LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES

Grado en Derecho

Universidad de Zaragoza

2021-2022

Leyre Lorente Laborda

Directora: Profª Drª Katia Fach Gómez

Resumen: La finalidad de este trabajo es poner en relieve la creciente importancia que la protección de datos personales alcanza en nuestros días en el ámbito de las transferencias internacionales. Para ello analizaremos las sentencias STJUE de 6 de octubre de 2015 y de 16 de julio de 2020, ambas conocidas como *Schrems I y II*. Asimismo, analizaremos cuáles son las consecuencias de sus respectivos fallos y cómo afectaron a la normativa vigente en materia de protección de datos a nivel europeo y mundial.

Palabras clave: Protección de datos de carácter personal. Schrems. Transferencias Internacionales de Datos Personales. Puerto Seguro. Escudo de Privacidad. Reglamento General de Protección de Datos. Nivel adecuado de protección.

Abstract: The purpose of this paper is to highlight the growing importance of personal data protection in the field of international transfers. To do so, we will analyze the CJEU judgments of 6 October 2015 and 16 July 2020, both known as *Schrems I and II*. We will also analyze the consequences of their respective rulings and how they affected the current data protection regulations at European and global level.

Key words: Personal Data Protection. Schrems. International Personal Data Transfers. Safe Harbour. Privacy Shield. RGPD. Adequate level of privacy protections.

1. ÍNDICE DE ABREVIATURAS

AEPD Agencia Española de Protección de Datos

Carta Carta de los Derechos Fundamentales de la Unión Europea

Decisión CPT Decisión de la Comisión, de 5 de febrero de 2010 , relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo

DPA Data Protection Act

EDPB European Data Protection Board

EEE Espacio Económico Europeo

EEUU Estados Unidos

GDPR General Data Protection Regulation

RGPD Reglamento General de Protección de Datos

Schrems I Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015. Asunto C-326/14, Maximilian Schrems y Facebook Ireland Limited.

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

SEPD Supervisor Europeo de Protección de Datos

STJUE Sentencia del Tribunal de Justicia de la Unión Europea

TID Transferencia Internacional de Datos

TJUE Tribunal de Justicia de la Unión Europea

UE Unión Europea

2. INTRODUCCIÓN

En un mundo globalizado gracias a la constante evolución de la tecnología, el flujo masivo de datos a nivel nacional, europeo y mundial supone una cuestión importante a tener en cuenta en los ámbitos político, jurídico, digital y económico. Junto a ella, la protección de dichos datos se encuentra en el punto de mira de las instituciones europeas y del resto de países con los que se entablan relaciones en este sentido desde hace años.

Especialmente desde que dos sentencias muy importantes del Tribunal de Justicia de la Unión Europea -las conocidas como *caso Schrems I* y *II*- tirasen por tierra los dos acuerdos transatlánticos en materia de protección de datos – a saber, el acuerdo *Safe Harbour* y el *Privacy Shield*- que permitían una circulación ininterrumpida entre la Unión Europea y los Estados Unidos de América. Y que, con ello, demostraran que las instituciones estadounidenses no estaban cumpliendo con su parte de los tratados al almacenar los datos de los ciudadanos europeos obtenidos a través de grandes plataformas de redes sociales empleadas por millones de personas y tampoco facilitaran a las partes que pudieran tomar la vía judicial ante los Tribunales estadounidenses para reparar los daños resultantes de la violación de su privacidad por parte del Gobierno[1].

Ello deriva de la asimetría en el nivel de protección de los datos personales en el que se basan las autoridades de control de la Unión Europea y la Administración de los Estados Unidos. Mientras que las primeras tratan de alcanzar el máximo nivel de protección, prevaleciendo el derecho fundamental a la protección de datos de carácter personal sobre el resto, las instituciones estadounidenses sitúan la seguridad nacional por encima de los derechos fundamentales a la intimidad y a la privacidad. Encontrándose así los legisladores un gran problema a la hora de crear un marco legislativo que garantice la

[1] Baumohl, Chris, *Piercing the Veil: Reconciling FISA and the State Secrets Privilege in the Schrems II Era* (November 2, 2021). Comment, Piercing the Veil: Reconciling FISA and the State Secrets Privilege in the Schrems II Era 71 Am. U. L. Rev. 235 (2021), Disponible en SSRN: https://ssrn.com/abstract=3938362

transferencia segura de los datos de los ciudadanos europeos a los servidores de las plataformas sociales cuando éstos se encuentren en suelo estadounidense.

De ahí que, siendo la protección de datos de carácter personal un derecho fundamental proclamado por el artículo 18.4 de nuestra Constitución, el 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea y el 16.1 del Tratado de Funcionamiento de la Unión Europea, además de encontrarse en vigor la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales, no es extraño que las autoridades de todos los países envueltos en este tipo de acuerdos se hayan visto en la necesidad de tomarse más en serio las medidas de control del tratamiento de los datos de carácter personal y asegurar su cumplimiento. Asimismo, es preciso señalar que la protección de datos se encuadra en la consagración de los derechos a la intimidad y a la vida (artículos 7 y 8 de la Carta), en combinación con el derecho a la tutela judicial[2] (artículo 47 de la misma).

Si bien es cierto que, en su momento, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos fue un gran paso en la gestación de este derecho en la Unión Europea, fue uno del que todavía se están subsanando errores, como podremos ver en las páginas siguientes.

[2] Kahansky, R., Marcela, C. (2019). *Vigencia del Derecho europeo de protección de datos personales*.

3. CONCEPTO DE TRANSFERENCIA INTERNACIONAL DE DATOS

La definición legal del concepto objeto de estudio la encontramos en el Informe explicativo del artículo 14 del Convenio 108+[3], que lo define como aquellos datos personales que se divulgan o se ponen a disposición de un receptor sujeto a la jurisdicción de otro Estado u organización internacional[4]. Se trata de una definición de carácter doctrinal y jurisprudencial que viene dada por la STJUE Lindqvist[5].

De este modo, entendemos que una transferencia internacional de datos se produce cuando los datos personales, que son tratados por un responsable o un encargado en el Espacio Económico Europeo (EEE; países de la Unión Europea, Islandia, Liechtenstein y Noruega), son enviados a un tercer país u organización internacional, fuera de dicho territorio[6].

En la regulación actual, el Capítulo V del Reglamento General de Protección de Datos (RGPD) se integra por los artículos 44 a 50, que se dedican a establecer el régimen que deben respetar tanto los responsables como los encargados cuando realicen las transferencias a un tercer país[7]. Ahondaremos en estos preceptos posteriormente.

---

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

[4] Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los Estados Miembros. Juan José Gonzalo Domenech. Cuadernos de Derecho Transnacional (Marzo 2019), Vol. 11, No 1, pp. 350-371 ISSN 1989-4570 - www.uc3m.es/cdt - DOI: https://doi.org/10.20318/cdt.2019.4624.

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

[6] Guías Jurídicas Wolter Kluwer (https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1jTAAAkNjEwNjE7Wy1KLizPw8WyMDQwsDU0OwQGZapUt-ckhlQaptWmJOcSoA6fqAajUAAAA=WKE)

[7] De Miguel Asensio, P. *Directrices sobre el concepto de transferencia internacional de datos personales y su interpretación con el ámbito de aplicación territorial del RGPD* (https://pedrodemiguelasensio.blogspot.com/2021/11/directrices-sobre-el-concepto-de.html).

3.1 Distinción necesaria entre datos de carácter personal y datos de carácter no personal

Esta distinción se debe a que, a efectos de transferencia, tienen su propia regulación: mientras que los datos no personales se recogen en el Reglamento (UE) 2018/1807, del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, que establece un marco de libre circulación de datos no personales en la UE; los datos de carácter personal tienen una normativa más estricta y protectora que se encuentra en el RGPD.

Concretamente, en el artículo 4, apartado 1, del Reglamento, se entiende por «datos personales» toda información sobre una persona física identificada o identificable (el interesado). Asimismo, se da una definición negativa del concepto de datos de carácter no personal, entendiendo por éstos a aquellos que no son datos personales tal y como se definen en el precepto anteriormente mencionado (artículo 3, apartado 1, del Reglamento 2018/1807).

El RGPD tiene su fundamento en la tutela de un derecho fundamental, referido únicamente a las personas físicas y que se vincula estrechamente con su intimidad y privacidad[8], según se desprende del artículo 1, apartado 2, del Reglamento. También se puede analizar la protección de datos personales cuando entendemos que éstos son un «activo» sobre el que su titular puede disponer para transacciones económicas[9].

De esta forma, el Reglamento establece unos mecanismos de control de protección de estos datos cuando circulen libremente y se transfieran a países que se encuentran fuera del EEE. Estos terceros países deben garantizar un nivel de protección equivalente al que exige la UE, demostrable a través de decisiones de adecuación, garantías adicionales, cláusulas contractuales tipo de protección y normas corporativas vinculantes. Si bien

---

[8] De Miguel Asensio, P. *Reglamento (UE) 2018/1807 sobre libre circulación de datos no personales* (https://pedrodemiguelasensio.blogspot.com/2018/12/reglamento-ue-20181807-sobre-libre.html).

[9] Rodriguez Pineau, E., & Torralba Mendiola, E. (2022). *Transferencia de datos personales fuera del EEE en el nuevo marco del reglamento general: Especial referencia al caso estadounidense y el reino unido tras el brexit*. *La protección de las transmisiones de datos transfronterizas* (1ª Ed. ed., pp. 1-412). Pamplona, Navarra: Aranzadi.

existen ciertas excepciones, reguladas en el artículo 49 del Reglamento, que permiten la transferencia internacional de datos personales cuando no existen una decisión de adecuación o garantías adecuadas.

3.2 Nivel adecuado de protección

El nivel adecuado de protección para las transferencias internacionales de datos es un concepto muy importante que garantiza que tanto los derechos de los titulares de esos datos, como los datos personales en sí, son objeto de un tratamiento respetuoso y dentro de unos límites que protegen de las injerencias y discriminaciones arbitrarias. El nivel adecuado de protección para la transferencia internacional de datos desempeña un importante papel para lograr los objetivos de una sociedad y una economía digitales inclusivas y prósperas[10].

A este respecto, cabe señalar que el RGPD no define el concepto de nivel adecuado, sino que es una construcción jurisprudencial del TJUE, que surge a raíz de la sentencia *Schrems I*[11]: «debe entenderse la expresión "nivel de protección adecuado" en el sentido de que exige que ese tercer país garantice, efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46/CE, entendida a la luz de la Carta de los Derechos Fundamentales de la Unión Europea» (apartado 73 de las Conclusiones del Abogado General).

Para determinar que un tercer país extracomunitario cuenta con un nivel de protección equivalente al de la UE se desarrolló el ≪modelo de adecuación≫, que es un mecanismo que tiene por finalidad asegurar la protección de las personas físicas cuando llevan a cabo

---

[10] Recio Gayo, M. (2019). *Nivel adecuado para transferencias internacionales de datos*. [Adequate Level of International Data Transfers] *Revista De La Facultad De Derecho Universidad CEU San Pablo (Brasil), nº83*(diciembre-mayo), 207-240.

[11] STJUE (Gran Sala) de 6 de octubre de 2015. Asunto C-326/14, *Maximilian Schrems y Facebook Ireland Limited.*

transferencias internacionales de datos personales[12]. Para ello, se realiza una evaluación del país al que se van a transferir los datos a efectos de que la Comisión Europea confirme formalmente, con efectos vinculantes para los Estados miembros, que el nivel de protección de datos en un tercer país u organización internacional es sustancialmente equivalente al nivel de protección de datos en la Unión Europea» (Grupo de Trabajo del Artículo 29[13], 2018, p. 2).

La Comisión Europea evaluará al país atendiendo a los siguientes elementos, recogidos en el artículo 45, apartado 2, del RGPD: el Estado de Derecho, la existencia y el funcionamiento efectivo de una o varias autoridades de protección de datos o autoridades de control independientes en el tercer país, y los compromisos internacionales.

El TJUE establece en la sentencia *Schrems I* que, en caso de que el tercer país no garantice el nivel adecuado de protección, las autoridades nacionales de control están facultadas para suspender o prohibir una transferencia de datos a dicho territorio (considerando 5 de la Decisión de Ejecución 2016/2297 [14] respecto de la Decisión CPT[15]).

---

[12] Recio Gayo, M. (2019). *Nivel adecuado para transferencias internacionales de datos*. [Adequate Level of International Data Transfers] *Revista De La Facultad De Derecho Universidad CEU San Pablo (Brasil), nº83*(diciembre-mayo), 207-240.

[13] Grupo de Trabajo del Artículo 29: es un órgano consultivo independiente creado a raíz de la Directiva 95/46/CE, y que está integrado por las Autoridades de Protección de Datos de todos los Estados miembros de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea. El GT29 fue disuelto con la entrada en vigor del RGPD en mayo de 2018. (https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_es y https://www.apcpd.es/que-es-y-quienes-forman-el-grupo-de-trabajo-del-articulo-29/)

[14] Decisión de Ejecución (UE) 2016/2297 de la Comisión, 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.

[15] Decisión de la Comisión, de 5 de febrero de 2010 , relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

4. MARCO NORMATIVO

4.1 Las Transferencias Internacionales de Datos con *Safe Harbour* y *Privacy Shield*

El 24 de octubre de 1995 entró en vigor la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos[16]. Esta Directiva permitía las transferencias internacionales de datos entre los Estados Miembros de la Unión Europea, pero no así respecto de terceros Estados.

De ahí que surgieran los acuerdos de *Safe Harbour* o «Puerto Seguro» [17] y, posteriormente, el *Privacy Shield* o «Escudo de Privacidad»[18] como mecanismos complementarios que regulaban la protección de datos en las transferencias internacionales entre la Unión Europea y Estados Unidos hasta sus respectivas derogaciones en 2015 y 2020, debido a que no cumplían con el nivel de protección adecuado que actualmente exige la Unión Europea.

El acuerdo de *Safe Harbour* surgió en el año 2000 como un mecanismo fundamental del entramado que facilitaba las transferencias internacionales de datos desde la UE a EEUU[19] y viceversa, resultando en un aumento del tráfico de la información transmitida. Para ello, contenía una serie de principios cuyo cumplimiento, *prima facie*, satisfacía el nivel de protección adecuado que la Unión Europea requería en el art. 25 de la Directiva

---

[16] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (http://data.europa.eu/eli/dir/1995/46/oj)

[17] Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO 2000, L 215, p. 7).

[18] 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.

[19] De Miguel Asensio, P. *Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia*, *La Ley Europea*, Número 31, 2015, pp. 1-10.

95/46/CE para que se pudiera dar de manera efectiva, ininterrumpida y segura el flujo de datos personales entre los ciudadanos europeos y las empresas estadounidenses.

Estos principios, de adhesión voluntaria, se encuentran en el Anexo I de la Decisión 2000/520/CE, y son los siguientes: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación. Junto a ellos, en el Anexo II de la Decisión, el Departamento de Comercio de Estados Unidos publicó una serie de preguntas frecuentes (FAQ) que los complementaban e instruían su aplicación en la práctica.

De acuerdo con este régimen, todas aquellas entidades estadounidenses, controladas por el Departamento Federal de Comercio de EEUU, que observaran estos principios en sus políticas de privacidad cumplían efectivamente con el nivel de protección adecuado que exigía en aquel momento la Unión Europea, y podían aplicar un sistema de auto certificación que les permitía prescindir de la negociación de cada uno de los contratos en materia de protección de datos personales y de la auditoría o supervisión por los órganos pertinentes. A su vez, dichas compañías debían proveer a los usuarios de mecanismos de resolución de conflictos para posibles reclamaciones y renovar anualmente su conformidad con dichos principios.

Este es el caso de la empresa Facebook Inc., que fue demandada por el Sr. Maximilian Schrems (Caso *Schrems I*, asunto C- 326/14) ante el Tribunal Regional Civil de Viena por, en opinión del reclamante, la reiterada vulneración de la normativa en materia de protección de datos y de intimidad, infringiendo disposiciones de los ordenamientos jurídicos austriaco, irlandés y de la Unión[20].

Dado que esta sentencia se comentará posteriormente, en este punto únicamente vamos a mencionar el gran impacto que tuvo su fallo en las transferencias internacionales de datos:

[20] Conclusiones del Abogado General Sr. M. Bobek, presentadas el 14 de noviembre de 2017. *Maximilian Schrems contra Facebook Ireland Limited*. Petición de decisión prejudicial planteada por el Oberster Gerichtshof. (https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:62016CC0498)

la Decisión 2000/520/CE es declarada inválida por el Tribunal de Justicia de la Unión Europea[21] por vulnerar las exigencias del artículo 25.6 de la Directiva 95/46/CE[22].

Las consecuencias inmediatas del fallo fueron la ilegalización de todas aquellas transferencias de datos que se llevasen a cabo tras la sentencia *Schrems I*, y la urgente necesidad de establecer un nuevo mecanismo de transmisión de datos entre Europa y Estados Unidos con las garantías de protección adecuadas.

De ahí que, en abril de 2016, el Parlamento Europeo adoptase nuevas normas de protección de datos focalizadas en proporcionar a los ciudadanos europeos un recurso para recuperar el control de sus datos personales[23]: el conocido como acuerdo de *Privacy Shield*.

Este mecanismo también se basaba, como el de *Safe Harbour*, en un sistema de auto certificación por el Departamento de Comercio de Estados Unidos. Sin embargo, se añaden a este sistema ciertos requisitos, como límites temporales en la custodia de los datos personales, derechos de acceso, políticas de publicidad o privacidad, etc. Además, las autoridades de protección europeas y estadounidenses tienen el deber de controlar anualmente el cumplimiento de los nuevos principios que integran este mecanismo. Y se crea la figura del Defensor, que recibirá y decidirá sobre las quejas y las dudas que presenten los ciudadanos europeos, y se incluye la supervisión judicial como mecanismo de protección.

Según la doctrina mayoritaria[24], las mejoras que, *a priori*, este acuerdo iba a suponer en las transferencias transatlánticas de datos no lograron acabar con las deficiencias de la

---

[21] STJUE (Gran Sala), De 6 De Octubre De 2015, Asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd*. 2015).

[22] De Miguel Asensio, P. *Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia*, *La Ley Europea*, Número 31, 2015, pp. 1-10.

[23] Tihomir Katulić, Ph.D., Goran Vojković, Ph.D. "From Safe Harbour to European Data Protection Reform", MIPRO 2016, May 30 - June 3, 2016, Opatija, Croatia.

[24] En especial gracias al informe que Grupo de Trabajo del Artículo 29 realizó respecto del acuerdo del Escudo de Privacidad.

legislación estadounidense en tres importantes sectores de la protección de datos: la circulación y custodia de los datos, el nivel de los derechos de protección y la efectividad y complicación de los mecanismos de queja[25].

La primera de las deficiencias fue de mayor calibre, dado que las autoridades estadounidenses cuentan con sistemas de vigilancia[26] que permiten el acceso y utilización de datos personales por motivos de seguridad nacional, lo cual infringe el principio de proporcionalidad. Esto se puso de manifiesto en la sentencia *Schrems II*, cuyo fallo invalidó el acuerdo de *Privacy Shield* en julio de 2020[27]. En consecuencia, nos encontramos con un marco jurídico de incertidumbre[28] en cuanto a la protección de datos que ha causado numerosos problemas entre la UE y las grandes plataformas tecnológicas como Google o Facebook.

Finalmente, el 25 de marzo de este año la presidenta de la Comisión Europea, Úrsula Von der Leyen, y el actual presidente de los Estados Unidos, Joe Biden, anunciaron un nuevo acuerdo transatlántico en materia de protección de datos. Éste incluye como novedades la creación de un Tribunal de Revisión de Protección de datos independiente a la administración estadounidense.

No obstante, ya han surgido críticas a este nuevo acuerdo, y la más significativa es la que señala que, mientras no se cambien las políticas de recopilación[29] en Estados Unidos, este acuerdo también fracasará. Así lo ha dejado caer Maximilian Schrems, el abogado y activista austriaco experto en Derecho informático y materia de protección de datos que

---

[25] Fabien Terpan, *EU-US Data Transfer from Safe Harbour to Privacy Shield: back to square one?, European papers: a journal on law and integration*, ISSN-e 2499-8249, Vol. 3, Nº. 3, 2018, págs. 1045-1059.

[26] PRISM: programa que garantiza a las autoridades estadounidenses el acceso a datos almacenados en servidores de los EEUU que son propiedad o están controlados por una serie de empresas de Internet, como Facebook USA.

[27] Sentencia del Tribunal de Justicia (Gran Sala) de 16 de julio de 2020. Asunto C-311/18, *Data Protection Commissioner contra Facebook Ireland Ltd y Maximillian Schrems.* (https://curia.europa.eu/juris/liste.jsf?num=C-311/18)

[28]https://www.eleconomista.es/tecnologia/noticias/11689279/03/22/Nuevo-acuerdo-entre-Europa-y-Estados-Unidos-por-la-transmision-y-proteccion-de-datos-.html
[29]https://www.eleconomista.es/tecnologia/noticias/11689279/03/22/Nuevo-acuerdo-entre-Europa-y-Estados-Unidos-por-la-transmision-y-proteccion-de-datos-.html

se querelló en 2010 contra Facebook y consiguió tumbar dos acuerdos transatlánticos en dicha materia, en su cuenta de Twitter en respuesta al anuncio de la presidenta de la Comisión.

4.2 Comentario sobre la sentencia del TJUE de 6 de octubre de 2015 (asunto C-326/14): *Schrems I*

El Sr. Maximilian Schrems, experto en Derecho informático y en materia de protección de datos, es usuario de la plataforma digital Facebook desde 2008, red social que utiliza tanto con fines privados como profesionales: posee una cuenta privada, cuyo nombre de usuario está en caracteres cirílicos para evitar que se le busque, y una página profesional en la que informa sobre sus acciones judiciales contra Facebook Ireland, sus conferencias, participaciones en debates públicos, solicitar donaciones y hacer publicidad de sus libros[30].

El Sr. Schrems interpuso varias reclamaciones en 2013 ante el Comisario irlandés de Protección de Datos, la autoridad nacional de control, en relación con la vulneración del derecho a la protección de datos y de otros derechos fundamentales, recogidos en la Carta de Derechos Fundamentales de la Unión Europea del año 2000 (en adelante, la Carta), a manos de servidores localizados en Estados Unidos y del programa de vigilancia masiva de la Agencia de Seguridad Nacional (en inglés: National Security Agency o NSA), conocido como PRISM[31]. Todo ello a la luz de las revelaciones realizadas por Edward Snowden[32] ese mismo año acerca de los programas de vigilancia estadounidenses, quien afirmaba que el Gobierno estadounidense había desarrollado un sistema global de vigilancia masiva y lo empleaba sin el conocimiento ni consentimiento de su ciudadanía[33]. Dichos programas estaban dirigidos, en principio, a la recopilación de

---

[30] Recopilación de la Jurisprudencia de la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*.
[31] Programa clandestino de vigilancia electrónica operada por la Agencia de Seguridad Nacional (NSA) de Estados Unidos para la recogida masiva de datos procedentes de, al menos, nueve grandes compañías de Internet.
[32] Es un consultor informático, antiguo empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA), que filtró a través de varios periódicos estadounidenses documentos clasificados como alto secreto acerca de los programas de vigilancia masiva de la NSA, éntrelos que se incluyen PRISM y XKeyscore.
[33] Pinto, T. (2019, 09-10-2019). El legado de Snowden: Las filtraciones que transformaron Internet. *El País* (https://elpais.com/tecnologia/2019/10/07/actualidad/1570455695_974155.html)

información para la prevención y represión del terrorismo, pero se empleaban para violar el derecho fundamental a la intimidad y privacidad a nivel mundial.

Las reclamaciones del Sr. Schrems no tuvieron éxito, puesto que el Comisario indicó que, dentro del marco normativo del Puerto Seguro, en relación con la Decisión 2000/520/CE, Estados Unidos garantizaba el nivel adecuado de protección de los datos transferidos. El Sr. Schrems interpuso un recurso ante el Tribunal Supremo de Irlanda.

El Alto Tribunal irlandés estimó que la legalidad de la Decisión 2000/520/CE debía apreciarse con arreglo al Derecho europeo, por lo que decidió suspender el procedimiento y plantear al TJUE dos cuestión prejudiciales, que comentaremos más adelante.

El Sr. Schrems demandó a Facebook Ireland Ltd. ante los tribunales austriacos, alegando que la política de Facebook contraviene la normativa en materia de protección de datos y de la intimidad, infringiendo disposiciones de los ordenamientos jurídicos austriaco, irlandés y de la Unión[34]. Los datos eran transferidos desde Irlanda a servidores localizados en Estados Unidos[35], en donde eran procesados y utilizados para Facebook. En Estados Unidos, los datos podían estar sujetos a un control estatal por parte de las agencias de investigación gubernamentales, lo cual afectaba a los derechos de protección de datos de los usuarios europeos.

En su demanda, el Sr. Schrems formula varias pretensiones, entre las que se encuentran una acción declarativa relacionada con el deber de cumplimiento de instrucciones por parte del prestador de los servicios, así como su posición como responsable del tratamiento de datos; una acción de información sobre el uso de los datos personales; y una acción de cesación respecto al uso de los datos.

El Tribunal Regional Civil de Viena desestimó la demanda basándose en que, puesto que el Sr. Schrems empleaba Facebook tanto para usos sociales como profesionales, no podía

---

[34] Conclusiones del Abogado General Sr. Y. Bot, presentadas el 23 de septiembre de 2015. *Maximillian Schrems c. Data Protection Commissioner*. Petición de decisión prejudicial planteada por la High Court of Ireland.

[35] Tuomas Ojanen, "*Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter: ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner*". (https://www-cambridge-org.cuarzo.unizar.es:9443/core/services/aop-cambridge-core/content/view/S1574019616000225)

acogerse al foro del consumidor que regulan los artículos 15 y 16 del entonces vigente Reglamento nº44/2001[36]. La otra razón por la cual el tribunal desestimó la demanda fue que el Sr. Schrems era el cesionario de acciones procedentes de otros siete usuarios de la plataforma social. Dichos usuarios estaban domiciliados en Austria, otros Estados miembros y en Estados no miembros, por lo que no se podía aplicar el apartado 1 segundo supuesto del artículo 16 del Reglamento nº44/2001, que señala lo siguiente: «La acción entablada por un consumidor contra la otra parte contratante podrá interponerse ante los tribunales del Estado miembro en que estuviere domiciliada dicha parte o ante el tribunal del lugar en que estuviere domiciliado el consumidor». Según dicho órgano jurisdiccional, el fuero privado del cedente no puede ser transmitido al cesionario[37].

Visto el auto, el demandante interpuso recurso de apelación ante el Tribunal Superior Regional de Viena, que modificó parcialmente la resolución, estimando las pretensiones relacionadas con la posición de consumidor del Sr. Schrems. Ambos litigantes recurrieron en casación ante el Tribunal Supremo Civil y Penal austriaco, que decidió suspender el procedimiento y plantear al TJUE las siguientes cuestiones prejudiciales[38]:

1º. Si el artículo 15 del Reglamento nº44/2001 debe interpretarse en el sentido de que un usuario de una cuenta privada de Facebook tiene la condición de consumidor.
2º. Si un consumidor puede invocar la regla especial de competencia para consumidores del artículo 16, apartado 1, del Reglamento nº44/2001 no sólo respecto a sus propias acciones, sino también respecto de las acciones que le hayan sido cedidas por otros consumidores domiciliados en el mismo Estado miembro, en otros Estados miembros y en terceros Estados.

[36] Reglamento (CE) nº 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil.
[37] Conclusiones del Abogado General Sr. Y. Bot, presentadas el 23 de septiembre de 2015. *Maximillian Schrems c. Data Protection Commissioner*. Petición de decisión prejudicial planteada por la High Court of Ireland.
[38] Conclusiones del Abogado General Sr. Y. Bot, presentadas el 23 de septiembre de 2015. *Maximillian Schrems c. Data Protection Commissioner*. Petición de decisión prejudicial planteada por la High Court of Ireland.

El TJUE responde a las cuestiones prejudiciales de forma conjunta. Y conviene destacar que las conclusiones que alcanza el Tribunal coinciden con las del abogado general Bot, que fueron presentadas tan solo dos semanas antes de que el TJUE dictara su sentencia[39].

Respecto de la primera cuestión prejudicial, el TJUE señala que, como regla general, la competencia de los tribunales se determina en función del domicilio del demandado. Si bien, existen ciertas situaciones, enumeradas de forma taxativa, en las que las acciones judiciales pueden llevarse a cabo ante el tribunal de otro Estado miembro. Dichos casos, que constituyen excepciones al principio general, deben interpretarse restrictivamente, aunque los conceptos que las configuran se interpretan de forma autónoma, siempre en relación con el sistema y objetivos del mencionado Reglamento, para garantizar su aplicación uniforme en todos los Estados miembros[40].

En este sentido, el Tribunal de Justicia se centra en el concepto de «consumidor» a la luz de los artículos 15 y 16 del Reglamento nº44/2001, que viene a interpretarse como «la posición de una persona en un contrato determinado y con la naturaleza y finalidad de éste, y no con la situación subjetiva de dicha persona, dado que una misma persona puede ser considerada consumidor respecto de ciertas operaciones y operador respecto de otras»[41]. Por lo tanto, sólo a aquellos contratos celebrados en el ámbito privado y sin fines profesionales se les podrá aplicar el régimen de los apartados 15 a 17 del Reglamento en materia de protección del consumidor.

En relación a lo anterior, se debe tener en cuenta que la delimitación del concepto de consumidor también obedece a la evolución por parte de quien es usuario durante un tiempo prolongado de la red social[42], en el sentido de que con el paso del tiempo la actividad profesional del usuario se funde con los fines privados. En el caso de autos,

---

[39] Uría Gavilán, E. (2016). Derechos fundamentales versus vigilancia masiva. *Revista de Derecho Comunitario Europeo*, 53, 261-282. Doi: http://dx.doi.org/10.18042/cepc/rdce.53.07

[40] Recopilación de la Jurisprudencia de la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*. Ap. 27.

[41] Recopilación de la Jurisprudencia de la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*. Ap. 29.

[42] De Miguel Asensio, P. "*Demandas internacionales contra redes sociales: el concepto de consumidor y la evolución de la legislación sobre datos personales*" (https://pedrodemiguelasensio.blogspot.com/2017/11/demandas-internacionales-contra-redes.html)

como ya se ha apuntado, el Sr. Schrems tiene habilitadas tanto cuentas privadas como una página profesional en la que publicita sus libros, conferencias e informaciones sobre las acciones judiciales, además de recaudar donaciones y aceptar la cesión de acciones por parte de otros usuarios de la plataforma digital. Lo que lleva a considerar que se trata de un contrato de «finalidad doble», que sirve tanto a objetos profesionales como privados[43].

De acuerdo con reiterada jurisprudencia del TJUE sobre la interpretación de la condición de consumidor, debemos tener en cuenta la naturaleza y finalidad de cada contrato y la vinculación entre ambos, ya que si ésta «es tan tenue que pudiera considerarse marginal»[44], se mantiene dicha condición. En consecuencia, si el demandante utilizó su cuenta de Facebook para fines privados en el momento de interponer la demanda, tendrá la condición de consumidor. Cuestión que parece desprenderse de los hechos probados, en palabras del Abogado General.

Asimismo, el TJUE dictó que, dentro del artículo 15 del Reglamento nº44/2001, la condición de «consumidor» también engloba las actividades como publicar libros, conferencias, recaudar donaciones, etc., dado que excluir dichas actividades del concepto equivaldría a impedir una defensa efectiva del consumidor[45].

En cuanto a la segunda cuestión prejudicial, debemos tener muy presentes las reglas de competencia judicial internacional en materia de consumidores, que suponen una excepción tanto a la regla general del artículo 2, apartado 1, de dicho Reglamento, con base en la cual ≪[…] las personas domiciliadas en un Estado miembro estarán sometidas, sea cual fuere su nacionalidad, a los órganos jurisdiccionales de dicho Estado≫, como a la regla de competencia especial en materia de contratos del artículo 5, apartado 1a, que señala que: «Las personas domiciliadas en un Estado miembro podrán ser demandadas

---

[43] Conclusiones Del Abogado General Sr. M. Bobek, Presentadas El 14 De Noviembre De 2017. *Maximillian Schrems c. Facebook Ireland Ltd.*Petición De Decisión Prejudicial Planteada Por El Oberster Gerichtshof.

[44] Sentencia de 20 de enero de 2005, *Gruber* (C-464/01, EU:C:2005:32), apartado 39, sobre los artículos 13 a 15 del Convenio de Bruselas.

[45] Recopilación de la Jurisprudencia de la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*.

en otro Estado miembro: en materia contractual, ante el tribunal del lugar en el que hubiere sido o debiere ser cumplida la obligación que sirviere de base a la demanda».

La competencia de los órganos jurisdiccionales varía en materia de contratos celebrados por consumidores en función del criterio de la parte más débil: el consumidor. De manera que el artículo 16, apartado 1, permite que la acción sea interpuesta ante los tribunales del Estado miembro en que estuviere domiciliado el consumidor. Pero, en palabras del TJUE, esto no quiere decir que un consumidor pueda ejercitar, junto con sus propias acciones, las acciones de idéntico sentido que le hayan sido cedidas por otros consumidores domiciliados en lugares del mismo Estado miembro, en otros Estados miembros o en terceros Estados.

4.2.1 Fallo y consecuencias

Por un lado, el TJUE sentenció que el Sr. Schrems tiene la condición de «consumidor» en el sentido de los artículos 15 a 17 del Reglamento nº44/2001. Sin embargo, dicha condición no le permite ejercitar las acciones de idéntico sentido que le sean cedidas por otros usuarios de la plataforma social Facebook, aunque estén domiciliados en el mismo Estado.

Por otro lado, dicha sentencia dio lugar a la invalidación de la Decisión 2000/520/CE de la Comisión relativa a los principios de puerto seguro. Esto trae causa de las dos cuestiones prejudiciales que planteó el Alto Tribunal irlandés al TJUE -bajo el paraguas del artículo 267 TFUE[46]-, y que son las siguientes:

- ¿Está vinculado dicho comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los arts. 7, 8 y 47 de la Carta [47]y no obstante lo dispuesto en el art. 25, apdo. 6, de la Directiva 95/46/CE?

[46] Artículo 267 TFUE. El Tribunal de Justicia de la Unión Europea será competente para pronunciarse, con carácter prejudicial: sobre la validez e interpretación de los actos adoptados por las instituciones, órganos u organismos de la Unión.

[47] Los artículos 7, 8 y 46 de la Carta recogen el respeto a la vida privada y familiar, la protección de datos de carácter personal y el derecho a la tutela judicial efectiva y a un juez imparcial.

– En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520? [48]

Como ya hemos mencionado anteriormente, la Decisión sobre los principios de Puerto Seguro se basaba en un sistema de auto certificado que, *a priori*, era supervisado por la Comisión Federal de Comercio de Estados Unidos, para garantizar que se cumplía el nivel adecuado de protección en las transmisiones de datos.

Sin embargo, durante la vigencia de la Decisión, ha quedado patente, en tres distintas evaluaciones sobre el cumplimiento por parte de las empresas estadounidenses de los principios de Puerto Seguro, que se estaba vulnerando el derecho de los usuarios de datos europeos, ya que los servidores de las compañías y organizaciones localizados en Estados Unidos analizaban y procesaban los datos, que luego eran empleados por los servicios de inteligencia gubernamentales bajo la premisa de seguridad nacional, defensa y seguridad del Estado.

A esto ha de sumársele que, en la evaluación llevada a cabo por la compañía australiana *Galexia*, se destacaba la ineficacia e incluso inexistencia de mecanismos de resolución de conflictos disponibles para los consumidores por parte las empresas y organizaciones estadounidenses[49], lo cual vulneraba el derecho a la tutela judicial efectiva del artículo 47 de la Carta.

En respuesta a las cuestiones prejudiciales planteadas, el TJUE sentenció que las autoridades nacionales no deben dejar de supervisar el cumplimiento de la legislación en materia de protección de datos y del nivel adecuado de protección por parte de terceros Estados. En concreto, bajo la legislación irlandesa la transferencia de datos fuera del territorio nacional está prohibida, salvo cuando el tercer país asegure un nivel de protección adecuado de los datos personales y del derecho a la vida privada. En

---

[48] Uría Gavilán, E. (2016). *Derechos fundamentales versus vigilancia masiva. Revista de Derecho Comunitario Europeo*, 53, 261-282. Doi: http://dx.doi.org/10.18042/cepc/rdce.53.07

[49] Tihomir Katulić, Ph.D., Goran Vojković, Ph.D. "*From Safe Harbour to European Data Protection Reform*", *MIPRO* 2016, May 30 - June 3, 2016, Opatija, Croatia.

consecuencia, el Comisario debería haber investigado las reclamaciones del Sr. Schrems[50].

Asimismo, el TJUE declaró nula la Decisión de los principios de Puerto Seguro debido a las reiteradas vulneraciones de la legislación europea por los proveedores y el Gobierno estadounidenses y a las carencias en materia de protección de datos que presentaba su legislación.

De acuerdo con el TJUE, el derecho al respeto de la vida privada a nivel de la UE exige que las excepciones a la protección de datos personales y las limitaciones a esa protección no excedan de lo estrictamente necesario. En consecuencia, en este caso, «no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización[51]».

Tras la publicación de esta sentencia, el Grupo de Trabajo del Artículo 29 dejó patente en su informe el hecho de que las instituciones europeas y estadounidenses debían iniciar conversaciones a fin de "encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos a Estados Unidos", respetando los derechos fundamentales, todo ello mediante "mecanismos claros y vinculantes".[52]

---

[50] Chicharro Lázaro, A. (2016). *La trascendencia práctica del caso facebook en relación con la transferencia masiva de datos personales desde la unión europea a estados unidos*. In Sociedad Latina de Comunicación Social (Ed.), *La pantalla insomne* [Practical Implication of Facebook Ruling on the large-scale Personal Data Transfer from the EU to the USA] (2ª Ed ed., pp. 1782-1809). España: Cuadernos artesanos comunicación, 103.

[51] STJUE (Gran Sala), De 6 De Octubre De 2015, Asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd.* 2015). (https://eur-lex.europa.eu/legal-content/ES-EN/TXT/?from=en&uri=CELEX%3A62014CJ0362)

[52] Statement of the Article 29 Working Party, 16 de octubre de 2015. (https://ec.europa.eu/justice/article-29/pressmaterial/pressrelease/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf)

Posteriormente, la Agencia Española de Protección de Datos comunicó a las empresas que habían empleado este mecanismo para llevar a cabo las transferencias internacionales de datos, que ya no se podía utilizar este canal y que, a partir de enero de 2016, los responsables del tratamiento de datos debían informar al Registro General de Protección de Datos de la AEDP sobre la continuidad de las transferencias y la adecuación a la normativa de protección de datos.

4.2.2 Valoración de la sentencia Schrems I

En primer lugar, debemos tener en cuenta el contexto y fin para el que se crean los sistemas de vigilancia masiva estadounidenses: prevenir los ataques terroristas. En este sentido, el TJUE entiende la importancia que se le debe dar a la seguridad nacional, pero siempre con ciertos límites, ya que las autoridades nacionales no deben poner ésta por encima de la protección de la privacidad de los ciudadanos.

El TJUE incide, siguiendo el criterio del Abogado General Y. Bot[53], en que debe darse el nivel adecuado de protección exigido por la UE en las transferencias internacionales de datos, y aclara que los mecanismos para garantizar dicho nivel de adecuación no tienen por qué ser idénticos a los que emplea la UE, pero sí "deben ser eficaces en la práctica" (par. 74). Asimismo, las autoridades nacionales de control tienen el deber de revisar periódicamente que se esté cumpliendo el nivel de protección adecuado.

Esta posición del TJUE dista mucho de la que presentó en el caso Lindqvist en 2003, donde insistió en que el régimen jurídico de terceros países en cuanto a la protección de datos no debe ser una copia del régimen europeo[54], sino que se debía llevar a cabo un análisis basado en la proporcionalidad. A su vez, el TJUE concluye que no contar con garantías eficaces a las que los ciudadanos puedan acudir cuando consideren vulnerados sus derechos fundamentales en relación con sus datos personales infringe el derecho a la tutela judicial efectiva y determina que el derecho comunitario tampoco puede impedir el

---

[53] Conclusiones Del Abogado General Sr. M. Bobek, presentadas el 14 de noviembre de 2017. *Maximillian Schrems c. Facebook Ireland Ltd*. Petición de decisión prejudicial planteada por el Oberster Gerichtshof.

[54] Peers, S. (2015). *The Party's Over: EU Data Protection Law after the Schrems Safe Harbor Judgment. EU Law Analysis*. 7 de octubre. Disponible en: http://eulawanalysis.blogspot.cl/2015/10/the-partys-over-eu- data-protection-law.html

ejercicio de la misma, que en materia de protección de datos personales se concreta acudiendo a las autoridades nacionales de control[55].

Siguiendo esta nueva doctrina, lo que hace el TJUE es dar más independencia y poder a las autoridades nacionales, dejando que sean ellas quienes decidan en el caso concreto si la empresa en cuestión vulnera la legislación. En consecuencia, se rompe la uniformidad del Derecho de la Unión.

En mi opinión, esta forma de sentar un nuevo precedente por parte del TJUE mediante la declaración de invalidez de una norma que permitía la vulneración continua y masiva de la privacidad de los ciudadanos estadounidenses y europeos por parte de las instituciones y agencias de inteligencia de EEUU tuvo buenas intenciones, pero su ejecución no fue del todo correcta.

La declaración de invalidez del acuerdo de Puerto Seguro tuvo efectos negativos, ya que, por un lado, dejó en un limbo jurídico la transferencia de datos entre EEUU-UE, provocando una innecesaria falta de seguridad económica y jurídica en las empresas que empleaban dicho medio. Y, por otro lado, la casi inmediata sanción a todas aquellas organizaciones que no se acomodasen a la legislación vigente -que ya en su momento presentaba un gran desfase con la realidad en España- trajo consigo sonadas batallas legales contra la AEPD que podían haberse evitado si se hubiesen hecho las cosas como se debían: con calma.

4.3 Comentario sobre la sentencia del TJUE de 16 de julio de 2020 (asunto C-3122/18): *Schrems II*

Dado que las relaciones comerciales entre Europa y Estados Unidos y las transferencias de datos personales constituyen una parte importante y necesaria de la relación transatlántica, en particular, en la economía digital de hoy[56], era imperativa la creación

---

[55] Puerto, I., Sferrazza Taibi, P. *La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional*. Revista Derecho del Estado nº40, enero-junio de 2018, pp. 209-236.

[56] Guía acerca del Escudo de Privacidad UE-EEUU (https://www.aepd.es/sites/default/files/2019-09/guia-acerca-del-escudo-de-privacidad.pdf).

de una nueva regulación de las transferencias de datos entre ambos tras la invalidación en el año 2015 de la Directiva sobre los principios de puerto seguro (Decisión 2000/520/CE).

De ahí que, en abril de 2016, la Comisión Europea y el Departamento de Comercio de Estados Unidos negociaran un nuevo acuerdo, denominado Escudo de Privacidad o *Privacy Shield*. En principio, esta nueva decisión de adecuación cumplía con las garantías de protección de datos que debían avalar las empresas estadounidenses. Sin embargo, tras el fallo de la sentencia *Schrems II* (asunto C-311/18) el 16 de julio de 2020, que se procede a analizar a continuación, se vio que no era así. A raíz de ello, el TJUE anuló el acuerdo de Escudo de Privacidad, dejando las transferencias transatlánticas de datos entre Europa y Estados Unidos bajo la regulación del artículo 49 del Reglamento General de Protección de Datos (apto. 202 de la sentencia).

El Sr. Schrems impugnó el Escudo de Privacidad en 2015 ante los tribunales irlandeses, alegando que el Derecho estadounidense obliga a Facebook Inc. a poner los datos personales que se le transfieren a disposición de las autoridades estadounidenses, como la NSA y el FBI. Esgrimió que, al utilizarse esos datos en el marco de diferentes programas de vigilancia de una manera incompatible con los artículos 7, 8 y 47 de la Carta, la Decisión CPT no puede justificar la transferencia de esos datos a los Estados Unidos. En esas condiciones, el Sr. Schrems solicitó al Comisario que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc[57]. El caso llegó de nuevo ante el TJUE por una petición de decisión prejudicial planteada por el Alto Tribunal irlandés acerca de, entre otros, los siguientes puntos:

Si el Reglamento General de Protección de Datos[58] (en adelante, RGPD) se podía aplicar a las transferencias de datos personales entre operadores económicos establecidos en la Unión Europea a otros operadores económicos establecidos en terceros países basadas en las cláusulas tipo de protección recogidas en la Decisión 2010/87/UE, y el nivel de

---

[57] STJUE (Gran Sala), De 16 De Julio De 2020, Asunto C-311/18, *Data Protection Commisioner c. Facebook Ireland Ltd. y Maximillian Schrems*. (https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=9841532 Ap. 55).

[58] Hemos de mencionar que la Directiva 95/46/CE fue derogada en 2018 y sustituida por 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.

protección exigido en el Reglamento. Y que se señalaran cuáles eran las obligaciones que incumben a las autoridades de control en ese contexto.

Asimismo, el Alto Tribunal irlandés plantea la cuestión de la validez de la Decisión 2010/87/UE, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países[59], de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo; y de la Decisión sobre el Escudo de Privacidad.

Respecto de la primera cuestión, referente a la aplicabilidad del RGPD en las transferencias de datos personales entre operadores económicos domiciliados en la Unión Europea y un tercer país, respectivamente, basadas en las cláusulas tipo de protección recogidas en la Decisión 2010/87/UE y el nivel de protección exigido en el artículo 46, apartados 1 y 2, letra c) del RGPD, el TJUE entendió que, el RGPD «se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero» (artículo 2, apartado 1, del Reglamento). Esta cuestión incluye la transferencia de datos personales desde un Estado miembro de la Unión a un tercer país, tal y como se señala en el artículo 4 del Reglamento.

Si bien el RGPD prevé excepciones a su aplicación en el apartado 2 del artículo 2, el TJUE no considera que el caso presentado se pueda incluir en ninguna de ellas. De esta forma, estima que la transferencia de datos personales por parte de un operador económico domiciliado en la Unión Europea a otro operador económico domiciliado en un tercer país es una práctica que entra dentro del ámbito de aplicación del RGPD.

Por otra parte, del artículo 46, apartados 1 y 2, letra c) del Reglamento se desprende que cuando no existe una decisión de adecuación, el nivel de protección exigido puede proporcionarse mediante cláusulas tipo adoptadas por la Comisión, siempre que el tercer país extracomunitario avale las garantías adecuadas, permitiendo a los interesados contar con derechos y mecanismos legales de protección de estos. Entendiendo, por ello, que las

[59] López Guzmán, J. *Sentencia Schrems II: Localización de datos personales y su impacto en los servicios digitales. Revista Lex Mercatoria*. Vol. 17, 2021. Artículo 4. Pág. 32.

cláusulas tipo de protección gozan del mismo nivel de protección que el que proporciona el Reglamento dentro de la UE.

En la segunda cuestión prejudicial, el Tribunal Supremo irlandés solicita que el TJUE aclare si, en virtud del artículo 58, apartado 2, letras f) y j) del RGPD, las autoridades de control nacionales tienen el deber de suspender o prohibir una transferencia de datos personales a un tercer país cuando considera que no se respeta el nivel de protección adecuado, infringiendo así el Derecho de la Unión y de la Carta.

A la luz del mencionado precepto y de la Carta, el TJUE indica que las autoridades nacionales de control (en el caso de España, la AEPD)están dotadas de la competencia necesaria para comprobar que la transmisión de datos personales entre un Estado miembro y un tercer país respeta las exigencias del Reglamento. De las anteriores disposiciones se deriva que las autoridades de control tienen como misión principal controlar la aplicación del RGPD y velar por su cumplimiento[60]. En este contexto, el considerando 107 del RGPD dispone que, cuando «un tercer país, un territorio o sector específico en un tercer país […] ya no garantiza un nivel de protección de datos adecuado […], debe prohibirse la transferencia de datos personales a dicho tercer país […], salvo que se cumplan los requisitos [de dicho Reglamento] relativos a las transferencias basadas en garantías adecuadas»[61].

Por lo tanto, el TJUE concluye que, en caso de que no exista una decisión de adecuación que garantice que el tercer país cumple con el nivel adecuado de protección en la transferencia de datos personales, es la autoridad nacional de control quien debe compensar dicha transferencia con las garantías adecuadas para cumplir, de esta forma, con los requisitos de protección de datos y derechos de los interesados dentro de la Unión.

En cuanto a la cuestión acerca de la validez de la Decisión 2010/87/UE a la luz de los artículos 7, 8 y 47 de la Carta, el TJUE señala que dicha norma garantiza un nivel

---

[60] STJUE (Gran Sala), De 6 De Octubre De 2015, Asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd.* 2015). (https://eur-lex.europa.eu/legal-content/ES-EN/TXT/?from=en&uri=CELEX%3A62014CJ0362). Ap. 108.

[61] STJUE (Gran Sala), De 6 De Octubre De 2015, Asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd.* 2015). (https://eur-lex.europa.eu/legal-content/ES-EN/TXT/?from=en&uri=CELEX%3A62014CJ0362). Ap. 95

adecuado de protección de los datos personales transmitidos a países terceros. Si bien, las cláusulas contractuales tipo de protección (en adelante, CTP) pueden necesitar de garantías complementarias por parte del responsable del tratamiento, debido a su naturaleza contractual.

En caso de que la autoridad competente no pueda adoptar dichas medidas complementarias para garantizar el nivel adecuado de protección en el tratamiento de los datos por un tercer país, dicha autoridad deberá suspender o prohibir la transferencia con ese país. Esto es lo que ocurre en el caso de Estados Unidos, cuyas empresas se ven en la obligación de proporcionar datos personales de ciudadanos no residentes a las autoridades públicas para su vigilancia en virtud de la sección 702 de la FISA (Foreing Intelligence Surveillence Act)[62] y en la E.O. 12333[63] (Executive Order 12333 United States Intelligence Activities).

Sin embargo, ello no quiere decir que la adopción de CTP al amparo del RGPD o de la Decisión 2010/87/UE sean inválidas, sino que debemos centrarnos en que la adopción de estas y las posibles medidas complementarias, interpretadas a la luz de los artículos 7, 8 y 47 de la Carta, garanticen en la práctica el nivel de protección exigido por el Derecho de la Unión y así evitar la injerencia en los derechos de protección de datos por parte de terceros países.

Por último, el TJUE debe valorar la validez de la Decisión sobre el Escudo de Privacidad. Para ello, el Tribunal debe relacionar dicha Decisión con los artículos 7, 8 y 47 de la Carta, que recogen los siguientes derechos fundamentales, respectivamente: al respeto a la vida privada y familiar, de su domicilio y de sus comunicaciones; a la protección de datos de carácter personal; y a la tutela judicial efectiva y a un juez imparcial.

En el punto I.5 del Anexo II de la Decisión se prevé que se limiten los principios del marco normativo por «exigencias de seguridad nacional, interés público y cumplimiento

---

[62] La sección 702 de la FISA recoge los distintos procedimientos para la selección de determinadas personas fuera de Estados Unidos que no sean estadounidenses.

[63] Esta orden ejecutiva establece el marco de trabajo al cual deben ceñirse las agencias de inteligencia estadounidenses para proteger la privacidad y libertades civiles en sus actos de vigilancia. Fue aprobada por el presidente Ronald Reagan en 1981.

de la Ley». De esta forma, se establece una primacía en virtud de la cual las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias y se manifiesten, por tanto, incompatibles con ellas[64]. En consecuencia, pueden darse situaciones en las que se vulnere el principio de proporcionalidad en el alcance de esas injerencias, ya que no se ciñen a lo estrictamente necesario[65]. Este es el caso de los programas de vigilancia masiva llevados a cabo por los servicios de inteligencia estadounidenses, como la NSA o el FBI.

El Tribunal, en el apartado 168 y siguientes de la sentencia, pone en entredicho que el Derecho de Estados Unidos garantice efectivamente el nivel de protección adecuado exigido por el artículo 45 del RGPD, ya que este país no limita las injerencias de las autoridades públicas en el tratamiento de los datos personales y tampoco pone a disposición de los titulares de dichos datos mecanismos legales que garanticen la tutela judicial efectiva, tal y como proclama el artículo 47 de la Carta.

Asimismo, el TJUE declara que la figura del Defensor del Pueblo en el ámbito del Escudo de Privacidad no puede subsanar las lagunas que presenta la normativa estadounidense, puesto que el Defensor no puede relacionarse con los tribunales (apartados 194 a 197 de la sentencia).

De lo anterior se desprende que los Estados Unidos no garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a entidades establecidas en ese país tercero en el marco del Escudo de Privacidad UE-EEUU[66]. Por lo tanto, la Decisión sobre el Escudo de Privacidad se declara inválida por parte del Tribunal de Justicia de la Unión Europea.

---

[64] STJUE (Gran Sala), De 6 De Octubre De 2015, Asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd.* 2015). (https://eur-lex.europa.eu/legal-content/ES-EN/TXT/?from=en&uri=CELEX%3A62014CJ0362) Ap. 164

[65] De Miguel Asensio, P. *Implicaciones de la declaración de invalidez del Escudo de Privacidad, La Ley Unión Europea*, Número 84, septiembre 2020.

[66]STJUE (Gran Sala), De 6 De Octubre De 2015, Asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd.* 2015). (https://eur-lex.europa.eu/legal-content/ES-EN/TXT/?from=en&uri=CELEX%3A62014CJ0362). Apdo. 198

Es necesario señalar, a este respecto, que la invalidez de dicha Decisión no crea un vacío legal en cuanto a las transferencias internacionales de datos entre la Unión y Estados Unidos, ya que se aplica el artículo 49 del Reglamento General de Protección de Datos, que opera en ausencia de una decisión de adecuación.

4.3.1 Fallo y consecuencias

Tras la STJUE *Schrems II*, el Comité Europeo de Protección de Datos [67](European Data Protection Board o «EDPB») publicó, el 24 de julio de 2020, una serie de preguntas y respuestas referidas al caso que pretendían solventar cualquier duda que surgiera respecto de las transferencias transfronterizas de datos tras la invalidación de la Decisión sobre Escudo de Privacidad.

En su pregunta número cuatro se aborda la manera de proceder en las transferencias entre operadores europeos y estadounidenses cuando éstos últimos se encuentran adheridos al Escudo de Privacidad. En concreto, según el EDPB, dichas transferencias son ilegales con carácter general[68] y deberán emplearse otros mecanismos llevarlas a cabo. Estos otros mecanismos son las cláusulas tipo de protección de datos o las normas corporativas vinculantes[69] (NCV).

En la referida sentencia, la parte demandada plantea la opción de utilizar dichas cláusulas como medio para las transferencias internacionales (artículo 46, apartado 2, letra c), del RGPD), ya que el artículo 44 del mencionado Reglamento dispone que «todas las disposiciones [del capítulo V del Reglamento] se aplicarán a fin de asegurar que el nivel

---

[67] Comité Europeo de Protección de Datos: es un organismo europeo independiente que contribuye a la aplicación coherente de las normas de protección de datos en toda la Unión Europea y promueve la cooperación entre las autoridades de protección de datos de la UE. Su objetivo principal es garantizar la aplicación coherente del Reglamento General de Protección de Datos y la Directiva europea sobre protección de datos en el ámbito policial (https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_es).

[68] García Miró, T. G. (2020). *Identidad, cesión de datos personales y la decisión privacy shield tras la STJUE schrems II. InDret: Revista Para El Análisis Del Derecho. 2020 (.3) 22-22,* (3), 22.

[69] Normas corporativas vinculantes: el art. 4.20) RGPD define las NCV 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>>. Su contenido mínimo se encuentra en el art. 47.2 del RGPD.

de protección de las personas físicas garantizado por el Reglamento no se vea menoscabado». Cuestión que es ampliamente discutida por el TJUE (apdos. 92 a 102 de la sentencia), que aprecia el empleo de dichas cláusulas, tal y como establece el Reglamento, cuando las garantías adecuadas cumplan con el nivel adecuado de protección que debe estar presente en las transferencias de datos personales entre Estados miembros y terceros Estados que se llevan a cabo a través de estas. Siempre y cuando el nivel adecuado de protección sea sustancialmente equivalente al garantizado dentro de la Unión, interpretado a la luz de la Carta[70].

Esto implica que la autoridad nacional de control debe tener en cuenta tanto las estipulaciones contractuales acordadas entre los operadores, así como un eventual acceso de las autoridades públicas de ese país tercero a los datos personales transferidos y a las normas que se incluyen en el sistema jurídico de dicho país. Puesto que, como ya hemos mencionado anteriormente, está permitida la injerencia de las autoridades públicas en las transferencias internacionales de datos bajo el pretexto de la seguridad nacional, defensa y seguridad del Estado.

4.3.2 Reacciones del fallo a nivel mundial y a nivel europeo

Por un lado, el hecho de que el TJUE afirmase la declaración del Sr. Schrems sobre que EEUU no cumple con el nivel de garantía exigido por la normativa de la Unión respecto de la protección de datos de carácter personal, llevó a otros Estados a invalidar sus decisiones de adecuación, como es el caso de Suiza.

El 8 de septiembre de 2020, el Comisionado Federal de Protección de Datos de Suiza (Federal Data Protection and Information Commisioner o «FDPIC») publicó un informe en el que declaraba la invalidación del acuerdo de Privacy Shield entre Suiza y Estados Unidos en base a la STJUE *Schrems II*, tras lo cual modificó la lista de aquellos países que proporcionaban un nivel de protección adecuado en las transferencias de datos, eliminando a los Estados Unidos de dicha lista.

---

[70] STJUE (Gran Sala), De 6 De Octubre De 2015, Asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd.* 2015). (https://eur-lex.europa.eu/legal-content/ES-EN/TXT/?from=en&uri=CELEX%3A62014CJ0362) Apdo. 105.

Con esta decisión, Suiza se encuentra en la misma situación que Europa respecto de la normativa aplicable a estas transferencias, puesto que en el sistema jurídico suizo también existen las cláusulas contractuales tipo de protección, pero éstas no cumplen con el nivel adecuado de protección que se requiere a menos que se complementen con medidas de garantías (p.e. que las empresas evalúen caso por caso cada transferencia de datos con Estados Unidos). De esta forma, es imperante que las autoridades suizas y estadounidenses se pongan de acuerdo a la hora de redactar una nueva decisión de adecuación que asegure el nivel de protección pertinente, ya que el intercambio de datos entre ambos países es una fuente económica en constante crecimiento dentro del sector comercial.

Asimismo, las agencias de protección de datos de países como Alemania, Irlanda y Finlandia se han enfocado en la necesidad de proteger los derechos fundamentales de sus ciudadanos. Para ello han cambiado las cláusulas de privacidad existentes en los contratos de transferencias internacionales de datos, verificando que se cumplen las exigencias del RGPD.

También considero que es necesario comentar brevemente el acuerdo de protección de datos entre Reino Unido y Europa tras el Brexit y el alcance extraterritorial del RGPD en este sentido. Esto es muy significativo si se considera que el 75% de los flujos de datos internacionales del Reino Unido son con la UE, y gran parte de la actividad económica del Reino Unido depende de estos flujos[71].

El RGPD permite las transferencias de datos personales entre miembros del Espacio Económico Europeo y con terceros países, siempre que se cumplan las garantías adecuadas de protección de datos. Durante el periodo de transición, las empresas del Reino Unido trataran datos de ciudadanos europeos debían seguir dos normativas: el RGPD y la Ley de Protección de Datos de 2018 (Data Protection Act o «DPA»). Esta última norma fue modificada en 2019 por el Reglamento de Protección de Datos,

[71] Gascón Marcén, A. (2020). *La regulación del flujo de datos personales entre la unión europea y el reino unido tras el brexit*. *Cuadernos De Derecho Transnacional (Marzo 2020), Vol.12, no 1, Pp 231-246 ISSN 1989-4570, 12*(1), 231-246.

Privacidad y Comunicaciones Electrónicas, que pasó a conocerse como «UK-GDPR» y vino a integrar las exigencias del Reglamento europeo.

Finalmente, el 28 de julio de 2021, la Comisión Europea adoptó sendas decisiones de adecuación para el Reino Unido: la Decisión relativa a la celebración del Acuerdo de Comercio y Cooperación entre la UE y el Reino Unido y del Acuerdo de Seguridad de la Información. Su consecuencia inmediatas es la libre circulación de datos entre Europa y el Reino Unido. Aunque es necesario destacar que dichas Decisiones cuentan con un plazo de vigencia de cuatro años, siendo prorrogables.

Por otra parte, la sentencia Schrems II puso de manifiesto la dificultad, e incluso, imposibilidad de acceso por parte de los ciudadanos europeos a la vía judicial estadounidense para reclamar los daños ocasionados por la injerencia del Gobierno en su privacidad. De ahí que, durante Administración Obama, el Congreso de Estados Unidos aprobara, el 10 de febrero de 2016, la "Judicial Redress Act", que es una Ley que permite a los ciudadanos no estadounidenses ciertos derechos en virtud de la Ley sobre protección de la Privacidad de 1974, entre los que se incluye la posibilidad de emplear la acción judicial contra ciertos actos gubernamentales. Pero sólo a los ciudadanos de aquellos países que permitan la transferencia transfronteriza de datos con fines comerciales y que no impongan políticas de transferencia de datos que obstaculicen materialmente los intereses de seguridad de EEUU[72].

5. CONCLUSIONES

En primer lugar, considero que a lo largo del trabajo ha quedado patente que, en lo que respecta a la protección de datos de carácter personal, las desavenencias que encontramos en la legislación de los Estados que intervienen en las transferencias de los mismos, implican una diferencia sustancial en la protección del derecho fundamental a la intimidad y a la privacidad de los titulares de dichos datos.

En este sentido, considero que el hecho de que las autoridades estadounidenses hayan justificado sus prácticas de vigilancia masiva basándose en motivos de seguridad nacional

[72] Andrews Kurth, H. (2016, 12 de febrero de 2016). *Congress Passes Judicial Redress Act*. Message posted to https://www.huntonprivacyblog.com/2016/02/12/congress-passes-judicial-redress-act/

-en ataques terroristas perpetrados en el pasado en suelo estadounidense- no es motivo suficiente para la injerencia indiscriminada de sus administraciones y servicios de inteligencia en los derechos fundamentales anteriormente mencionados. También se han dado ataques terroristas en países europeos y no por ello nuestras instituciones han supeditado la protección de la intimidad, los datos personales y la privacidad a la seguridad de los Estados.

De hecho, la Comisión Europea ha presentado este año 2022, como iniciativa legislativa, una nueva "Ley de Datos" que pretende complementar el RGPD. En concreto, se trata de la Propuesta de Reglamento sobre normas armonizadas para un acceso justo a los datos y su utilización[73]. Con esta nueva norma se pretenden resolver los problemas relacionados con el retorno de los datos cedidos a empresas mediante Internet, buscar el equilibrio entre los titulares y los usuarios de los datos, resolver la insuficiencia de potestades públicas de acceso a los datos en situaciones excepcionales, etc.[74]. Con ello se pone de manifiesto que el nivel adecuado de protección de los datos de carácter personal que exige la Unión Europea es superior al que exigen los Estados Unidos, buscándose en el contexto europeo proteger de manera más precisa a los titulares de dichos datos cuando éstos se transfieren a terceros países por el uso o servicio de productos.

Es más, en reciente jurisprudencia del TJUE, C-140/20 (Commissioner of An Garda Síochána y otros)[75], el Alto Tribunal europeo ha reafirmado su doctrina respecto de la conservación preventiva e indiscriminada de datos de tráfico y localización de comunicaciones electrónicas[76]: reiterando que es necesario ponderar los intereses jurídicos en juego, a saber, el respeto a la vida privada y a la protección de los datos

---

[73] De Miguel Asensio, P. *La futura Ley de Datos (I): objeto, contenido y ámbito de aplicación*.

[74] Aparicio, J. & Vidal, M. *¿Qué implica la nueva Ley de Datos?*

[75] STJUE (Gran Sala) de 5 de abril de 2022, asunto C-140/20, *G.D c. Commissioner of An Garda Síochána y otros*.

[76] Rodríguez Lainz, J.L. *La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G.D. y Commissioner An Garda Síochána*.

personales frente a la intrusión que suponen la conservación de datos de tráfico y su localización con fines de seguridad nacional.

Recordemos que el artículo 15.1 de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas supone una excepción a la prohibición que recoge el artículo 5.1 de la misma, ya que recoge una serie de circunstancias exhaustivas por las cual es legítima la conservación de los datos de carácter personal y las comunicaciones electrónicas por parte de las autoridades nacionales. Pues bien, el TJUE reitera que, si bien es cierto que el artículo 52, apartado 1, de la CDFUE admite limitaciones al ejercicio de los derechos fundamentales recogidos en los artículos 4, 7 y 8 de la misma, siempre que estén basadas en una ley y se respete su contenido esencial; la normativa nacional debe responder en todo caso a criterios objetivos y, asimismo, ha de existir una relación entre los datos que deban conservarse y el objetivo que se pretende lograr (Apdo. 55 de la STJUE 258/22). Con ello se permite a los proveedores de servicios de comunicaciones electrónicas la conservación de datos de tráfico y de localización, en situaciones en las que el Estado miembro en cuestión se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible (Apdo. 58 de la STJUE 258/22).

El TJUE establece en el apartado 105 de la mencionada sentencia que conceder un acceso general a datos de carácter personal a las autoridades nacionales no puede considerarse limitado a lo estrictamente necesario, por lo que deben existir criterios objetivos y requisitos conforme a los cuales se les conceda acceso a los mismos. Sólo será posible conceder un acceso a este tipo de datos con el objetivo de luchar contra la delincuencia o el terrorismo, siempre y cuando sean los datos de las personas sospechosas de planear, cometer o haber cometido un delito grave. Por lo que no pueden conservarse los datos personales de todas aquellas personas que no representan una amenaza para la seguridad pública o nacional del Estado miembro de que se trate (apdo. 88 de la STJUE 258/22).

En segundo lugar, vivimos en la Era de la Información, donde una herramienta primordial para la comunicación entre millones de personas y la expansión de los mercados se lleva a cabo mediante el Internet de las cosas, consiguiendo que los datos personales se hayan convertido en el petróleo de la era digital[77]. Por lo tanto, si nuestros datos más sensibles

[77] Almajano, C. *El dato, el activo más estratégico de las organizaciones*.

son una moneda de cambio para las empresas estadounidenses, es necesario que se tomen medidas que aseguren la protección de los mismos, empezando por garantizar que el consentimiento del titular de los datos para su uso y conservación es respetado por las organizaciones y autoridades nacionales.

En definitiva, si las empresas estadounidenses quieren seguir enriqueciéndose a base de los datos de los ciudadanos europeos, su legislación debe blindar los derechos fundamentales a la privacidad, la intimidad y la protección de los datos de carácter personal respecto de cualquier tipo de intrusión gubernamental.

Esperemos que con el futuro acuerdo transatlántico que regulará las transferencias internacionales de datos entre la Unión Europea y Estados Unidos se termine de una vez por todas con la trascendente asimetría que existe entre ambas legislaciones, y que se subsanen de esta forma los errores cometidos por los dos anteriores intentos (los acuerdos de Safe Harbour y Privacy Shield).

6. BIBLIOGRAFÍA

CAPÍTULO DE LIBRO

Chicharro Lázaro, A. (2016). *La trascendencia práctica del caso facebook en relación con la transferencia masiva de datos personales desde la unión europea a estados unidos*. In Sociedad Latina de Comunicación Social (Ed.), *La pantalla insomne* [Practical Implication of Facebook Ruling on the large-scale Personal Data Transfer from the EU to the USA] (2ª Ed ed., pp. 1782-1809). España: Cuadernos artesanos comunicación, 103.

Rodriguez Pineau, E., & Torralba Mendiola, E. (2022). *Transferencia de datos personales fuera del EEE en el nuevo marco del reglamento general: Especial referencia al caso estadounidense y el reino unido tras el brexit*. *La protección de las transmisiones de datos transfronterizas* (1ª Ed. ed., pp. 1-412). Pamplona, Navarra: Aranzadi.

ARTÍCULO DE REVISTA ACADÉMICA (JOURNAL)

Álvarez Caro, M. y Recio Gayo,M. (2015). *Hacia un acuerdo safe harbour renovado para la transferencia internacional de datos entre EEUU y la UE. Papeles De Derecho Europeo e Integración Regional, iDeir nº 25*.

Almajano, C. (2018, 23 de junio de 2018). *El dato, el activo más estratégico de las organizaciones.* Computerworld España. Disponible en: https://www.computerworld.es/negocio/el-dato-el-activo-mas-estrategico-de-las-organizaciones

Baumohl, Chris, *Piercing the Veil: Reconciling FISA and the State Secrets Privilege in the Schrems II Era* (November 2, 2021). Comment, Piercing the Veil: Reconciling FISA and the State Secrets Privilege in the Schrems II Era 71 Am. U. L. Rev. 235 (2021), Available at SSRN: https://ssrn.com/abstract=3938362

Bowden, C. (2013). *The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights*. Brussels: European Parliament - Directorate-General for Internal Policies.

Cole, D. (2014). *The Three Leakers and what to do about them. The New York Review of Books* [En línea], 6 de febrero. Vol. 61(2). Disponible en:

http://www.nybooks.com/articles/2014/02/06/three-leakers-and-what-do-about-them/

Darcy, S., 2015. *Battling for the Rights to Privacy and Data Protection in the Irish Courts*. *Utrecht Journal of International and European Law*, 31(80), pp.131–136. DOI: http://doi.org/10.5334/ujiel.cv

De Miguel Asensio, P. *Aspectos internacionales de la protección de datos: Las sentencias schrems y weltimmo del tribunal de justicia*. *La Ley Europea, no. 31, 2015, Pp.1-10.*

Díaz Díaz, E. (2016). *El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*. *Revista Aranzadi Doctrinal*. (6), 155-190.

García Miró, T. G. (2020). *Identidad, cesión de datos personales y la decisión privacy shield tras la STJUE schrems II*. *InDret: Revista Para El Análisis Del Derecho. 2020 (.3) 22-22,* (3), 22.

Gascón Marcén, A. (2020). *La regulación del flujo de datos personales entre la unión europea y el reino unido tras el brexit*. *Cuadernos De Derecho Transnacional (Marzo 2020), Vol.12, no 1, Pp 231-246 ISSN 1989-4570, 12*(1), 231-246.

Gonzalo Domenech, J. J. *Las decisiones de adecuación en el derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros*. *Cuadernos De Derecho Transnacional (Marzo 2019), Vol.11, no 1, Pp 350-371 ISSN 1989-4570, Vol. 11*(No. 1), 350-371.

Fabbrini, F. (2015). *Human Rights in the Digital Age: The European Court of Human Rights in the Data Retention Case and its Lessons for Privacy and Surveillance in the United States. Human Rights in the Digital Age*. (28), 65-95.

López Guzmán, J. (2021). *Sentencia Schrems II: Localización de datos personales y su impacto en los servicios digitales. Revista Lex Mercatoria, Vol. 17* (Artículo 4), 32.

Milanovic, M. (2015). *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. Harvard International Law Journal*. Winter, 56(1), 81-146.

Ojanen, T. *Making the essence of fundamental rights real: The court of justice of the european union clarifies the structure of fundamental rights under the charter: ECJ 6 october 2015, case C-362/14, maximillian schrems v data protection commissioner*. *European Constitutional Law Review; Sep 2016; 12; 2; p318-p329,*

Ortega Giménez, A. y Gonzalo Domenech, J. J. (2018). *Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea*. *Revista de la Facultad de Derecho*, 44, 1-35 (http://dx.doi.org/10.22187/rfd2018n44a2).

Puerto, M.I y Sferrazza Taibi, P. (2018). *La sentencia Schrems del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional*. *Revista Derecho Del Estado, nº40,* Universidad Externado de Colombia (enero-junio de 2018), pp. 209-236. DOI: https://doi.org/10.18601/01229893.n40.09

Recio Gayo, M. (2019). *Nivel adecuado para transferencias internacionales de datos*. [Adequate Level of International Data Transfers] *Revista De La Facultad De Derecho Universidad CEU San Pablo (Brasil), nº83*(diciembre-mayo), 207-240.

Terpan, F. *EU-US data transfer from safe harbour to privacy shield: Back to square one?*. *European Papers: A Journal on Law and Integration, ISSN-e 2499-8249, Vol. 3, Nº. 3, 2018, Págs. 1045-1059.*

Tihomir Katulić, Ph.D., Goran Vojković, Ph.D. *From safe harbour to european data protection reform*. *MIPRO 2016, may 30 - June 3, 2016, Opatija, Croatia.*

Tracol, X. (2016). *"Invalidator" Strikes Back: the Harbor has Never Been Safe*. *Computer Law & Security Review*. 32(2), 345-362.

Uría Gavilán, E. (2016). *Derechos fundamentales versus vigilancia masiva*. *Revista de Derecho Comunitario Europeo*, 53, 261-282. Doi: http://dx.doi.org/10.18042/cepc/rdce.53.07

Voss, W. G. (2016). *European Union Data Privacy Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*. *Business Layer*, 72(1), 221-234.

TESIS DOCTORAL

Kahansky, R., Marcela, C. (2019). *Vigencia del Derecho europeo de protección de datos personales.*

ARTÍCULO DE PERIÓDICO

Pinto, T. (2019, 09 de octubre de 2019). *El legado de Snowden: las filtraciones que transformaron internet*. *El País.*

Terán Haughey, M. (2022, 28 de marzo de 2022). *Nuevo acuerdo entre europa y estados unidos por la transmisión y protección de datos*. *El Economista.Es.*

FORO DE DISCUSIÓN EN LÍNEA

Andrews Kurth, H. (2016, 12 de febrero de 2016). *Congress Passes Judicial Redress Act*. Message posted to https://www.huntonprivacyblog.com/2016/02/12/congress-passes-judicial-redress-act/

Aparicio, J. & Vidal, M. (2022, 6 de abril de 2022). *¿Qué implica la nueva Ley de Datos?* Message posted to https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/que-implica-la-nueva-ley-de-datos-2022-04-06/

De Miguel Asensio, P. (2017, 24 de noviembre de 2017). *Demandas internacionales contra redes sociales: El concepto de consumidor y la evolución de la legislación sobre datos personales*. Message posted to https://pedrodemiguelasensio.blogspot.com/2017/11/demandas-internacionales-contra-redes.html

De Miguel Asensio, P. (2018, 21 de diciembre de 2018). *Reglamento (UE) 2018/1807 sobre libre circulación de datos no personales*. Message posted to https://pedrodemiguelasensio.blogspot.com/2018/12/reglamento-ue-20181807-sobre-libre.html

De Miguel Asensio, P. (2021, 30 de noviembre de 2021). *Directrices sobre el concepto de transferencia internacional de datos personales y su interpretación con el ámbito de aplicación territorial del RGPD*. Message posted to

https://pedrodemiguelasensio.blogspot.com/2021/11/directrices-sobre-el-concepto-de.html

De Miguel Asensio, P. (2022, 12 de mayo de 2022). *La futura Ley de Datos (I): objeto, contenido y ámbito de aplicación*. Message posted to https://pedrodemiguelasensio.blogspot.com/2022/05/la-futura-ley-de-datos-i-objeto.html

Peers, S. (2015, 7 de octubre de 2015). *The Party's Over: EU Data Protection Law after the Schrems Safe Harbor Judgment*. *EU Law Analysis*. Disponible en: http://eulawanalysis.blogspot.com/2015/10/the-partys-over-eu-data-protection-law.html

Rodríguez Lainz, J.L. (2022, 28 de abril de 2022). *La evolución de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de conservación indiscriminada de datos de comunicaciones electrónicas en la STJUE del Caso G.D y Commissioner An Garda Síochána*. Diario La Ley, nº 10058, Sección Tribuna. Wolters Kluwer. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmNTI2MDI7Wy1KLizPw8WyMDIyMDE0NLtbz8lNQQF2fb0ryU1LTMvNQUkJLMtEqX_OSQyoJU27TEnOJUtdSk_PxsFJPiYSYAAGi40aZjAAAAWKE

PÁGINAS WEB

Agencia Española de Protección de Datos. *Guía acerca del escudo de privacidad UE-EEUU.* Disponible en: .https://www.aepd.es/sites/default/files/2019-09/guia-acerca-del-escudo-de-privacidad.pdf

Asociación profesional de consultores de protección de datos. (2016). *Qué es y quiénes forman parte del trabajo del artículo 29.* Disponible en: https://www.apcpd.es/que-es-y-quienes-forman-el-grupo-de-trabajo-del-articulo-29/

Comité Europeo de Protección de Datos. *Quiénes somos.* Disponible en: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_es

Transferencia internacional de datos (Protección de Datos). Guías Jurídicas Wolter Kluwer. Disponible en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjEwNjE7Wy1KLizPw8WyMDQwsDU0OwQGZapUt-ckhlQaptWmJOcSoA6fqAajUAAAA=WKE

Falchetta, T. (2016). How to Bridge the Gap? Corporate and Government Surveillance Examined at the UN. ejil*: Talk!*. Disponible en: https://www.ejiltalk.org/how-to-bridge-the-gap-corporate-and-government-surveillance-examined-at-the-un/

JURISPRUDENCIA

Conclusiones del Abogado General Sr. Y. Bot, presentadas el 23 de septiembre de 2015. *Maximillian Schrems c. Data Protection Commissioner*. Petición de decisión prejudicial planteada por la High Court of Ireland. Disponible en: https://curia.europa.eu/juris/document/document.jsf?docid=168421&doclang=ES

Conclusiones Del Abogado General Sr. M. Bobek, presentadas el 14 de noviembre de 2017. *Maximillian Schrems c. Facebook Ireland Ltd*. Petición de decisión prejudicial planteada por el Oberster Gerichtshof. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62016CC0498&from=EN

Informe explicativo del protocolo que modifica el convenio para la protección de las personas con respecto al procesamiento automático de datos personales, p.17 apdo. 102.

Recopilación de la Jurisprudencia de la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14, *Maximilian Schrems vs. Data Protection Commissioner*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62014CJ0362&from=LT

Sentencia de 20 de Enero de 2005, asunto C-464/01, *Gruber*. Apartado 39, Sobre Los Artículos 13 a 15 Del Convenio De Bruselas.

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

STJUE (Gran Sala), de 6 de octubre de 2015, asunto C-326/14, *Maximillian Schrems c. Facebook Ireland Ltd*. 2015).

STJUE (Gran Sala), de 16 de Julio de 2020, asunto C-311/18, *Data Protection Commisioner c. Facebook Ireland Ltd. y Maximillian Schrems*.

STJUE (Gran Sala) de 5 de abril de 2022, asunto C-140/20, *G.D c. Commissioner of An Garda Síochána y otros*.

LEGISLACIÓN

Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (2000/520/CE).

Decisión de la Comisión, de 5 de febrero de 2010 , relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

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-EEUU.

Decisión de Ejecución (UE) 2016/2297 de la Comisión, 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.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050).

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Reglamento (CE) nº 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia Civil y Mercantil. Núm 12.1 (2000).

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