permitan acceder a sus datos personales o para solicitar su rectificación o supresión, de tal manera que también así se vulnera el contenido esencial del derecho fundamental a la tutela judicial efectiva.

42. La declaración de la invalidez de la Decisión de la Comisión por la que se aprobaba el acuerdo de *Safe Harbor* o Puerto Seguro, supuso que aquellas empresas o entidades estadounidenses adheridas al sistema de *Safe Harbor* perdieran automáticamente su condición de entidad adecuada para ser destinatarias de datos personales transferidas desde la UE. Esto trajo como consecuencia que, durante los meses que siguieron a la declaración de invalidez del Acuerdo de *Safe Harbor*, miles de empresas europeas buscaron mecanismos jurídicos alternativos que hicieran lícitas sus transferencias de datos a EEUU o que mitigaran los riesgos de incumplimiento de la normativa europea de protección de datos: la firma de cláusulas contractuales tipo de la UE, de cláusulas *ad hoc* o el recurso las Reglas corporativas vinculantes[128] (mecanismos previstos en la Directiva, pero implementados por los Estados Miembros de distinta forma, por lo que los resultados eran inciertos y desiguales en función del Estado miembro de referencia).

La ausencia de soluciones fáciles que fueran alternativas reales al inválido sistema de *Safe Harbor*, ponía de manifiesto que la única solución pasaba necesariamente por encontrar una solución política, esto es, un nuevo acuerdo político entre la UE y EEUU. Así, el 2 de febrero de 2016 la Comisión Europea alcanzó un acuerdo político con los EEUU para el establecimiento de un nuevo marco para las transmisiones de datos personales entre ambos. El 29 de febrero, la Comisión Europea hizo público un proyecto de decisión sobre la idoneidad de este nuevo marco (el "proyecto de decisión") y sus siete anexos, incluidos los principios del escudo protector de la intimidad y una serie de declaraciones y compromisos por escrito por parte de funcionarios y autoridades

128. Al margen del posible recurso a otras soluciones que permitieran soslayar la aplicación del régimen de las transferencias internacionales. Como sería, por ejemplo, la aplicación de técnicas que permitan convertir los datos personales en datos anónimos; o que concurriera alguna de las excepciones a la aplicación del régimen general de las transferencias (art. 26 Directiva, art. 49 del Reglamento); o el desarrollo de códigos de conducta de contenido similar a las Reglas corporativas vinculantes o la creación de mecanismos de certificación que permitiesen avalar, de alguna manera, el cumplimiento de las garantías necesarias y facilite, en su caso, la obtención de la autorización –en los términos del art. 46 del Reglamento–.

estadounidenses[129], que fue sometido a la evaluación de las instituciones especializadas en la matera como es el GT29[130] y el Supervisor Europeo de Protección de datos[131] (en adelante, SEPD). Lo que condujo finalmente a la adopción por la Comisión Europea, el 12 de julio de 2016, del acuerdo de adecuación para las transferencias de datos a EEUU denominado *Privacy Shield* o Escudo de Privacidad ()Decisión de Ejecución (UE) 2016/1250[132], después de más de dos años de negociación. El objetivo fundamental del acuerdo de *Privacy Shield* era claro: subsanar los principales defectos del acuerdo *Safe Harbor*, reestableciendo así la confianza de los europeos en la economía digital y en las transferencias a EEUU. Para ello se trata de fortalecer los derechos fundamentales de los ciudadanos europeos, creando un marco jurídico más consistente de protección que satisfaga las recomendaciones de la Comisión y las exigencias del Tribunal de Justicia. A estos efectos, una de las novedades esenciales del acuerdo de Escudo de Privacidad[133] es su ámbito de aplicación, pues éste reglamenta tanto las transferencias internacionales de carácter comercial como el acceso de las autoridades públicas de EEUU a los datos transferidos desde la UE, incluso por motivos de seguridad nacional –lo que, sin embargo, no significa que su inclusión evite que en la práctica siga prevaleciendo la normativa estadounidense en este ámbito[134] y por tanto su eficacia se vea matizada

129. Decisión de Ejecución de la Comisión de 9 de noviembre de 2018 (JUST.C.4/CM) con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección conferida por el escudo protector de la intimidad UE-EE. UU., disponible en inglés en: *http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf*.
130. *Vid*. Dictamen del Grupo de Trabajo del Artículo 29, de 13 de abril de 2016 (01/2016), sobre el proyecto de decisión de adecuación del Escudo de la privacidad UE-EEUU (*http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf*) y su declaración de 26 de julio de 2016 (*http://ec.europa.eu/justice/article-29/press-material/press-release/art 29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf*).
131. *Vid*. Dictamen 4/2016 del Supervisor Europeo de Protección de Datos, de 30 de mayo de 2016, sobre el proyecto de decisión relativo a la adecuación del escudo protector de la intimidad entre la UE y los Estados Unidos (DOUE 257/8 de 15.7.2016, p. 20).
132. *Loc. cit*.
133. El texto puede consultarse en *http://ec.europa.eu/justice/data-protectio/iles/privacy-shield-adequacy-decision_en.pdf*.
134. A modo de ejemplo, al poco de entrar en vigor este acuerdo, ya se manifestaron los primeros conflictos con el ordenamiento estadounidense. Así, el 25 de enero de 2017, la primera Orden Ejecutiva que firmó el presidente Trump bajo el título de "Aumento de la Seguridad Pública en el Interior de los EEUU" ya decía que "Las Agencias [estatales] deberán asegurar que sus políticas de privacidad excluyan de la protección de la Ley de Privacidad a personas que no sean ciudadanos de los EEUU o residentes legales permanentes en relación con los datos personales, en tanto sea posible de acuerdo con el derecho en vigor" (art. 14) (texto disponible en ingles en: *https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/*). Parece evidente que esta declaración resulta incompatible con el acuerdo *Privacy Shield*. Con la aprobación de la denominada *Cloud Act* el 23 de marzo de 2018, las circunstancias para la efectividad de este Acuerdo empeoran, en la medida que esta ley permite acceder a datos almacenados por empresas americanas, cualquiera que sea la ubicación de sus servidores

y se continúen con las injerencias–. Analizaremos, en primer lugar, cuáles son las características y principios del nuevo Acuerdo para posteriormente ver si efectivamente este nuevo marco jurídico cumple con sus objetivos en lo que respecta a la protección de los derechos y libertades fundamentales de los ciudadanos europeos en el contexto actual y, en consecuencia, cuál puede ser su destino viendo los precedentes.

43. Partiendo de los dos principales motivos del Tribunal de Justicia para anular el anterior sistema: por un lado, la ausencia de un marco legislativo claro en EEUU para los casos en los que se restringen los derechos y libertades de los ciudadanos europeos en materia de protección de datos (por ejemplo, por motivos de seguridad nacional) y, por otro, la ausencia de mecanismos judiciales y de control efectivos que permitan a los ciudadanos europeos ejercitar sus derechos en ese país; el nuevo acuerdo de Escudo de Privacidad se articula alrededor de una serie de principios acordes con el Derecho europeo. Estos principios se pueden resumir en los siguientes: a) el derecho del ciudadano europeo a ser informado sobre los tratamientos de los datos; b) el establecimiento de limitaciones al uso de los datos con distintos fines de aquellos para los que se recogieron los datos legítimamente; c) el respeto al principio de minimización de los datos y la obligación de conservar los datos únicamente durante el tiempo necesario; d) la obligación de tratar los datos mediante sistemas seguros; e) La obligación de proteger los datos en el caso de que se transfieren a otra entidad; f) el reconocimiento y, sobre todo, la efectividad del derecho de los ciudadanos europeos a acceder a los datos y a su rectificación; g) el derecho a presentar una reclamación y a obtener reparación en caso de incumplimiento de estos principios. En consecuencia, este acuerdo impone a las empresas adheridas ciertas obligaciones relativas al procesamiento de los datos y exige unas garantías más estrictas para la tutela los derechos de los ciudadanos europeos, incluso para las trasferencias a terceros excluidos del acuerdo. A este respecto, las autoridades de EEUU se han comprometido a realizar un seguimiento periódico y riguroso del cumplimiento de estas obligaciones y, en su caso, a sancionar las posibles infracciones.

Por cuanto a las posibles injerencias externas a este acuerdo, éstas se tratan de limitar. Así, el acceso de las autoridades públicas estadounidenses por motivos de seguridad nacional, aplicación de la ley o interés público están sujetas a limitaciones y salvaguardias claras y bajo mecanismos de supervisión que impidan un acceso generalizado a los datos personales. Con tal objeto se crea la figura de un mediador independiente de las agencias nacionales de seguridad que realizará el seguimiento de las denuncias y de las consultas de los particulares.

(incluyendo dentro de la UE), evitando así la necesidad de acudir a mecanismos de colaboración internacional a través de tratados de cooperación judicial o, como es el caso, al Acuerdo *Privacy Field*. Texto íntegro disponible en ingles en: *https://www.congress.gov/bill/115th-congress/house-bill/4943/text*.

En lo que respecta a las garantías de los derechos de los interesados, se prevén vías en principio adecuadas para que los ciudadanos europeos puedan conseguir una reparación individual y acudir a mecanismos alternativos de resolución de conflictos sin coste alguno. Estas garantías o vías puede sintetizarse en las siguientes: a) las empresas o entidades adheridas a este acuerdo deberán responder en un plazo de 45 días a cualquier reclamación y, cuando se trate de datos personales, deberán cumplir la decisión de la Autoridad Nacional de Control del Estado miembro competente; b) los afectados podrán presentar su queja ante la Autoridad de Control de su país de residencia que la derivará al Departamento de Comercio y a la Comisión Federal de Comercio para facilitar la investigación y posterior resolución de la reclamación en un plazo razonable; y, como último recurso c) podrán recurrir a un mecanismo alternativo de resolución de conflictos que adopte decisiones vinculantes y ejecutables contra las empresas adheridas al acuerdo. Se prevé también la revisión anual y conjunta de este Acuerdo por la Comisión, pudiendo en este sentido suspenderlo si, como consecuencia de esta revisión o de información obtenida de otras fuentes (*v.gr*., los informes voluntarios de transparencia emitidos por las empresas sobre el grado de acceso a los requerimientos gubernamentales) verifica que las empresas adheridas o las autoridades públicas de EEUU no están cumpliendo sus compromisos.

44. Pese a la buena intencionalidad con la que fue planteado y las sustanciales mejoras introducidas en el nuevo marco propuesto, el acuerdo de *Privacy Shield* ha estado acompañado –incluso antes de su aprobación–, de polémica y de gran escepticismo en cuanto a su efectividad real en la protección de los derechos y libertades que puedan resultar afectados en el desarrollo de las transferencias transatlánticas cubiertas por este Acuerdo. De hecho, los principales actores europeos en materia de protección de datos, como es el GT29 o el SEPD, han manifestado desde su propuesta reiteradas críticas respecto a la suficiencia del acuerdo alcanzado[135] (lo que se ha confirmado tras la primera revisión anual del funcionamiento del acuerdo)[136].

Siguiendo el análisis de la propuesta que realizó el GT29 (Dictamen de 13 de abril de 2016), son tres los principales problemas que este Acuerdo adolece –y que afectan principalmente a su alcance–. En primer lugar, que el texto de la Decisión no obliga a las entidades u organizaciones adheridas al borrado de los datos personales cuando ya no sean necesarios. Esto supone la infracción

135. *Vid*. notas a pie nº 129 y 130.

136. *Vid*. Informe de la Comisión, de 18 de octubre de 2017, al Parlamento Europeo y al Consejo sobre la primera revisión anual del funcionamiento del Escudo de la privacidad UE-EE. UU. (COM(2017)0611) y el documento de trabajo de los servicios de la Comisión que lo acompaña (SWD(2017)0344) y el Documento del Grupo de Trabajo del Artículo 29, de 28 de noviembre de 2017, titulado "EU-US Privacy Shield – First Annual Joint Review" (WP 255, disponible en: *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612621*).

del principio de calidad del dato, según el cual los datos no deben almacenarse por más tiempo del estrictamente necesario para cumplir la finalidad para la cual fueron recopilados. En segundo lugar, el gobierno de EEUU, amparándose en las excepciones por motivos de seguridad nacional, no excluye totalmente la posibilidad de que se recopile de forma masiva e indiscriminada datos personales desde la UE. Lo que para el GT29 supone permitir una vigilancia indiscriminada de las personas –aunque sea escudándose en investigaciones sobre terrorismo– que es una práctica inadmisible en una sociedad democrática. Por último, si bien la previsión de un nuevo mecanismo de reparación extrajudicial para los interesados: un organismo que se encargue de resolver las quejas o consultas planteadas por los ciudadanos de la UE, no se indica cómo va a garantizase la independencia del mismo o el poder suficiente para que pueda ejercer de forma efectiva sus funciones; lo que en definitiva supone que no se garantiza en última instancia una reparación satisfactoria para el interesado en caso de desacuerdo entre las partes implicadas. Con todo ello, ni la propuesta inicial, ni en definitiva la Decisión por la que se establece el Escudo de privacidad, ofrece un nivel equivalente de protección al que existe en la UE para que las transferencias de datos a EEUU amparadas en este marco fueran lícitas.

45. En este contexto, resulta muy significativa la Resolución de 5 de julio de 2018, del Parlamento Europeo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EEUU[137]. Este documento reconoce que este sistema incluye cambios relevantes respecto de las obligaciones que deben asumir las entidades estadounidenses que decidan adherirse, tendentes a proteger el derecho fundamental a la protección de datos personales de los ciudadanos europeos. Entre otras novedades, por ejemplo, el acuerdo de *Privacy Shield* refuerza el derecho de los interesados a decidir sobre determinados tratamientos[138] –como puede ser el tratamiento para fines de marketing directo–, reconociendo el derecho de los interesados a decidir sobre si consienten el tratamiento de sus datos para finalidades distintas a aquellas para las que se recogieron inicialmente sus datos, incluso si esas finalidades son compatibles con los originales. Pero en este sentido también plantea ciertas objeciones, como que no se establezca más claramente los plazos que deben otorgarse para que los interesados puedan decidir sobre estos tratamientos[139]. Para el Parlamento Europeo entre los retos que debe afrontarse, para que este acuerdo pueda constituir un marco jurídico válido para las transferencias transatlánticas, está la revisión periódica por la Comisión de la implementación real y de la efectividad de los compromisos asumidos por los Gobiernos y las empresas al

137. 2018/2645(RSP). Texto disponible en: *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0315+0+DOC+XML+V0//ES#ref_1_9*.
138. Dentro de lo que se denomina el *principle of choice*.
139. Cuestión que tampoco está resuelta en el Reglamento de forma exhaustiva.

amparo del Escudo de Privacidad, así como la necesidad de analizar el acuerdo para garantizar su adecuación al nuevo Reglamento.

Concluye el Parlamento en su documento la falta de adecuación manifestada por el Acuerdo desde su puesta en práctica para cumplir con los objetivos marcados respecto de su predecesor –al margen del limitado alcance de los resultados, dado el número de entidades estadounidenses adheridas al sistema que sigue siendo significativamente inferior al que contaba el *Safe Harbor*–. Para ello, el Parlamento se fundamenta en casos recientes de empresas estadounidenses adheridas al sistema *Privacy Shield*, como son Facebook y Cambridge Analytica, hecho que no ha evitado el mal uso de los datos. De lo que se deduce, razonablemente, que ese marco jurídico no es suficientemente protector de los derechos de los interesados, dado que no permite que las obligaciones de supervisión y control se estén ejercitando de forma adecuada. Consecuentemente, el Parlamento pide a la Comisión que adopte todas las medidas necesarias para garantizar que el Escudo de la privacidad cumpla plenamente con la normativa europea y jurisprudencia del TJUE en la materia –en particular, con el Reglamento–, con la CDFUE y el CEDH. Si bien, deben aplicarse de forma que no obstaculicen innecesariamente el comercio o las relaciones internacionales, pero que no pueden "compensarse" con intereses comerciales o políticos. Por todo ello, considera que, "a menos que los Estados Unidos cumplan plenamente el 1 de septiembre de 2018, la Comisión habrá dejado de actuar de conformidad con el artículo 45, apartado 5, del Reglamento general de protección de datos", solicitando expresamente a la Comisión que suspenda el Escudo de la privacidad hasta que las autoridades estadounidenses cumplan con sus condiciones[140].

46. En definitiva, los problemas de eficacia y alcance que este nuevo marco ha manifestado desde su puesta en práctica, hacen prever que su vigencia no parezca que vaya a ser muy longeva dadas las circunstancias. En la medida que mantienen los mismos problemas de falta de garantía para la protección de los datos personales de los ciudadanos europeos en el país de destino –que motivaron la anulación del *Safe Harbor* por el Tribunal de Justicia–, y por cuanto que (al margen de la referida iniciativa del Parlamento Europeo que supone la suspensión del sistema por la Comisión) aún está pendiente de resolver ante este Tribunal el Asunto T-738/16, recurso por el que se solicita que se declare que la Decisión 2016/1250 de la Comisión, es contraria a los artículos 7, 8 y 47 de la CDFUE y, en consecuencia, sea anulada[141].

140. A tales efectos, el Parlamento encarga a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior que continúe controlando la evolución en este ámbito, incluidos los asuntos presentados ante el TJUE, y que haga un control del seguimiento de las recomendaciones realizadas en la Resolución.

141. Recurso interpuesto el 25 de octubre de 2016, *La Quadrature du Net y otros c. Comisión*, Asunto T-738/16.

En un contexto como éste, las empresas y entidades adheridas al Escudo de privacidad y que fundamentaban sus transferencias transatlánticas en este sistema, deberían estar adoptando las medidas necesarias para que sus transferencias de datos de UE a EEUU cumplan con la normativa europea, la jurisprudencia del TJUE y la CDFUE Y CEDH; pues en caso contrario podrían ver suspendidas sus operaciones más pronto que tarde[142]. En este sentido, al igual que ocurrió en los momentos posteriores a la anulación del Acuerdo de Puerto Seguro, las empresas podrán acogerse al régimen general de transferencias internacionales previsto en el Reglamento –incluyendo los supuestos de excepción al régimen general del art. 49 –. Ahora bien, incluso cuando se hayan adoptado medidas de garantías que en principio son suficientes, como pueden ser las cláusulas contractuales tipo de la UE (Decisión CCT[143]), la condición de estas medidas como "apropiadas" para permitir las transferencias de datos puede quedar en entredicho cuando el destinatario o importador de los datos está localizado en EEUU –principalmente por su normativa interna, en particular en materia de seguridad nacional–. De esto da muestra la petición de decisión prejudicial planteada por la High Court de Irlanda el 9 de mayo de 2018 (Asunto C-311/18)[144]. La relevancia de este asunto radica en que, si bien ha sido interpuesto en relación con la interpretación del régimen de transferencias internacionales recogido en la ya derogada Directiva –en particular sobre transferencias de datos destinadas a EEUU–, las cuestiones planteadas a resolver por el Tribunal de Justicia son extrapolables al nuevo instrumento europeo.

47. La base de la cuestión prejudicial, en el Asunto C-311/18, se encuentra en el alcance real de las cláusulas contractuales tipo UE, pues de ello depende su virtualidad como mecanismo de garantía efectivo para las transferencias internacionales de datos. Estas cláusulas son aplicables al exportador de datos y al importador de datos, pero no resultan vinculantes para las autoridades nacionales del tercer país de destino, por lo que pueden exigir al importador de datos que facilite a sus servicios de seguridad los datos personales transferidos –con arreglo a las cláusulas establecidas en la Decisión CCT–, para su posterior tratamiento. Por tanto, este es un factor que hay que valorar para determinar si un tercer país –el de destino– garantiza el nivel de protección que exige la normativa de la Unión para transferir datos personales a dicho país a través de este mecanismo (art. 26.2 Directiva, art. 46.1 c) Reglamento); y cuál es ese nivel de protección que ha de garantizarse según la normativa europea interpretada

142. *Vid*. art. 45 apartado 5 del Reglamento.

143. *Loc. cit*. En su versión modificada por la Decisión 2016/2297, de 16 de diciembre de 2016, por la que se modifican las Decisiones 2001/497/CE y 2010/87/UE, relativas 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 2016, L 344, p. 100).

144. Petición de decisión prejudicial, *Data Protection Commissioner, Facebook Ireland Limited, Maximillian Schrems*, Asunto C-311/18, (2018/C 249/21).

a la luz de la CDFUE y el CEDH. Partiendo de la normativa interna existente en EEUU –probada por el órgano jurisdiccional remitente–, en particular en el ámbito de la seguridad nacional, se plantea si para el caso objeto de análisis –y todos aquellos en los que el país de importación de los datos desde la UE sea EEUU– dichas transferencias realizadas en el marco de la Decisión CCT pueden suponer una violación de los artículos 7 y/8 de la CDFUE.

Asimismo, se plantea qué relevancia tiene, en su caso, la Decisión sobre el Escudo de la privacidad en la valoración efectuada en cuanto a la adecuación de la protección ofrecida a los datos transferidos a EEUU conforme a la Decisión CCT. Y si constituye la figura del Defensor del Pueblo en el ámbito de este Acuerdo (anexo A del anexo III de la Decisión sobre el Escudo de la privacidad), en combinación con el régimen vigente en EEUU, una garantía de que este país ofrece a una vía de recurso compatible con el artículo 47 de la CDFUE a los interesados cuyos datos personales son transferidos a EE.UU (con arreglo a la Decisión CCT). En consecuencia, por todo ello, se plantea en definitiva si la Decisión CCT vulnera en este caso los artículos 7, 8 y/o 47 de la CDFUE, dada cuenta de la constatación del nivel de protección del derecho a la protección de los datos personales existente en EEUU –y las vías de recurso reales de las que disponen los interesados para su tutela en dicho país–, pese a la existencia de las Decisiones institucionales referidas.

El planteamiento de esta cuestión prejudicial, del aún pendiente recurso de anulación de la Decisión sobre el Escudo de privacidad, la reciente resolución del Parlamento europeo sobre la inadecuación del Escudo de privacidad solicitando su suspensión y la adopción de medidas a la Comisión para no permitir las transferencias de datos a EEUU en las circunstancias actuales con base en este marco jurídico, da muestra de la ineficacia real de los mecanismos existentes respecto de importación de datos personales a EEUU en la consecución de los objetivos buscados: permitir la transferencia internacional de datos solo a aquellos países donde se garantice un nivel adecuado de protección de los derechos y libertades de los ciudadanos europeos según la normativa europea a la luz del CDFUE y la CEDH.

2. EL FUTURO DE LAS TRANSFERENCIAS DE DATOS TRANSATLÁNTICAS TRAS LA "CLOUD ACT"

48. Con la aprobación el 23 de marzo de 2018 de la *Clarifying Lawful Overseas Use of Data Act*, más conocida como la *Cloud Act*[145], la incertidumbre sobre la continuidad –lícita de conformidad con la normativa europea– de las transferencias de datos personales desde la UE a EEUU se acrecienta. La aprobación de esta norma ha generado controversia no sólo a nivel internacional (en particular desde

145. Como parte de la *Consolidated Appropriations Act*, 2018, Pub. L. 115-141

Europa) sino también nacional desde la perspectiva de los EEUU, en la medida que supone un cambio significativo en la legislación con respecto a los proveedores de servicios de comunicación electrónica o servicios de computación remota y, más concretamente, respecto de su obligación de divulgar el contenido de las comunicaciones electrónicas, los datos almacenados y los registros transaccionales[146]. En particular, respecto de las operaciones de transferencias de datos personales, hay una novedad esencial introducida por esta ley: la posibilidad de compartir datos a través de acuerdos ejecutivos (§ 2523, *Cloud Act*), los denominados "executive agreements" o acuerdos bilaterales que puede suscribir el presidente de los Estados Unidos con gobiernos extranjeros ("qualifying foreign government"), cuestión que merece un análisis específico en este trabajo.

49. En términos generales, la *Cloud Act* es una ley que regula el acceso de las autoridades norteamericanas a los datos almacenados en servidores de empresas norteamericanas (como correos electrónicos, mensajes de texto o chats) con independencia de su ubicación, esto es, también cuando se encuentren fuera de sus fronteras –incluida la UE–, al amparo de una orden judicial. Esto se traduce en la práctica en que se podrán realizan transferencias de datos internacionales con destino a EEUU con base en esta norma (cuando exista una simple orden judicial justificada por motivos de seguridad nacional), al margen de cualquier acuerdo internacional existente en el ámbito de la cooperación internacional o de acuerdo específico en materia de protección de datos al que se esté obligada la entidad o empresa norteamericana responsable (como es el caso del Escudo de Privacidad cuando los datos tienen como origen cualquier Estado miembro de la UE y la empresa está adherida a este sistema para legitimar en principio tal transferencia). Así, por ejemplo, esta nueva norma permitiría al FBI solicitar a un tribunal de un Estado norteamericano una orden para obtener archivos de un ciudadano que es residente en EEUU, pero cuyos datos están alojados en un Estado miembro de la UE, por razones de seguridad nacional sin tener que cumplir la normativa de privacidad y protección de datos europea. Ahora bien, en la medida que esta ley no establece límites a las facultades de las autoridades norteamericanas respecto de la recopilación de datos a las empresas y organismos de los EEUU, esta información podría ser de cualquier persona, no solo de ciudadanos residentes en aquel país, si así las autoridades lo consideran y si un juez de los EEUU.

146. *Vid.* MEYER, J. E., "Foreign Companies: Does the U.S. Government Now Have Access to Your Overseas Data?", *National Law Review, 4 de diciembre de 2018, https://www.natlawreview.com/article/foreign-companies-does-us-government-now-have-access-to-your-overseas-data*; MEVISSEN, C., "The Cloud Act and its consequences", 8 noviembre de 2018, *https://legalict.com/2018/11/08/the-cloud-act-and-its-consequences/* (última visualización el 29.03.2019); SWIRE, P., HEMMINGS, J., "The Cloud Act and its Impact on Cross-Border Access to the Contents of Communications", 25 de marzo de 2018; *https://www.alstonprivacy.com/cloud-act-impact-cross-border-access-contents-communications/* (última visualización el 29.03.2019).

50. Vamos a centrarnos, por razón del objeto de estudio, en el contenido de esta ley que afecta a las transferencias internacionales de datos desde la UE, dejando al margen otras cuestiones, igualmente relevantes, que excedan a esta cuestión. La justificación de esta norma es la de proteger la seguridad pública y combatir los delitos graves, incluido el terrorismo, lo que explica su alcance y contenido. La *Cloud Act* modifica varias normas norteamericanas vigentes relativas al tratamiento de datos personales. La más relevante es la modificación efectuada sobre la *Stored Communications Act* de 1986 (Ley de Comunicaciones Almacenadas o SCA)[147], incorporando una nueva disposición (§2703) que genera importantes obligaciones para los proveedores de servicios y permite a las autoridades un nuevo recurso para solicitar a los tribunales órdenes para recabar datos personales[148]; También modifica un apartado de la *Electronic Communications Privacy Act* (Ley de privacidad de las comunicaciones electrónicas o ECPA)[149], que regula el acceso de las autoridades norteamericanas a los datos de las comunicaciones de los ciudadanos, contenida en el capítulo 121 del título 18 del *United States Code*[150].

Precisamente estas modificaciones legislativas tienen su origen en el caso *entre Microsoft y el gobierno de los Estados Unidos* (Asunto *United States v. Microsoft Corporation*), iniciado a finales de 2013 y que llegó hasta el Tribunal Supremo norteamericano, en relación con la pretensión del gobierno de EEUU de acceder a los datos de una persona objeto de una investigación, alojados en un servidor de la compañía situado en Irlanda, al amparo de la SCA (18 U. S. C. §2703)[151]. Antes de que se resolviera por el Tribunal Supremo de EEUU este asunto la *Cloud Act* fue adoptada, por lo que la petición del Gobierno de EEUU ya tenía fundamento legal para su concesión, dejando sin causa al Tribunal Supremo[152].

Es indudable que son significativas las consecuencias prácticas que para los actores implicados esta reforma les conlleva. Con la nueva regulación se obliga a los proveedores de servicios a que conserven, realicen copias de seguridad y faciliten el contenido de las comunicaciones electrónicas o por cable,

147. 18 U.S.C. Chapter 121 §§ 2701-2712.
148. *Cloud Act* §103 (a) (1).
149. 18 U.S.C.A. § 2510 y ss. (2012).
150. Compilación de la legislación federal general de los Estados Unidos. Texto disponible en ingles en: *https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121* (consultado el 26.10.2018).
151. Asunto nº 17-2 *United States v. Microsoft Corporation*, 829 F.3d 197, aceptado por el Tribunal Supremo norteamericano el 10/16/2017. Puede consultarse todo el iter procedimental del caso hasta llegar al Tribunal Supremo y toda las resoluciones recaídas en las distintas instancias en *https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html*.
152. *Vid. Opinion UNITED STATES, PETITIONER v. MICROSOFT CORPORATION on writ of certiorari to the united states court of appeals for the second circuit, April 17, 2018, Per Curiam*. Disponible en inglés en: *https://supreme.justia.com/cases/federal/us/584/17-2/*.

así como cualquier registro u otra información perteneciente a un cliente o suscriptor bajo la posesión, custodia o control de dicho proveedor, independientemente de si dicha comunicación, registro u otra información se encuentra dentro o fuera de los Estados Unidos[153]. Si bien, los proveedores podrían dejar sin efecto o modificar esta solicitud si el objetivo –el titular de los datos personales cuya información se solicita– no fuese un ciudadano estadounidense y si el cumplimiento de estas obligaciones entrase en conflicto con la ley del país donde estén almacenados los datos. En estos casos, se requeriría que un tribunal considere la posibilidad de acceder a los datos por otros medios, el grado de interés de las autoridades de los EEUU en acceder a dichos datos y los intereses y leyes del gobierno extranjero[154].

51. La *Cloud Act* abre otra posibilidad de supuestos de transferencias internacionales de datos personales entre EEUU y terceros Estados (incluyendo Estados miembros de la UE/EEE). Esta nueva opción se articula a través de la celebración de los llamados "executive agreements" o acuerdos bilaterales ejecutivos que puede suscribir el presidente de los Estados Unidos con gobiernos extranjeros (aquellos que tengan la consideración de "qualifying foreign government")[155]. En este sentido, por el objeto de estudio marcado parece necesario hacer un examen de estos posibles acuerdos, sus requisitos, su relevancia y trascendencia con respecto a los demás instrumentos de cooperación entre la UE y los EEUU.

Como ya se ha anticipado, este tipo de acuerdos bilaterales sólo pueden ser firmados por el presidente de los Estados Unidos con gobiernos extranjeros que tengan la consideración de cualificados ("qualifying foreign government"), y se somete a un rígido sistema de control y verificación para que pueda entrar en vigor. En este sentido, el Presidente de EEUU sólo firmará un acuerdo ejecutivo después de un estricto control por parte del Fiscal General y el Secretario de Estado y la aprobación del Congreso (§2523 (b) *Cloud Act*). A mayor abundamiento, el Congreso puede votar una resolución conjunta de desaprobación dentro de los 90 días siguientes, y en cuyo caso tendrá como consecuencia que el acuerdo ejecutivo no entrará en vigor (§ 2523 (d) (4) *Cloud Act*).

En lo que respecta a la parte co-contratante del acuerdo ejecutivo, esto es, el "gobierno extranjero calificado", la Cloud Act, recoge una definición a tales efectos en dos partes: la sección 2703 y la sección 2523. De conformidad con la §2703 un gobierno extranjero es uno con el que los Estados Unidos tiene

153. *Cf.* 18 U.S. Code § 2713. Texto disponible en ingles en: *https://www.law.cornell.edu/uscode/text/18/2713*.

154. *Ibídem*.

155. *Vid.* AVOCATS, M., "What are executive agreements under the Cloud Act?", 25 de junio de 2018, *https://www.avocats-mathias.com/actualites/executive-agreements-cloud-act* (última visualización el 29.03.2019).

un acuerdo ejecutivo que ha entrado en vigor de conformidad con la sección 2523 y sus leyes brindan a los proveedores de servicios de la sociedad de la información[156] medidas sustanciales y procesales "similares" a las mociones (a las estadounidenses) para anular o modificar el proceso legal de divulgación y de las reglas que establecen que la divulgación por parte de aquellos no será considerada como una violación de una orden de protección. Por su parte, la Sección 2703 brinda una definición parcial de lo que es un "gobierno extranjero calificado", en la medida que hay que acudir a los requisitos de la sección 2523 para evaluar si se cumplen las condiciones para ser parte de un acuerdo ejecutivo.

En lo que respecta a las condiciones que debe cumplir el acuerdo ejecutivo para que permita la transferencia de datos, la sección 2523 establece una larga lista de requisitos sobre su contenido (*v.gr.,* confidencialidad de los datos, requisitos para la solicitud del gobierno extranjero, derechos y obligaciones de cada parte, etc.). No obstante, cabe referir que la mayoría de los requisitos referidos a este respecto son también requisitos para el gobierno extranjero. En este sentido, la sección 2523 puede dividirse en tres grandes categorías de requisitos, cada uno de los cuales tiene sus propias condiciones:

1) El ordenamiento jurídico del gobierno extranjero debe ofrecer "sólidas protecciones sustantivas y procesales para la privacidad y las libertades civiles a la luz de la recopilación de datos y las actividades del gobierno extranjero que estarán sujetas al acuerdo".

La sección continúa enumerando cuáles son estas protecciones que deben ofrecerse, tales como: leyes sustantivas y procesales adecuadas sobre ciberdelincuencia y las pruebas electrónicas (presumiéndose su cumplimiento por el hecho de ser parte de la Convención sobre ciberdelincuencia, realizada en Budapest el 23 de noviembre de 2001[157]); obligaciones y compromisos internacionales de derechos humanos o muestras de respeto por los derechos humanos universales internacionales; o mecanismos suficientes para proporcionar responsabilidad y transparencia apropiada con respecto a la recopilación y el uso de datos electrónicos por parte del gobierno extranjero, entre otros.

2) Que el gobierno extranjero haya adoptado "procedimientos apropiados para minimizar la adquisición, retención y difusión de información relativa a personas de los Estados Unidos sujetas al acuerdo"; y

3) Que las órdenes sujetas al acuerdo ejecutivo deben cumplir con rigurosas condiciones como es "no apuntar intencionalmente a una persona de los Estados Unidos o una persona ubicada en los Estados Unidos", realizarse "con

156. Proveedores de servicios de comunicación electrónica y proveedores de servicios de computación remota.

157. Del que España es parte, desde septiembre de 2010, mediante instrumento de ratificación. BOE núm. 226, de 17 de septiembre de 2010, páginas 78847 a 78896.

el propósito de obtener información relacionada con la prevención, detección, investigación o el enjuiciamiento de delitos graves, incluido el terrorismo" y que estar "sujetas a revisión o supervisión por parte de un tribunal, juez, magistrado u otra autoridad independiente".

En definitiva, los acuerdos ejecutivos permiten a los gobiernos extranjeros solicitar directamente los datos de una persona que no sea estadounidense si pueden cumplir con los numerosos requisitos exigidos. Sin embargo, para solicitudes relacionadas con personas de los Estados Unidos, el gobierno extranjero tendrá que utilizar en su caso el proceso previsto en los Tratados de Asistencia Judicial firmados por EEUU con terceros Estados (*Mutual Legal Assistance Treaty* o *MLAT*) que le vincule[158] u obtener asistencia concreta en una investigación o proceso penal (28 U.S. Code §1782 y 18 U.S. Code §3512). Consecuentemente, la delimitación del término "persona de los EEUU" resulta esencial. Este término incluye ciudadanos o nacionales de los Estados Unidos (por lo que no tienen necesariamente que residir allí) o nacionales extranjeros que hayan sido admitidos legalmente para residir de forma permanente en EEUU o corporaciones constituidas en aquél país (§2523 (a) (2) *Cloud Act*). En conclusión, en la práctica los gobiernos extranjeros deberán prestar especial atención al tipo de datos solicitados y a quiénes conciernen, dado que los procedimientos para obtener los datos son distintos.

52. La crítica más evidente a la *Cloud Act* viene motivada por las restricciones que su puesta en práctica supone a la privacidad y otros derechos y libertades civiles fundamentales[159]. Consecuentemente, la principal cuestión que surge con la puesta en práctica de la *Cloud Act* es su compatibilidad con el nuevo Reglamento general de protección de datos. En particular, una de las cuestiones más importantes en este contexto está referida precisamente a la reglamentación de las transferencias internacional de datos.

En términos generales, las eventuales transferencias de datos personales desde la UE a EEUU que con base a la *Cloud Act* puedan producirse, no cumplirán las garantías en el tratamiento de datos personales de los ciudadanos europeos que el Reglamento exige –en los términos establecidos por el TJUE, a la luz de la CDFUE y del CEDH–. Toda vez que la *Cloud Act* permite transferencias de datos personales en el seno de una investigación (de seguridad nacional en EEUU) soslayando la aplicación de convenios internacionales de asistencia judicial mutua u otros acuerdos particulares que pudieran resultar de aplicación, como sería el caso del Acuerdo de Escudo

158. Si se trata de un Estado miembro de la UE a través del Tratado de asistencia judicial firmado entre UE y EEUU firmado en Washington el 25 de Junio de 2003, que resulta aplicable desde el 1 de febrero de 2010 (DOUE L 181/34, 19.7.2003).

159. VOGEL, P. S.; JONES, S., "The Cloud Act's Dramatic Impact on International Privacy Laws", 7 de junio de 2018, *https://www.ecommercetimes.com/story/85374.html* (última visualización el 29.03.2019).

de Privacidad (sin perjuicio de que ya antes de la *Cloud Act* este Acuerdo haya manifestado su falta de adecuación como marco jurídico suficiente para permitir estas transferencias). El Reglamento prohíbe la transferencia o divulgación de datos personales a terceros países, aunque estén dentro del marco de una investigación judicial, a menos que se haga de conformidad con un acuerdo de asistencia legal mutua u otro acuerdo internacional (art. 48), sin perjuicio de otros motivos para la transferencia de conformidad con el régimen general y las excepciones previsto en el Capítulo V. En consecuencia, no se permitirá este tipo de transferencias (adoptándose medidas de bloqueo y/o suspensión) salvo que los EEUU lleguen a un acuerdo con la UE o que la UE resuelva que las investigaciones de los EEUU y las posteriores transferencias o divulgaciones en cumplimiento de los procedimientos de la *Cloud Act* no entran en conflicto con el Reglamento –cualquiera de las dos posibilidades parece poco probable–.

Ahora bien, cabe plantearse si a través de los acuerdos bilaterales ejecutivos previstos en la *Cloud Act* (§2523) podría buscarse encaje a las transferencias internacionales dentro del Reglamento; esto es, si éstos serán suficientes en sí mismos para cumplir con las condiciones establecidas en los artículos 44 a 50. En este sentido, por ejemplo, cabría plantearse si estos acuerdos ejecutivos pudieran considerarse necesarios "por razones importantes de interés público" para permitir la transferencia como excepción del art. 49.1 letra d) del Reglamento. No obstante, parece que estos supuestos pudieran encajar mejor en relación con el art. 48 del Reglamento, si pudieran considerarse dichos acuerdos ejecutivos como un acuerdo internacional a los efectos de este precepto. En ese caso, habría que plantearse si fueran suficientes por sí mismos o si por el contrario deberían cumplir a tales efectos con los principios establecidos en el art. 5 del Reglamento (además de las condiciones establecidas en la *Cloud Act* para su vigencia o en lugar de aquellas). En cualquier caso, no sería admisible esta posibilidad si no se puede encontrar un acuerdo ejecutivo entre EEUU y la UE antes de que se produzca la transferencia internacional. Asimismo, cabe plantearse cómo interactuarán la nueva norma estadounidense con el Acuerdo marco entre EEUU y la UE de cooperación judicial de 2003, en la medida que éste último establece las condiciones para la transferencia de datos entre las autoridades ambas partes. Sin embargo, este Acuerdo no autoriza tales transferencias.

Otro problema potencial es que la *Cloud Act* establece claramente la posible elusión de la ley nacional extranjera según la § 2523 (b) (3); en la medida que según este precepto si la ley del gobierno extranjero prohíbe a los proveedores de servicios de comunicaciones divulgar los datos, el gobierno extranjero debe eliminar esas restricciones para permitir los mismos derechos de acceso a los datos que en los Estados Unidos. En definitiva, no parece que exista una posición clara sobre la compatibilidad de ambas normas y cómo

interactuarán en la práctica internacional, y sobre todo qué normativa tendrán que cumplir los proveedores de servicios de la sociedad de la información.

VI. CONCLUSIONES

53. Con el nuevo Reglamento de protección de datos se unifica la normativa europea en esta materia, de manera que en toda la UE se aplica un único sistema en lugar de las veintiocho legislaciones nacionales que hasta el momento coexistían, lo que unido a la creación del mecanismo de ventanilla única, trae como consecuencia que la seguridad jurídica en este ámbito se haya visto reforzada en todo el Espacio Económico Europeo. Incluso cuando intervengan varias Autoridades nacionales de control en asuntos transfronterizos, el Reglamento garantiza una interpretación uniforme y coherente de las nuevas normas, por cuanto que se adoptará una única decisión con el objeto de asegurar que las soluciones sean las mismas ante los mismos problemas.

Con la ampliación del alcance espacial del Reglamento –respecto de su predecesora la Directiva–, se asegura que se apliquen las mismas reglas tanto a las empresas europeas como aquellas domiciliadas fuera de las UE si suministran bienes y servicios o vigilan la conducta de los ciudadanos europeos. Esta igualdad de condiciones impuesta conduce necesariamente a un aumento de la confianza de los consumidores europeos que, sin duda, revertirá en beneficios tanto para los operadores comerciales de la UE como de terceros países.

El Reglamento muestra así un evidente avance legislativo respecto de la anterior normativa europea, más adecuado al contexto actual de un mundo globalizado y totalmente digitalizado, donde las transferencias internacionales de datos son la pieza clave. En consecuencia, estas operaciones tienen un lugar preminente en el nuevo instrumento. Con su reglamentación se busca un doble objetivo: por un lado, la protección del sujeto (de sus derechos y libertades fundamentales) y, por otro, el correcto tráfico mercantil de una sociedad y economía de este siglo.

54. El nuevo régimen de las transferencias internacionales de datos busca conseguir mayor transparencia en este tipo de operaciones, para ello se recogen reglas detalladas y comprensibles que comprenden tanto las transferencias con fines comerciales como aquellas derivadas del cumplimiento de la ley. Aunque la arquitectura del régimen de las transferencias internacionales de datos en el Reglamento en esencia es la misma que la prevista por la Directiva, la reforma practicada en este ámbito aclara la reglas y simplifica su utilización e introduce nuevos instrumentos de transferencia.

Respecto del control de este tipo de operaciones, la nueva normativa aumenta el poder de la Autoridades nacionales de control y regula más detalladamente su independencia, funciones y facultades, entre las que se en-

cuentra expresamente la de suspender el flujo de datos a un tercer país o una determinada organización internacional si considera que no se cumple con las garantías exigidas para el tratamiento de datos en el país de destino o importación. Asimismo, el Reglamento prevé un catálogo preciso y minucioso de los elementos y factores que la Comisión europea deberá tener en consideración al evaluar el nivel de protección de los terceros países para permitir las transferencias internacionales de datos de ciudadanos europeos. En este sentido, ha de evaluarse tanto el acceso de las autoridades públicas del país de destino a los datos personales como la eficacia de los mecanismos y recursos de protección previstos en su ordenamiento jurídico y la posibilidad cierta de su utilización o de solicitar efectivamente una compensación administrativa y judicial por parte del interesado (el titular de los datos personales), siguiendo la doctrina establecida por el TJUE en el caso *Schrems*.

Se refuerza la labor de seguimiento la Comisión a tales efectos, sin que terminen sus obligaciones en este ámbito con la adopción de las decisiones de adecuación; puesto que deberá revisar, al menos cada cuatro años, todas las decisiones que emita. De esta forma, podrá detectarse más fácilmente los cambios que se produzcan con relación al nivel de protección ofrecido por cada tercer país al que se dirigen transferencia de datos desde la UE, con fundamento en una decisión de adecuación. Y cuando se traten de transferencias internacionales a terceros países que no cuenten con un nivel adecuado de protección, para permitir este tipo de operaciones el Reglamento prevé acudir a mecanismos alternativos como son los códigos de conducta y mecanismos de certificación, junto con las ya habituales cláusulas contractuales tipo o la adopción de reglas corporativas vinculantes que, por primera vez, tiene virtualidad propia al reconocerse expresamente en la normativa europea.

55. Al margen del régimen general de transferencias internacionales (con las novedades y mejoras incorporadas con la reforma), el Reglamento prevé supuestos excepcionales en los que el exportador –el responsable o el encargado– pueda mover los datos fuera del espacio europeo sin cumplir con ninguna de las situaciones previstas en el régimen general. Se sigue en este ámbito la línea marcada por la Directiva (art. 26.1), recogiendo condiciones ya previstas como fundamento para la transferencia o grupo de transferencias (la prestación de consentimiento del interesado, la ejecución de un contrato o razones importantes de interés público, etc.). Si bien, se regulan de forma más amplia y específica, con significativas consecuencias prácticas para su apreciación y se incorpora una nueva condición de excepción respecto a las transferencias que puedan tener lugar en aras de los intereses legítimos de una determinada empresa. Ahora bien, entre todas las excepciones previstas, resulta de particular importancia la nueva reglamentación sobre la verificación consentimiento del interesado como base para la transferencia internacional, mucho más restrictiva y exigente que en lo previsto en la Directiva.

56. La relevancia de las transferencias de datos desde UE a EEUU en las relaciones económicas entre ambos continentes (y en el desarrollo de la economía global), impone la necesidad de contar con un marco normativo estable que permita que el flujo transatlántico de este tipo de datos se realice con las máximas garantías (de manera que se respeten los derechos y libertades de los interesados, entre ellos el derecho fundamental al tratamiento de datos personales de los ciudadanos europeos). Pese a los avances conseguidos con las reformas practicadas en materia de transferencias internacionales, en lo que respecta a aquellas que tengan como destino EEUU, su futuro se manifiesta incierto. La principal razón radica en la dificultad de conseguir un marco jurídico válido que permita este tipo de operaciones sin vulnerar la normativa europea vigente, a la luz de la jurisprudencia del TJUE y de la CDFUE y el CEDH.

Hay varios factores que determinan la inadecuación de los mecanismos existentes para garantizar la importación de datos personales a EEUU en los términos exigidos por la normativa europea. De ello da muestra la existencia de la cuestión prejudicial planteada en el Asunto C-311/18, sobre la adecuación de la Decisión CCT; del aún pendiente recurso de anulación de la Decisión sobre el Escudo de privacidad (Asunto T-738/16); o la resolución del Parlamento europeo de 5 de julio de 2018 sobre la inadecuación del Escudo de Privacidad, solicitando su suspensión y la adopción de medidas a la Comisión para no permitir las transferencias de datos a EEUU en las circunstancias actuales con base en este marco jurídico.

A mayor abundamiento, con la aprobación de la conocida como *Cloud Act*, se plantean nuevas cuestiones sobre sobre la continuidad de las transferencias de datos personales desde la UE a EEUU y su compatibilidad con el nuevo instrumento europeo. Esta norma estadounidense va a permitir realizar transferencias de datos internacionales desde la UE con destino a EEUU (a solicitud de sus autoridades públicas) al margen de cualquier acuerdo internacional existente en el ámbito de la cooperación internacional, o de acuerdo específico en materia de protección de datos al que se esté obligada la entidad o empresa norteamericana responsable de esos datos (como sería por ejemplo, el Acuerdo de Escudo de privacidad) y, en definitiva, soslayando la aplicación de la normativa europea sobre protección de datos.

1. BIBLIOGRAFÍA

AVOCATS, M., "What are executive agreements under the Cloud Act?", 25 de junio de 2018, *https://www.avocats-mathias.com/actualites/executive-agreements-cloud-act*.

BHASIN, M., "Challenge of guarding online privacy: role of privacy seals, government regulations and technological solutions", *Socìal no-ekonomìčnì*

Problemì ì Deržava, 2016, nº 15 (2), pp. 85-104 (*https://core.ac.uk/download/pdf/131446056.pdf*).

BU-PASHA, S. "Cross-border issues under EU data protection law with regards to personal data protection", *Information & Communications Technology Law*, 24.05.2017, pp. 213-228 (*https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740*).

CRESPI, S, "The Applicability of Schrems Principles to the Member States: National Security and Data Protection within the EU Context", *European Law Review*, Nº 5, 2018, pp. 669-686.

DE MIGUEL ASENSIO, P.A., "Un par de reflexiones sobre la sentencia Schrems", 16 de octubre de 2015 (*https://pedrodemiguelasensio.blogspot.com/2015/10/un-par-de-reflexiones-sobre-la.html*).

Id. "Transferencias de datos personales entre la UE y EEUU: el futuro de los Principios de Puerto Seguro", 4 de diciembre de 2013 (*http://pedrodemiguelasensio.blogspot.com/2013/12/transferencias-de-datos-personales.html*).

GHORBEL, A.; GHORBEL, M. y JMAIEL, M., "Privacy in cloud computing environments: a survey and research challenges", *The Journal of Supercomputing*, June 2017, Volume 73, Issue 6, pp. 2763-2800.

GRANDE SANZ, M., "La transferencia internacional de datos personales: presente y futuro", *Diario La Ley*, Nº 8808, Sección Tribuna, 21 de Julio de 2016, Ref. D-293.

GREENLEAF, G., "Global data privacy laws 2015: 109 countries, with European laws now in a minority", informe publicado en *Privacy Laws & Business International*, n.º 133, febrero de 2015, pp. 14-17 (*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2603529*).

GUASCH PORTAS, V. y SOLER FUENSANTA, J. R., "Cloud computing: cláusulas contractuales y reglas corporativas vinculantes", *RDUNED*, Nº. 14, 2014, pp. 247-270.

KUNER, C. "Reality and Illusion in EU Data Transfer Regulation Post Schrems", *German Law Journal*, vol. 18, n1 4, 2017, pp. 881-918.

LÓPEZ LAPUENTE, L., "Las transferencias de datos a EEUU: la transición del Safe Harbor al Privacy Shield y un paso más allá", *Actualidad Jurídica Uría Menéndez, nº 45, año 2017, pp. 36-38. Disponible en https://www.uria.com/documentos/publicaciones/5315/documento/art 03.pdf?id=6965*.

MEVISSEN, C., "The Cloud Act and its consequences", 8 noviembre de 2018, *https://legalict.com/2018/11/08/the-cloud-act-and-its-consequences/* (última visualización el 29.03.2019).

MEYER, J. E., "Foreign Companies: Does the U.S. Government Now Have Ac-

cess to Your Overseas Data?", *National Law Review,* 4 de diciembre de 2018, *https://www.natlawreview.com/article/foreign-companies-does-us-government-now-have-access-to-your-overseas-data.*

ORTEGA GIMÉNEZ, A., "Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield", *Revista Lex Mercatoria*, Nº. 4, 2016, pp. 85-90.

PIÑAR MAÑAS, J. L., "Transferencias de datos personales a terceros países u organizaciones internacionales", en *Reglamento general de protección de datos: Hacia un nuevo modelo europeo de privacidad*, VVAA (Dir. J. L. Piñar Mañas), Ed. Reus, 2016, pp. 427-460.

Id. "La mayoría de las transferencias de datos desde Europa a EEUU, en el aire", *Abogacía Española*, 26 octubre de 2015. Disponible en *https://www.abogacia.es/2015/10/26/la-mayoria-de-las-transferencias-de-datos-desde-europa-a–eeuu-en-el-aire/* (consultado el 19 de octubre de 2018).

PIÑAR MAÑAS, J. L. y RECIO GAYO, M., *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Ed. Wolters Kluwer, 2018, pp. 156-160.

RALLO LOMBARTE, A., "Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", *Revista de derecho político*, Nº 85, 2012, pp. 13-56.

REBOLLO DELGADO, L.: *El derecho fundamental a la intimidad,* Ed. Dikynson, 2ª ed. Madrid, 2005.

REQUEJO ISIDRO, M. "La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el Reglamento (UE) 2016/679", *La Ley Mercantil*, nº 42, diciembre 2017, pp. 1-25.

RIPOLL CARULLA, S., "Aplicación territorial del reglamento", en *Reglamento general de protección de datos: Hacia un nuevo modelo europeo de privacidad*, VVAA (Dir. J. L. Piñar Mañas), Ed. Reus, 2016, pp. 77-186.

SWIRE, P., HEMMINGS, J., "The Cloud Act and its Impact on Cross-Border Access to the Contents of Communications", 25 de marzo de 2018; *https://www.alstonprivacy.com/cloud-act-impact-cross-border-access-contents-communications/* (última visualización el 29.03.2019).

URIARTE LANDA, I., "Ámbito de aplicación material", en *Reglamento general de protección de datos: Hacia un nuevo modelo europeo de privacidad*, VVAA (Dir. J. L. Piñar Mañas), Ed. Reus, 2016, pp. 63-76.

VV.AA, *Monográfico de la Asociación Profesional Española de Privacidad (APEP) sobre sentencia del TJUE que anula el acuerdo para la transferencia de datos*

personales UE – EEUU "Safe Harbor", disponible en *https://www.apep.es/monografico-safe-harbor/?v=04c19fa1e772*.

VOGEL, P. S.; JONES, S., "The Cloud Act's Dramatic Impact on International Privacy Laws", 7 de junio de 2018, *https://www.ecommercetimes.com/story/85374.html* (última visualización el 29.03.2019).

ZABÍA DE LA MATA, J.(Coord.), VV.AA., *Protección de datos: Comentarios al Reglamento*, Ed. Lex Nova, 2008.