Universidad de Valladolid

Facultad de Derecho

Grado en DADE

Sentencia del Tribunal de Justicia de la Unión Europea de 16 de Julio de 2020 (Asunto C-311/18)

Presentado por:
Celia Pascual Cabrito

Tutelado por:
Antonio Adrián Arnaiz

Valladolid, 21 de julio de 2020

RESUMEN:

La finalidad de este trabajo consiste en analizar la sentencia del TJUE de 16 de julio de 2020 (en adelante Schrems II) como presupuesto para entender cuál son las razones que llevaron al Tribunal de Justicia de la Unión Europea a invalidar la Decisión 2016/1250 de la Comisión (*Privacy Shield*), cuál son las consecuencias de este dictamen y, cuál es la situación actual en relación con la protección de datos personales en las transferencias internacionales. La sentencia Schrems II surge como consecuencia de una resolución previa del Tribunal de Justicia de la Unión Europea igual de relevante, la sentencia de 6 de octubre de 2015 (en adelante Schrems I), la cual tuvo como resultado la declaración de invalidez de la Decisión 2000/52 de la Comisión, comúnmente denominada *Safe Harbor*. Tanto el *Privacy Shield* como el *Safe Harbor* no cumplían con los estándares de protección adecuados, es decir, no ofrecían un nivel de protección equivalente al de la Unión Europea. Actualmente no se ha aprobado ninguna otra ley que sustituya a las dos anteriores, pero contamos con el Reglamento General de Protección de Datos como base jurídico para las transferencias de datos de la Unión Europea a países terceros.

PALABRAS CLAVE: Scherms II**,** invalidez, Privacy Shield, Safe Harbor.

ABSTRACT:

The purpose of this work is to analyze the Schrems II judgment as a presupposition to understand what are the reasons that led the Court of Justice of the European Union to invalidate Commission Decision 2016/1250 (*Privacy Shield*), what are the consequences of this judgment and, what is the current situation in relation to the protection of personal data. The judgment of July 16, 2020 (Schrems II) arises as a consequence of a previous resolution of the Court of Justice of the European Union that is equally relevant, the judgment of October 6, 2015, also called Schrems I, which resulted in the declaration of invalidity of Commission Decision 2000/52, commonly referred to as Safe Harbor. Both the Privacy Shield and the Safe Harbor did not meet adequate protection standards, that is, they did not offer a level of protection equivalent to that of the European Union. Currently no other law has been approved to replace the previous two, but we have the General Data Protection Regulation as the legal basis for data transfers from the European Union to third countries.

KEY WORDS: Schrems II, invalidity, Privacy Shield, Safe Harbor.

ÍNDICE DE ABREVIATURAS

AEPD Agencia Española de Protección de Datos.

Carta Carta de Derechos Fundamentales de la Unión Europea. (2000/C 364/01).

Decisión CPT Decisión 2010/87, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento[1] establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.
→ Actualmente las cláusulas contractuales tipo se regulan en la Decisión de Ejecución (UE) 2021/914 de 4 de junio de 2021 de conformidad con el Reglamento (UE) 2016/679 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 datos personales y a la libre circulación de estos datos.
→ Derogada el 25 de mayo de 2018 por el Reglamento (UE) 2016/679.

EEE Espacio Económico Europeo.

EE. UU. Estados Unidos.

High Court (of Ireland) Tribunal Superior de Irlanda.

Privacy Shield/Escudo de Privacidad 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.

RGPD Reglamento General de Protección de Datos. Reglamento de la Unión Europea 2016/679 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.

[1] "El encargado del tratamiento es la persona física o jurídica, autoridad, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de este." (AEPD, 2018)

Safe Harbor/Puerto Seguro Decisión 2000/520 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.

Schrems I Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, asunto C-326/14.

Schrems II Sentencia del Tribunal de Justicia de la Unión Europea de 16 de julio de 2020 (asunto C-311/18).

SEPD Supervisor Europeo de Protección de Datos.

STJUE Sentencia del Tribunal de Justicia de la Unión Europea.

TJUE Tribunal de Justicia de la Unión Europea.

TUE Tratado de la Unión Europea, de 7 de febrero de 1992.

UE Unión Europea.

ÍNDICE

1. INTRODUCCIÓN

La situación económica y social de los países se ha visto influida por los avances tecnológicos introducidos por la globalización, algo que también ha tenido repercusión a nivel jurídico. Todos los ámbitos de una sociedad se han tenido que adaptar a los nuevos métodos utilizados para relacionarse, tanto en el medio social como en el profesional. Por ejemplo, las formas de contratación son cada vez mas dependientes de internet, las empresas y los consumidores forman parte de una sociedad digitalizada, usuaria de los servicios electrónicos en su vida cotidiana. Esto también se observa en los acuerdos comerciales, los cuales se realizan mayoritariamente de manera electrónica en la actualidad, incluyendo transferencias de datos, debido a que son parte necesaria de la relación contractual para que las empresas puedan iniciar y completar una transacción. Además, son útiles, ya que permiten a las empresas almacenar datos de los clientes y adaptarse mejor a sus necesidades en relaciones futuras, es decir, les permite ser cada vez más eficientes y productivos. Al mismo tiempo, desde otro punto de vista totalmente opuesto, la digitalización puede suponer la violación de derechos fundamentales de los ciudadanos cuyos datos personales han sido transferidos si no se toman las precauciones adecuadas. Todo ello deriva en la necesidad de que las autoridades nacionales se encarguen de asegurar una protección adecuada en las transferencias de datos a través de una regulación completa y de garantía, algo que no ocurría con el *Safe Harbor*[2] y el *Privacy Shield*[3].

La sentencia del Tribunal de Justicia de la Unión Europea (en adelante TJUE), de 16 de Julio de 2020, asunto C-311/18 (en adelante Schrems II), que tiene por objeto un procedimiento prejudicial planteado por el Tribunal Superior de Irlanda (en adelante High Court) referente a la protección de las personas físicas en relación con el tratamiento de datos personales, es una de las sentencias más destacadas dentro del ámbito europeo en relación con la protección de datos personales. A raíz de esta sentencia se examinó la disparidad existente entre la normativa europea de protección de datos (recogida en el *Safe Harbor* y posteriormente el *Privacy Shield)* dentro de la Unión Europea y la normativa de Estados Unidos referente a la protección ofrecida a los ciudadanos de un país tercero en las transmisiones de datos. Se comprobó que la legislación del país americano en relación con la seguridad nacional no brindaba las garantías convenientes a los ciudadanos europeos, por lo que, mediante la sentencia Schrems II quedó invalidada el *Privacy Shield.*

[2] Decisión 2000/520/CE.
[3] Decisión 2016/1250 de la Comisión.

El *Privacy Shield* era el marco jurídico usado por las empresas instauradas en la Unión Europea, que, como parte de su actividad empresarial, transferían datos personales desde sus filiales europeas hasta las empresas matrices establecidas en Estado Unidos. Este *Escudo de Privacidad* adoptado en 2016 suponía la garantía y protección de los datos personales de los ciudadanos europeos, pero, el TJUE dictaminó que era inválido como marco legal de protección de datos personales en las transferencias de datos entre la Unión Europea y un país tercero.
Esta resolución llama la atención debido a que el *Privacy Shield* había sido aprobado solamente cuatro años antes, en 2016, después de que la Decisión 2000/520, o también denominada *Safe Harbor* fuese considerada inválida mediante la sentencia del TJUE, de 6 de octubre de 2015, asunto C-326/14 (en adelante Schrems I). Todo esto nos lleva a una situación de incertidumbre e inseguridad jurídica en relación con la protección de datos personales, ya que actualmente hay numerosas empresas establecidas en la Unión Europea que transfieren datos a compañías estadounidenses sin el amparo de una regulación como la que ofrecía el *Privacy Shield*, o anteriormente, el *Safe Harbor*.

Para entender mejor este asunto comenzaremos con un análisis de la Sentencia del TJUE de 16 de Julio de 2020, tanto los antecedentes, como el desarrollo y las consecuencias. Posteriormente explicaremos qué se entiende por transferencia internacional de datos, cuál es su nivel de protección dentro del Espacio Económico Europeo (en adelante EEE) a través del Reglamento de la Unión Europea 2016/679 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 (en adelante RGPD), y, también, cuál era su protección trasnacional recogida en primer lugar en el *Safe Harbor*, y posteriormente, el *Privacy Shield*. Por otro lado, explicar cuál es el alcance y la validez de las Cláusulas Contractuales Tipo y las Normas Corporativas Vinculantes como medio de protección de las transferencias de datos personales transnacionales, las cuales son aplicadas en acuerdos entre exportadores e importadores de datos.
Se hará un análisis de estas cuestiones con el objetivo de conocer las garantías en la protección de datos personales cuando son transferidos desde una empresa situada en la Unión Europea hasta una empresa situada en un país tercero.

2. SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UE DE 16 DE JULIO DE 2020 (ASUNTO C-311/18)

2.1 Antecedentes

2.1.1 Hechos que dieron lugar al litigio entre Maximilian Schrems y Facebook Inc.

En 2013, Edward Snowden, un trabajador de la Agencia de Seguridad Nacional de Estados Unidos publicó un libro en el cual exponía numerosas pruebas demostrando la escasa seguridad que existía en la transferencia de datos internacional. Snowden reveló que no había privacidad en las comunicaciones, debido a que el gobierno de Estados Unidos controlaba todos los datos, tenía vigilados e interceptados los medios de comunicación, incluyendo teléfonos, *routers*, o antenas de telefonía, es decir, todos los datos que se movieran en las empresas de telecomunicación más importantes del país.

Esto era posible puesto que la mayoría de las páginas web no estaban cifradas[4], lo que permitía a las empresas acceder fácilmente a todos los datos que compartían los usuarios dentro de esas páginas web, incluyendo información personal y bancaria.

Los usuarios de todo el mundo comenzaron a exigir unas nuevas condiciones y garantías en sus comunicaciones al sentirse desprotegidos tras conocer esta información. Entre esos usuarios se encontraba Maximilian Shrems, un jurista de origen austriaco que, como consecuencia de las filtraciones realizadas por Snowden decidió presentar una demanda ante la High Court contra Facebook Ireland, la filial que tiene Facebook Inc. en Irlanda, al observar que los datos personales que se transferían entre la filial y la empresa matriz situada en Estados Unidos no estaban suficientemente protegidos. El ordenamiento jurídico estadounidense permitía que esos datos fueran manipulados por las autoridades a través de la Agencia de Seguridad Nacional de Estados Unidos. A pesar de ello, la High Court dictó sentencia en 2014 desestimando la petición del Maximilian Shrems y dictaminando que sí existen garantías suficientes en la transferencia de datos personales entre las dos sociedades[5], las cuales, están recogidas en la Decisión 2000/52 de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo[6].

---

[4] "El cifrado de una página web es el proceso de codificación o encriptación de datos para que sólo pueda leerlo alguien con los medios para devolverlo a su estado original." (Internet Society, n.d.)

[5] Facebook Ireland y Facebook Inc.

[6] Decisión 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.

En esta Decisión denominada "Puerto Seguro" o *Safe Harbor* se establecían los límites impuestos a las empresas que transferían datos personales entre distintos países, se les exigía un nivel de protección y de información adecuado. Esto significaba que las empresas debían explicar cuál eran sus pretensiones en relación con los datos, es decir, el uso que darían a los datos, y, además, debían consultar a los usuarios si daban su consentimiento para que se operara con sus datos.

Según lo explicado hasta ahora, se entiende que el *Safe Harbor* garantizaba un nivel de protección adecuado en la transferencia de datos, y además se presuponía que las leyes de Estados Unidos también garantizaban la protección adecuada, pero existían dudas sobre las competencias de las autoridades del país tercero. Por esa razón, la High Court plantó una cuestión prejudicial al TJUE, consultando la capacidad que tiene una autoridad nacional de control[7] para detener una transferencia de datos sobre la que se ha interpuesto una denuncia alegando falta de protección en la transmisión. Al mismo tiempo, en el mismo litigio, se cuestiona la propia validez de la Decisión 2000/520/CE de la Comisión, con arreglo a la Directiva 95/46, que será examinada por el TJUE.

2.1.2 La sentencia del TJUE de 6 de octubre de 2015, asunto C-362/14.

La cuestión prejudicial planteada al TJUE tenía por objeto: "la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea[8], de los artículos 25, apartado 6, y 28 de 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, así como, en sustancia,

---

[8] Carta de los Derechos Fundamentales de la Unión Europea. (2000/C 364/01).

Artículo 7. Respeto de la vida privada y familiar.
Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
Artículo 8. Protección de datos de carácter personal.
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.
Artículo 47
Derecho a la tutela judicial efectiva y a un juez imparcial
Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo.
Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar.
Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia.

la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, 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"[9] dentro del litigio comenzado en 2013 entre el jurista Maximilian Schrems y el Data Protection Commissioner.

Siguiendo este planteamiento, habría que analizar primero el artículo 25 de la Directiva 95/46/CE para conocer qué se entiende por "nivel de protección adecuado", y posteriormente, conocer los límites de las autoridades nacionales de control.

En primer lugar, debemos acudir al artículo 25, apartado 6 de la Directiva 95/46/CE, el cual establecía que: "La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas."[10] De acuerdo con este artículo, para saber cuando se da ese "nivel de protección adecuado" debemos acudir al artículo 25.2 de la Directiva 95/46/CE: "El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países"[11]. Este artículo no especifica cuando se da efectivamente "el nivel de protección adecuado", sino que se evaluará caso por caso atendiendo a la protección de la vida privada y de las libertades o de los derechos fundamentales de las personas.

[9] STJUE de 6 de octubre de 2015, C-362/14, *Maximilian Schrems,* §1.

[10] Unión Europea. Directiva (CE) 95/46/CE de la Comisión Europea, 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.

[11] Unión Europea. Directiva (CE) 95/46/CE de la Comisión Europea, 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.

El TJUE soluciona este problema exponiendo que cuando se habla de "nivel de protección adecuado" garantizado por los países terceros, debemos entender un nivel de protección de las libertades y derechos fundamentales semejante al establecido dentro de la UE conforme a la Directiva 95/46.

No se exige la utilización de los mismos medios de protección usados por la UE, sino aquellos que permitan llegar a garantizar los derechos de los ciudadanos de la misma manera. Por lo tanto, para aquellos países en los que se garantice un nivel de protección adecuado en la transmisión de datos personales, el TJUE establece que las autoridades nacionales de control, de acuerdo con la Carta de los Derechos Fundamentales y la Directiva 95/46/CE, tienen plenas facultades para controlar si las transferencias de datos personales cumplen con lo dispuesto en la Directiva 95/46/CE. Pero, en caso de haber llegado a la autoridad nacional de control una solicitud de declaración de invalidez de una decisión de la Comisión, la autoridad nacional de control deberá plantear la cuestión ante los órganos jurisdiccionales nacionales.

Serán los tribunales nacionales quienes decidan si existen dudas sobre la validez de la decisión de la Comisión, y en caso afirmativo, se planteará una cuestión prejudicial ante el TJUE, ya que es que es el órgano que cuenta con la competencia exclusiva para declarar la invalidez de una decisión de la Comisión, u otro tipo de normativa legal europea.

A continuación, el TJUE analiza la validez de la Decisión 2000/520/CE de la Comisión. El tribunal comienza explicando que las disposiciones de esta Decisión sólo pueden ser aplicadas a las empresas que hayan firmado y ratificado la misma. Por lo tanto, las autoridades públicas, incluidas las de EE. UU. no tienen la obligación de cumplir con lo dispuesto en la Comisión, solo están sometidas a la ley estadounidense en relación con la seguridad nacional y el interés público.

Además, el principio de jerarquía normativa nos indica que las leyes de EE. UU. prevalecen sobre las normas europeas dentro del territorio americano, y en este caso, la legislación estadounidense permite a las autoridades públicas acceder a los datos personales transferidos. Esta situación entre en conflicto con los derechos fundamentales de los ciudadanos europeos, y, en parte, con la propia Decisión 2000/520/CE de la Comisión. Como consecuencia de este conflicto normativo, el TJUE estableció que el *Safe Harbor* resulta ineficaz como régimen jurídico de protección porque no puede evitar la interferencia de las autoridades de Estados Unidos, lo que supone una violación del derecho fundamental al respeto de la vida privada.

Además, los ciudadanos afectados por esta situación no cuentan con los medios legales para poder defenderse y exigir una suspensión o rectificación, provocando una vulneración del derecho a la tutela judicial efectiva.

Con todo ello, el TJUE declara en la sentencia de 6 de octubre de 2015, asunto C-362/14, también conocida como Schrems I, y que pone fin a este procedimiento, que la Decisión 2000/520/CE de la Comisión es inválida.

2.2 Consecuencias de la sentencia Schrems I.

Al haber sido declarada inválida la Decisión 2000/520/CE, la reclamación interpuesta por Maximilian Schrems ante la autoridad nacional de control al inicio de este proceso volvió a estimarse y plantearse en diciembre de 2015, aunque fue necesaria una modificación, ya que se apoyaba en el *Safe Harbor* como fundamento jurídico y, este había sido derogado. En esa modificación se pidió a la empresa hacia la que iba dirigida la reclamación, tanto en su filial irlandesa, Facebook Ireland, como la empresa matriz estadounidense, Facebook Inc. que explicaran cuál era la nueva base jurídica sobre la que se apoyan para seguir transfiriendo datos personales hacia el tercer país (en este caso, los países de la Unión Europea). La filial irlandesa, se apoyaba en los *Data Transfer Processing Agreement*[12] y la empresa matriz de Estados Unidos, en la Decisión 2010/87 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.

Maximilan Schrems planteó en la modificación, que las cláusulas del *Data Transfer Processing Agreement* no son una justificación válida desde un punto de vista jurídico al no ser acordes a las cláusulas contractuales tipo de la Decisión 2010/87, dado que en Estados Unidos no se garantiza una protección adecuada sobre los ciudadanos de países terceros cuyos datos personales son transferidos.

[12] "Se trata de un acuerdo de procesamiento de datos (DPA), un documento legalmente vinculante que debe celebrarse entre el importador y exportador de datos. Regula las particularidades del tratamiento de datos, como su alcance y finalidad, así como la relación entre el responsable del tratamiento y el encargado del tratamiento." (Kovacsics. P, 2018).

Existen autoridades estadounidenses como la Agencia Nacional de Seguridad y el Buró Federal de Investigaciones que tienen acceso a los datos personales a través de programas de vigilancia[13], contradiciendo lo establecido en los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea. Además, los ciudadanos europeos afectados no tienen la posibilidad de ejercer acciones de Derecho en caso de ver perjudicados sus derechos relativos a la vida privada y de protección de sus datos personales en territorio estadounidense. Por lo tanto, las cláusulas del *Data Transfer Processing Agreement* no sirven como justificación legal para continuar transfiriendo datos personales entre la filial y la matriz de Facebook, pidiendo que las transferencias entre los países miembros y países terceros queden suspendidas por no estar protegidas adecuadamente.

La High Court llega a la conclusión que las cláusulas del *Data Transfer Processing Agreement* no son suficientes para garantizar la protección de los datos de los ciudadanos de la UE, pero surge la duda de si las cláusulas contractuales tipo garantizan o no esa protección.

Para resolver esta duda, la autoridad de control acude a la High Court para que presente una nueva cuestión prejudicial ante el TJUE solicitando el examen de la Decisión 2010/87, con el objetivo de aclarar si la Decisión es válida o no.

2.3 Contexto jurídico de Schrems II. Entrada en vigor del *Privacy Shield*.

La demanda que da lugar a la sentencia Schrems II planteada por la High Court se interpuso ante el TJUE en mayo de 2018, casi tres años más tarde desde la declaración de invalidez del *Safe Harbor*. En este lapso se aprobó la Decisión 2016/1250[14], también llamado *Privacy Shield*, el acuerdo firmado entre Estados Unidos y la Unión Europea para la protección de datos que actuaba como sucesor al *Safe Harbor*. En términos generales, el Escudo de Privacidad planteaba un marco jurídico más seguro para los usuarios, ya que las empresas estadounidenses ofrecían unas garantías similares a las existentes en la Unión Europea.

[13] En concreto, "los programas PRISM y Upstream, basados en el artículo 702 de la Foreign Intelligence Surveillance Act (FISA), que permite a las autoridades estadounidenses la vigilancia de extranjeros no residentes en los Estados Unidos, y la E.O. 12333, que habilita a la Agencia de Seguridad Nacional estadounidense para obtener datos en tránsito antes de su llegada al territorio nacional." (Fuentes Máiquez, 2021)

[14] 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.

Mediante este acuerdo, las empresas establecidas en Estados Unidos que recibían datos personales de ciudadanos de los países miembros debían cumplir con la normativa europea de protección de datos, de tal manera que el nivel de protección sería equivalente en Estados Unidos y la Unión Europea. El problema era que seguían existiendo insuficiencias en la legislación norteamericana al no reconocer el derecho de los ciudadanos de la UE a poder ejercer acciones de Derecho en caso de no verse respetado el nivel de protección en la transferencia de datos personales, violando el artículo 47 de la Carta de Derechos Fundamentales de la UE. El *Privacy Shield* no incluye ninguna referencia a esta situación, y tampoco plantea ninguna solución, lo que llevó a dudar sobre su validez. Además de la aprobación de la Decisión 2016/1250, en 2016 también se modifica la decisión que regula las cláusulas contractuales tipo, aprobándose la Decisión de Ejecución (UE) 2016/2297 de la Comisión[15].

2.4 Cuestiones prejudiciales planteadas en la sentencia del TJUE de 16 de julio de 2020.

La cuestión planteada por la High Court ante el TJUE tiene como finalidad aclarar si la Decisión 2010/87 es válida o no. Ante esta situación, se suspendió el procedimiento y se plantearon las siguientes cuestiones prejudiciales al TJUE:

"1) ¿Es la normativa de la Unión, incluida la Carta, sin perjuicio de lo dispuesto en los artículos 4 TUE, apartado 2, respecto a la seguridad nacional, y 3, apartado 2, primer guion, de la Directiva [95/46], en relación con la seguridad pública, la defensa y la seguridad del Estado, aplicable a la transferencia de datos personales en un contexto en el que una empresa privada de un Estado miembro de la [Unión] transfiere, con arreglo a la Decisión [CPT], a una empresa privada de un tercer país datos personales con fines comerciales que pueden ser tratados posteriormente por las autoridades de ese tercer país no sólo por razones de seguridad nacional, sino también a efectos de la aplicación de la ley y de la administración de los asuntos exteriores del país?

[15] 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.

2) a) A efectos de la Directiva [95/46], al determinar si el hecho de transferir con arreglo a la Decisión [CPT] datos desde la [Unión] a un tercer país en el que posteriormente pueden tratarse dichos datos por razones de seguridad nacional constituye una vulneración de los derechos de una persona, ¿el elemento de referencia pertinente es:

i) la Carta, el Tratado UE, el Tratado FUE, la Directiva [95/46], el [Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950,] (o cualquier otra disposición del Derecho de la Unión), o bien

ii) la legislación nacional de uno o varios Estados miembros?

b) Si el elemento de referencia pertinente es el mencionado en [el inciso ii)], ¿deben incluirse en él también las prácticas seguidas en el contexto de la seguridad nacional en uno o varios Estados miembros?

3) Al valorar si un tercer país garantiza el nivel de protección que exige la normativa de la Unión para transferir datos personales a dicho país a efectos del artículo 26 de la Directiva [95/46], ¿deberá evaluarse el nivel de protección ofrecido en ese tercer país atendiendo a:

a) las reglas aplicables en ese tercer país derivadas de la legislación interna o de los compromisos internacionales de este, así como a la práctica seguida para asegurar el cumplimiento de esas reglas, al efecto de incluir las normas profesionales y las medidas de seguridad que aplica dicho país, o bien

b) las reglas referidas en la letra a) junto con tales prácticas administrativas, reglamentarias y de ejecución y las medidas de protección y los procedimientos, protocolos, mecanismos de control y recursos extrajudiciales aplicables en el tercer país?

4) ¿Constituye una violación de los derechos de toda persona contemplados en los artículos 7 y/u 8 de la Carta la transferencia de datos personales desde la [Unión] a EE. UU. [con arreglo a la Decisión CPT], habida cuenta de los hechos probados por la High Court [(Tribunal Superior)] en relación con la normativa de EE. UU.?

5) Habida cuenta de los hechos probados por la High Court [(Tribunal Superior)] respecto a la normativa de EE. UU., en el supuesto de que se transfieran datos personales desde la [Unión] a EE. UU. con arreglo a la Decisión [CPT]:

a) ¿Respeta el nivel de protección proporcionado por EE. UU. el contenido esencial del derecho de toda persona a la tutela judicial efectiva garantizado por el artículo 47 de la Carta en caso de violación del derecho a mantener la privacidad de sus datos?

En caso de respuesta afirmativa a la cuestión planteada en la letra a):

b) ¿Son proporcionadas, en el sentido del artículo 52 de la Carta, las limitaciones impuestas por la legislación de EE. UU. al ejercicio del derecho de toda persona a la tutela judicial en el contexto de la seguridad nacional de ese país y no van más allá de lo necesario para salvaguardar la seguridad nacional en una sociedad democrática?

6) a) ¿Cuál es, en virtud del artículo 26, apartado 4, de la Directiva [95/46], a la luz de las disposiciones de [esta] Directiva, y en particular de [sus] artículos 25 y 26, interpretados a la luz de la Carta, ¿el nivel de protección que debe proporcionarse a los datos personales transferidos a un tercer país con arreglo a cláusulas contractuales tipo estipuladas de conformidad con una decisión de la Comisión?

b) ¿Cuáles son los elementos que han de tomarse en consideración al valorar si el nivel de protección proporcionado a los datos transferidos a un tercer país en virtud de la Decisión [CPT] cumple los requisitos establecidos por la Directiva [95/46] y la Carta?

7) El hecho de que las cláusulas contractuales tipo sean aplicables al exportador de datos y al importador de datos, pero no resulten vinculantes para las autoridades nacionales de un tercer país, que pueden exigir al importador de datos que facilite a sus servicios de seguridad, para su posterior tratamiento, los datos personales transferidos con arreglo a las cláusulas establecidas en la Decisión [CPT], ¿impide que se incluyan en las cláusulas contractuales tipo las garantías de protección adecuadas previstas en el artículo 26, apartado 2, de la Directiva [95/46]?

8) Si un importador de datos de un tercer país está sujeto a normas de vigilancia que, en opinión de una autoridad de protección de datos, entran en conflicto con las cláusulas tipo de protección, los artículos 25 y 26 de la Directiva [95/46] o la Carta, ¿está obligada una autoridad de protección de datos a ejercer las facultades en materia de aplicación de la legislación que le confiere el artículo 28, apartado 3, de la Directiva [95/46] para suspender los flujos de datos, o bien el ejercicio de dichas facultades se limita únicamente a situaciones excepcionales, a la luz del considerando 11 de la Decisión [CPT], o acaso puede la autoridad de protección de datos hacer uso de su potestad discrecional para no suspender tales flujos de datos?

9) a) A los efectos del artículo 25, apartado 6, de la Directiva [95/46], ¿constituye la Decisión [EP] una constatación de alcance general vinculante para las autoridades de protección de datos y los órganos jurisdiccionales de los Estados miembros en el sentido de que EE. UU., en virtud de su legislación nacional o de los compromisos internacionales que ha suscrito, garantiza un nivel de protección adecuado en el sentido del artículo 25, apartado 2, de la Directiva [95/46]?

b) Si no es así, ¿qué relevancia tiene, en su caso, la Decisión [EP] en la valoración efectuada en cuanto a la adecuación de la protección ofrecida a los datos transferidos a EE. UU. conforme a la Decisión [CPT]?

10) Habida cuenta de las consideraciones de la High Court [(Tribunal Superior)] respecto a la legislación de EE. UU., ¿constituye la figura del defensor del pueblo en el ámbito del Escudo de la Privacidad a que se refiere el anexo A del anexo III de la Decisión [EP], en combinación con el régimen vigente en EE. UU., una garantía de que este país ofrece una vía de recurso compatible con el artículo 47 de la Carta a los interesados cuyos datos personales son transferidos a EE. UU. con arreglo a la Decisión [CPT]?

11) ¿Viola la Decisión [CPT] los artículos 7, 8 y/o 47 de la Carta?»"[16]

[16] STJUE 16 de julio de 2020, C-311/18, *Data Protection Commissioner*, §68.

Vamos a realizar un análisis general de las once cuestiones prejudiciales planteadas por la High Court, las cuales son contestadas por el TJUE a lo largo de la sentencia Schrems II para resolver las dudas existentes sobre el posible incumplimiento de los artículos 7, 8 y 47 de la Carta al aplicarse la Directiva 95/46/CE; sobre la validez de la Decisión 2010/87/CE; y sobre la validez de la Decisión 2016/1250/CE.

Para poder comenzar con el análisis es necesario indicar que la Directiva 95/46[17] fue derogada y sustituida por el Reglamento General de Protección de Datos[18] desde el 25 de mayo de 2018, por lo que, en el momento del planteamiento de la cuestión prejudicial[19] al TJUE la Directiva 95/46 todavía estaba en vigor. Además, el RGPD reproduce los artículos 3, apartado 2, primer guion, 35, 26 y 28 que se recogían en la Directiva 95/46 en los artículos 2, apartado 2, 45, 46 y 58 respectivamente. Estos son los artículos usados en la petición prejudicial planteada ante el TJUE como fundamento jurídico. Este cambio normativo no supone una causa de inadmisibilidad y procede continuar con el procedimiento.

Con la primera cuestión prejudicial se resuelve la duda existente sobre la posibilidad de transferir datos personales desde un Estado miembro a un tercer país cuando es conocido que esos datos no están protegidos de forma adecuada y pueden llegar a las autoridades nacionales del país tercero con el pretexto de proteger la seguridad nacional. Para contestar hay que acudir al RGPD, que regula el tratamiento total o parcial de los datos personales. En el artículo 4 del RGPD se recoge qué se entiende por "tratamiento": "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no"[20].

No distingue entre operaciones realizadas dentro de la UE o en el exterior, pero en el Capítulo V del RGPD sí que se recogen normas específicas para las transferencias de datos personales a países terceros, otorgando competencias a las autoridades nacionales en materia de transmisión de datos.

---

[17] 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.

[18] 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).

[19] El 4 de mayo de 2018.

[20] Unión Europea. 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.

Conociendo esta información el TJUE manifiesta que las operaciones de transmisión de datos con fines comerciales del caso Schrems se incluyen en el ámbito de aplicación del RGPD al no poder aplicarse ninguna excepción recogida en este mismo Reglamento.

En relación con las cuestiones segunda, tercera y sexta se resuelve la duda sobre cuál es el nivel de protección exigido en los artículos 46.1 y 46.2 c) del RGPD[21] aplicados a las transferencias de datos entre países de la UE y un país tercero que tienen como base cláusulas contractuales tipo. En relación con esta cuestión debemos acudir al artículo 45 del RGPD, según el cual la transferencia de datos se permitirá siempre que se apruebe una decisión de la Comisión que corrobore un nivel de protección adecuado en el país tercero[22]. En caso de no existir este nivel de protección adecuado se prohibirá la transferencia de datos personales al país tercero, conforme a lo establecido en el artículo 58 del RGPD[23]. Este artículo no se aplicará si en caso de no darse el nivel de protección adecuado se han establecido en las cláusulas contractuales tipo unas garantías que avalen un nivel de protección similar al de la UE sobre las transferencias de datos personales.

[21] Unión Europea. 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.

Artículo 46. Transferencias mediante garantías adecuadas.
1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.
2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:
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;

[22] Como ya se ha explicado en un apartado anterior el nivel de protección adecuado se evaluará caso por caso, pero tiene que asegurar un nivel de protección equivalente al establecido en la UE.
[23] Unión Europea. 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.

Artículo 58. Poderes.
2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición; j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

El TJUE también aclara cuáles son los requisitos que se tendrán en cuenta a la hora de evaluar el nivel de protección en la transferencia de datos personales a un país tercero en base al artículo 46 del RGPD. Se establece que la autoridad competente de la UE respecto al tratamiento de datos, en cooperación con el destinatario será el encargado de comprobar si se dan las garantías adecuadas en la transferencia de datos personales.

Mediante la resolución de las cuestiones prejudiciales segunda, tercera y sexta se establece que el artículo 46.1 y 46.2 c) del RGPD debe ser interpretado entendiendo que sus disposiciones pretenden garantizar la protección de los datos transferidos a través de las cláusulas tipo de una manera similar a como se da esa protección en la UE a través del RGPD en conformidad con lo dispuesto en la Carta.

Además, el TJUE expresa que a la hora de evaluar el nivel de protección adecuado debe tenerse en cuenta las cláusulas del contrato entre el responsable de la UE y el destinatario, lo que conllevará un cierto acceso por parte de las autoridades públicas a los datos personales transferidos, y también se tendrá en cuenta la legislación del país tercero referente a la transferencia de datos, según lo dispuesto en el artículo 45.2 del RGPD.

En siguiente lugar hablaremos de la cuestión prejudicial octava, donde se plantea al TJUE si conforme al artículo 58.2 f) y j) del RGPD la autoridad nacional de control tiene competencia para suspender o prohibir una transferencia de datos personales a un país tercero en base a cláusulas contractuales tipo aprobadas por la Comisión cuando la autoridad observa que no se da un nivel de protección adecuado y no se cumple con las cláusulas acordadas. El TJUE determina que siempre que se presente una reclamación de protección de derechos y libertades referentes a una transmisión de datos ante una autoridad competente tendrá la obligación de comprobar si se cumplen los requisitos del RGPD para las transferencias de datos entre la UE y un país tercero. En caso de no cumplirse, y no poder hacerlo por otras vías, suspenderá o prohibirá la transferencia de datos al país tercero al no garantizarse la protección adecuada (a menos que se adopte una decisión de la Comisión que lo contradiga).

En las cuestiones prejudiciales séptima y undécima se cuestiona la validez de la Decisión CPT en virtud de los artículos 7, 8 y 47 de la Carta de Derechos Fundamentales de la UE. La High Court plantea si la Decisión CPT asegura un nivel de protección adecuado en las transferencias de datos personales sabiendo que las cláusulas contractuales tipo no son vinculantes para las autoridades de los países terceros, aunque sí que lo son para el responsable de la UE y el destinatario de los datos.

Por lo tanto, si las autoridades están al margen de las cláusulas y pueden interferir en las transferencias de datos, se pueden dar situaciones en las que las cláusulas contractuales tipo no sean suficientes para asegurar el nivel de protección adecuado en esa transferencia de datos personales.

Siguiendo lo establecido en el artículo 46.1 RGPD si la decisión de la Comisión relativa a la cláusula contractual de transferencias de datos personales no garantiza un nivel de protección adecuado, el responsable de la transferencia en la UE cumplirá con el acuerdo siempre y cuando se ofrezcan las garantías suficientes por parte del país tercero en relación con el tratamiento de los datos y con los derechos de los ciudadanos para defender una posible intromisión. Estas garantías pueden ser incluidas en las cláusulas tipo de protección de datos a través de una decisión de la Comisión cuando se asegure que el ordenamiento jurídico del país tercero garantice una protección adecuada.

En conformidad con lo anterior, en el artículo 46.2 c) del RGPD se busca la uniformidad de los contratos de transmisión de datos personales en todos los países terceros, es decir, que en todos ellos se exijan las mismas garantías de seguridad. Se permite que las garantías se incluyan dentro de las cláusulas tipo, o a través de unas garantías adicionales externas, y en caso de no existir estas garantías, se adopten medidas excepcionales para garantizar el nivel de protección adecuado.

De esto se deduce que el responsable de la UE y el destinatario del país tercero tienen el deber de verificar en un momento previo a la transferencia que el nivel de protección es adecuado. Si el destinatario del país tercero manifiesta que no es posible cumplir con las exigencias establecidas en la cláusula 5 b) del anexo de la Decisión 2016/2297 en relación con las cláusulas tipo de protección de datos, y tampoco cuenta con otros medios para garantizar la protección de los datos, tiene que devolver al encargado de la UE todos los datos transferidos, o destruirlos.

A partir de esta información podemos evaluar la validez de la Decisión 2016/2297. El hecho de que las cláusulas tipo no sean aplicables sobre las autoridades públicas de los países terceros no implica que la Decisión CPT sea inválida, eso dependerá de la interpretación del artículo 46.1 y 46.2 c) del RGPD en virtud de los artículos 7, 8 y 47 de la Carta.

Según analiza el TJUE, la Decisión CPT es válida conforme a que incluye medios para garantizar la seguridad en las transferencias de datos personales dirigidas a países terceros, y en caso de no cumplir con la protección adecuada, se prohibirá la transferencia. No se contradice lo dispuesto en los artículos 7, 8 y 47 de la Carta.

A continuación, corresponde atender a las cuestiones prejudiciales cuarta, quinta, novena y décima. En la cuestión novena se pregunta si las autoridades de control de los países de la UE están sujetas al *Privacy Shield,* y en las cuestiones restantes la High Court cuestiona la propia validez del *Privacy Shield*, dudando de la compatibilidad entre la figura de Defensor del Pueblo mencionada en el *Privacy Shield* y el artículo 47 de la Carta. Respecto a la duda de la cuestión prejudicial novena, el TJUE explica que, mientras el *Privacy Shield* siga vigente las autoridades nacionales de control no pueden suspender ni prohibir una transferencia de datos realizada bajo el amparo del *Privacy Shield*, aunque esta no asegure la protección adecuada. Sin embargo, la autoridad de control tiene competencia para presentar una cuestión prejudicial ante el órgano jurisdiccional nacional correspondiente en caso de que una persona les plantee una reclamación.

Y, por otro lado, respecto a la validez de la Decisión 2016/1250 se pone en duda porque incumple con los artículos 7 y 8 de la Carta al permitir que las autoridades de EE. UU. conozcan los datos personales transferidos. En la Carta se establece que ante la existencia de normas que limiten los derechos de los ciudadanos es necesario el consentimiento del afectado, así como la fijación de unos márgenes que no se deben sobrepasar.

Esto no se cumple en el caso de Estados Unidos, ya se comprobó que cuentan con unos programas de vigilancia que vulneran los derechos de los ciudadanos europeos, que excede el principio de proporcionalidad. La vulneración de los derechos pretende equilibrarse con la creación de la figura del Defensor del Pueblo dentro del *Privacy Shield*, que tiene por objetivo garantizar el derecho a la tutela judicial efectiva reconocido en el artículo 47 de la Carta. El problema es que el Defensor del Pueblo está vinculado directamente al Secretario de Estado, lo que provoca que sea visto como una figura poco imparcial, además de no tener competencia suficiente para dictar decisiones vinculantes para los Estados.

A pesar de que el Abogado General manifestara que el TJUE no debería decidir sobre la validez de la Decisión 2016/1250, al final de la sentencia de 16 de julio de 2020, el TJUE dictaminó que el *Privacy Shield* es inválido al no proteger de forma adecuada los derechos de los ciudadanos en las transferencias internacionales entre los estados miembros y los terceros.

El problema se encontraba en el artículo 702 del *Foreign Intelligence Surveillance Act, (o Ley de Vigilancia de la Inteligencia Extranjera* en castellano). Siguiendo este artículo los proveedores de servicios de comunicación electrónica de EE. UU. se pueden ver obligados a entregar datos personales de ciudadanos no estadounidenses[24] a las autoridades de seguridad de los Estados Unidos con fines de diversa naturaleza. Además de la violación del derecho a la protección de la vida privada de los ciudadanos europeos mediante la aplicación del artículo 702 FISA, existen otras dos normas legislativas estadounidenses que no garantizan el nivel de protección adecuado. Estas normas son, una orden ejecutiva (*Executive Order 12333 – United States intelligence activities*) y, una orden presidencial (*Presidential Policy Directive 28 – Signals Intelligence Activities*) que permiten al poder ejecutivo acceder a los datos personales de ciudadanos extranjeros.[25]

2.5 Fallo y consecuencias de la sentencia Schrems II.

Los hechos principales derivados de la sentencia del TJUE de 16 de julio de 2020 son los siguientes:

- La Directiva 95/46/CE queda derogada por el Reglamento 2016/679 del Parlamento Europeo y del Consejo, 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.
  Este nuevo reglamento se aplica a las transferencias de datos personales entre un Estado miembro y un país tercero en las que existen fines comerciales de por medio y, en las que las autoridades del país tercero tienen acceso a los datos con el pretexto de la seguridad nacional y la defensa.

- El RGPD establece en su artículo 46 que los derechos de los ciudadanos cuyos datos se están transfiriendo al país tercero se protejan a través de las clausulas tipo de protección de datos de una manera similar a como son protegidos y garantizados dentro de la UE. Para examinar el nivel de protección ofrecido se evaluarán las disposiciones establecidas en el contrato comercial firmado entre las partes, y, también, los elementos del ordenamiento jurídico del país tercero a los que se refiere el artículo 45.2 RGPD, con el fin de determinar las competencias otorgadas a las autoridades públicas del país tercero en relación con los datos transferidos.

[24] Cualquier persona que no tenga la nacionalidad o la residencia en EE. UU.
[25] STJUE 16 de julio de 2020, C-311/18, *Data Protection Commissioner.* (Pp. 16-21 de este trabajo.)

- En cuanto a la competencia de la autoridad nacional de control, el artículo 58.2 f) y j) del RGPD determina que son competentes para prohibir o suspender una transferencia de datos personales realizada en base a una clausula contractual tipo cuando no se asegura o no puede asegurarse el nivel de protección adecuado en la transferencia hacia el país tercero. Como excepción, la Comisión puede dictar decisiones que contradigan este artículo e impidan que la autoridad de control prohíba la transferencia.

- Sobre 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, modificada por la Decisión de Ejecución (UE) 2016/2297 el TJUE ha dictaminado que no existe ninguna disposición que viole los artículos 7, 8 y 47 de la Carta, y por ello sigue siendo válida y aplicable.

- En último lugar, tras examinar la Decisión de Ejecución 2016/1250/UE sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU el TJUE observó que el derecho nacional de EE. UU. no cubre determinados derechos fundamentales establecidos en la Carta[26], declarando inválida la Decisión de Ejecución por no proporcionar suficiente protección sobre los ciudadanos europeos cuyos datos personales se transferían hacia EE. UU. A partir de ese momento, el *Privacy Shield* no es aplicable en ninguna transferencia de datos realizada desde un país miembro de la UE con destino EE. UU. y, todas aquellas transferencias que se hayan hecho conforme al *Privacy Shield* se consideran ilegales.[27]

2.6 Reacción a la sentencia Schrems II.

2.6.1 A nivel mundial

Cuando la sentencia del TJUE de 16 de julio de 2020 fue publicada se produjo una situación de incertidumbre en el mercado, teniendo que revisar todos los acuerdos y contratos comerciales que implicaran transferencias de datos hacia terceros países y estuvieran amparados en el *Privacy Shield.*

[26] La Decisión de Ejecución 2016/1250/UE no cumplía con lo dispuesto en el artículo 8 de la Carta, la protección de datos material y efectiva sobre los ciudadanos europeos.
[27] STJUE 16 de julio de 2020, C-311/18, *Data Protection Commissioner.* Conclusiones del Abogado General.

El caso Schrems II tiene lugar en un mundo globalizado e informatizado donde las transferencias de datos están a la orden del día. Además, una de las características de la globalización es el dinamismo provocado por los constantes cambios tecnológicos y políticos, que nos llevarán a situaciones similares[28] a la ocurrida con el *Privacy Shield* si no se desarrolla una normativa global que asegure la protección de los derechos de los ciudadanos en las transferencias de datos personales.

Hay que aclarar que la resolución del TJUE no prohíbe las transferencias de datos hacia terceros países, sino que las limita a exigir que se cumplan las garantías de protección recogidas en el RGPD[29] para poder realizarlas. Las agencias de protección de datos de distintos países se han pronunciado para apoyar la invalidación del *Privacy Shield*, exigiendo que se protejan los derechos fundamentales de sus ciudadanos. Algunos ejemplos son los siguientes:

- La Agencia Irlandesa de Protección de Datos (DPC) ha manifestado la importancia de asegurar un nivel de protección adecuado en las transferencias de datos personales hacia países terceros.
- La Agencia Federal Alemana de Protección de Datos y Libertad de Información puso de relieve la necesidad de cambiar las cláusulas de privacidad existentes en los contratos, de tal manera que sí se permite la transferencia de datos a EE. UU. siempre que se asegure el nivel de protección adecuado. Alemania es un país comprometido con la protección de datos y, en distintas regiones como Berlín, Hamburgo y Renania se van a llevar a cabo controles sobre las empresas para comprobar si están realizando cambios en sus contratos, cumpliendo con las garantías exigidas en el RGPD.
- La Agencia de Protección de datos de Finlandia también está realizando consultas sobre las empresas establecidas en Finlandia que transfieren datos personales a EE. UU. con el fin de investigar si han realizado cambios en sus contratos y de que tipo. Además, han nombrado en 2019 un nuevo Defensor del Pueblo Adjunto a la Protección de Datos como figura adicional que asegure el cumplimiento del RGPD.

[28] Por ejemplo, el Brexit podría plantear dudas similares a las del caso Schrems II sobre las transferencias de datos hacia Reino Unido.
[29] Al carecer de normas técnicas que regulen las transferencias internacionales, las empresas se han acogido al RGPD como ley marco.

2.6.2 A nivel europeo

La UE a través de su Supervisor Europeo de Protección de Datos[30] (en adelante SEPD) se pronunció sobre las medidas que se llevarían a cabo para mejorar la protección de los derechos en las transferencias de datos personales internacionales, surgidas a raíz de conocerse la sentencia Schrems II. Estas medidas se recogen en la "Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE"[31] (en adelante la Recomendaciones 01/2020), adoptadas en noviembre de 2020 con el objetivo de mejorar la protección de los datos personales en las transferencias dirigidas a terceros países, incluyendo EE. UU. Wojciech Wiewiórowski[32], en calidad de SEPD manifestó que la Recomendación 01/2020 se basa en la cooperación y la responsabilidad de los responsables del tratamiento para evaluar si el estándar de protección en los países terceros es esencialmente equivalente al de la UE recogido en la Carta.

También se aclara que el SEPD seguirá cooperando estrechamente con las autoridades de protección de datos (APD[33]) y el Comité Europeo de Protección de Datos (CEPD[34]) para que los datos personales de las personas estén protegidos de forma coherente en todo el EEE, cuando se produzcan transferencias de datos a terceros países.

La sentencia Schrems II repercutió directamente sobre los medios legales utilizados para transferir datos personales desde el EEE a cualquier tercer país, incluidas las transferencias entre autoridades públicas. Si bien la Recomendación 01/2020 tiene como objetivo hacer que todas las transferencias se ajusten al RGPD a medio plazo, el SEPD ha identificado dos prioridades para abordar a corto plazo: contratos continuos de responsable a encargado;

[30] "El SEPD es la autoridad de supervisión independiente responsable de supervisar el tratamiento de datos personales por parte de las instituciones y órganos, oficinas y agencias de la UE, asesorar sobre las políticas y la legislación que afectan a la privacidad y cooperar con autoridades similares para garantizar una protección de datos coherente." (European Data Protection Supervisor, 2020).

[31] (European Data Protection Board, 2020).

[32] Fue elegido por decisión conjunta del Parlamento y el Consejo Europeo como SEPD en diciembre de 2019 por un periodo de cinco años.

[33] "Las APD son autoridades públicas independientes que vigilan y supervisan, mediante los poderes de investigación y correctivos, la aplicación del Reglamento de protección de datos." (Comisión Europea, 2016)

[34] "El Comité Europeo de Protección de Datos (CEPD) 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. El CEPD está compuesto por representantes de las autoridades nacionales de protección de datos y del Supervisor Europeo de Protección de Datos (SEPD)" (European Data Protection Supervisor, 2020).

y/o contratos de encargado a subencargado que implican transferencias de datos a terceros países. En el documento "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento"[35] se regulan estos dos tipos de contratos mencionados:

- Los contratos continuos consisten en normalizar el acuerdo entre responsable y encargado del tratamiento mediante un contrato o un acto jurídico similar realizado por escrito, ya sea en forma física o electrónica. "El contenido del acto o acuerdo puede basarse en cláusulas tipo establecidas por la Comisión Europea o por la autoridad de control, inclusive cuando formen parte de una certificación otorgada al responsable o al encargado del tratamiento."[36]

  Todos los acuerdos realizados entre responsable y encargado del tratamiento deben contener como mínimo "el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de los interesados, y las obligaciones, y derechos del responsable". "Es necesario identificar de forma clara y concreta cuáles son los tratamientos de datos a realizar por el encargado del tratamiento, atendiendo al tipo de servicio prestado y a la forma de prestarlo.

  Es especialmente necesario determinar de forma clara las comunicaciones a terceros que el responsable encomienda al encargado o que se derivan del servicio prestado"[37].

- El régimen de subcontratación: Para que se de la subcontratación, se tiene que expresar por escrito en el acuerdo. "El RGPD exige que se de una autorización previa por escrito del responsable del tratamiento para que el encargado del tratamiento pueda recurrir a otro encargado (subencargado) para desarrollar el servicio encomendado, cuando esto conlleve el tratamiento de los datos personales por parte de un tercero. Esta autorización puede ser especifica (identificación de la entidad concreta) o general (solo autorizando la subcontratación, pero sin concretar la entidad).

[35] Agencia Española de Protección de Datos, 2018.

[36] Agencia Española de Protección de Datos, 2018, pp 4 de las "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento".

[37] Agencia Española de Protección de Datos, 2018, pp 6 de las "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento".

En todo caso, el subencargado del tratamiento debe estar sujeto a las mismas condiciones[38] y en la misma forma[39] que el encargado del tratamiento en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En caso de incumplimiento por el subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones del subencargado."[40]

El SEPD ha incluido en la Recomendación 01/2020 el proceso mediante el cual se garantiza que las transferencias de datos serán compatibles con el RGPD. Los pasos a seguir son:

a. Evaluación de las transferencias. El responsable de la transmisión debe conocer quién va a procesar sus datos, en qué lugar y con qué propósito. Además de asegurar que el exportador cumpla con las medidas técnicas, organizativas y de seguridad necesarias. "Conocer las transferencias es un primer paso esencial para cumplir sus obligaciones en virtud del principio de responsabilidad proactiva."
b. "Determinar los instrumentos de transferencia en los que se está basando". Verificar que los instrumentos usados como base legal para realizar las transferencias son los que recoge el RGPD, en su capítulo V.
c. "Evaluar si el instrumento de transferencia del articulo 46 del RGPD en el que se está basando es eficaz a la luz de todas las circunstancias de la transferencia".

   Examinar los riesgos que conlleva la legislación nacional del país tercero, es decir, ver si la herramienta de transferencia en la que se basa es eficaz con respecto a la normativa europea.
d. Adoptar e identificar medidas complementarias para proteger los datos personales. Si la legislación de los países terceros no permite una protección de datos suficiente, entonces se deben tomar medidas complementarias de carácter técnico, organizativo o contractual para proteger los datos que se pretenden transferir.

[38] instrucciones, obligaciones, medidas de seguridad...
[39] acuerdo por escrito o acto jurídico vinculante.
[40] Agencia Española de Protección de Datos, 2018, pp 8 de las "Directrices para la elaboración de contratos entre responsables y encargados del tratamiento".

Si las medidas complementarias elegidas, en combinación con la herramienta de transferencia (artículo 46 RGPD) garantizan una protección de datos adecuado, igual a los estándares dispuestos en el Reglamento General de Protección de Datos, la transferencia de datos puede continuar.

e. "Fases del procedimiento si ha determinado medidas complementarias eficaces". Llevar a cabo las medidas procesales necesarias, de tal manera que se asegure que las medidas complementarias y la herramienta de transferencia del RGPD no se contradigan.

   En este quinto paso se incluye referencia a las "Cláusulas tipo de protección de datos (CPT) [artículo 46, apartado 2, letras c) y d), del RGPD]"; "NCV [artículo 46, apartado 2, letra b), del RGPD]"; y "cláusulas contractuales específicas [artículo 46, apartado 3, letra a), del RGPD]".

f. "Volver a evaluar a intervalos adecuados". Examinar de forma periódica la protección legal ofrecida por los terceros países en materia de protección de datos.[41]

Puede parecer que la Recomendación 01/2020 del SEPD soluciona el problema que se planteaba en la sentencia Schrems II con respecto a la protección de datos, pero resulta insuficiente, dando lugar a algunas dudas, como ocurre con el tercer y cuarto apartado de la Recomendación 01/2020. En el apartado c) se plantea la necesidad de examinar la legislación nacional para concretar si su nivel de protección es adecuado o no. Tener que examinar las legislaciones extranjeras puede suponer una tarea difícil para los profesionales europeos. En el apartado d) se plantea la posibilidad de adoptar medidas complementarias para minimizar el riesgo de que las autoridades del país tercero accedan a los datos personales.

A nivel teórico parece fácil, pero desde un punto de vista práctico, la Comisión no ha especificado los pasos que deben seguir las empresas para adoptar esas medidas complementarias.

[41] Unión Europea. Recomendación (UE) 01/2020 de 10 de noviembre de 2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE.

La Recomendación 01/2020 ha desencadenado que a nivel europeo se hayan iniciado los primeros pasos para asegurar que los contratos comerciales realizados entre la UE y grandes empresas estadounidenses como Amazon Web Services y Microsoft contengan un nivel de protección adecuado sobre las transferencias de datos personales. El Supervisor Europeo de Protección de Datos ha comenzado una investigación sobre las garantías ofrecidas por las multinacionales en los contratos de servicios digitales, como, por ejemplo, los contratos de almacenamiento en la nube firmados por la UE. También se está investigando si el software de Microsoft, *Microsoft Office 365*, cumple con los requisitos exigidos en el RGPD.
Se sospecha que el uso de ese programa informático conlleva la transferencia de datos personales hacia países terceros sin el consentimiento de los usuarios, es decir, el uso del almacenamiento en la nube no es del todo seguro para los datos de la UE.

La solución para la UE sería crear un sistema informático propio para el almacenamiento de datos, controlado internamente por las instituciones de la UE, que no conllevara transferencias hacia empresas extranjeras. Con esa intención de reducir laa dependencia del exterior en materia tecnológica, Alemania y Francia están desarrollando su propia plataforma en la nube llamada GAIA- X para gestionar y almacenar los datos de la UE. Al mismo tiempo, la UE ha presentado un plan de digitalización con objetivo 2030: "Brújula de digitalización hacia 2030".

3. TRANSFERENCIAS INTERNACIONALES DE DATOS.

3.1 Definición

El RGPD no recoge una definición, pero entendemos como transferencia internacional de datos al flujo de datos personales desde el EEE (los países miembros de la UE, Liechtenstein, Islandia y Noruega) hacia países terceros u organizaciones internacionales[42] situadas en países distintos a los del EEE.

Las partes que intervienen en la transferencia de datos internacionales son los responsables y los encargados del tratamiento de datos de los países situados dentro de la EEE, por un lado, y los de los países terceros u organizaciones internacionales por otro lado.

[42] Entendiendo como organización internacional todas las personas jurídicas independientes constituidas y regidas en base a sus propios Tratado de constitución. (Hervías Costa, 2021)

Dependiendo de como se lleve a cabo la transferencia de datos, las partes que intervienen pueden ser "a) dos responsables del tratamiento, uno establecido en el EEE y otro establecido en un tercer país o ser una organización internacional, b) un responsable y un encargado del tratamiento, estando establecido el responsable del tratamiento en el territorio del EEE y el encargado del tratamiento fuera del mismo, o c) dos encargados del tratamiento, al igual que en los casos anteriores, uno en el territorio del EEE y otro fuera del mismo."[43]

Las transferencias internacionales se basan en un principio general de prohibición recogido en el artículo 44 RGPD: "Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado."[44]

El nivel adecuado en las transferencias de datos significa que las garantías ofrecidas en el país tercero hacia donde se dirigen deben ser similares a las garantías establecidas por la UE en la Carta.

3.2 Regulación de las transferencias internacionales de datos.

Las transferencias internacionales de datos han sido un tema relevante y controvertido desde la primera sentencia del TJUE que resolvía el litigio comenzado por Maximilian Schrems en 2013. A partir de ese momento han surgido numerosos cambios en las regulaciones referentes a la protección de datos en las transferencias internacionales derivados de la falta de medios de defensa ofrecidos por los terceros países a los ciudadanos europeos.

[43]Guías Jurídicas, 2020.

[44] Unión Europea. 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.

3.2.1 Las transferencias internacionales de datos con el Safe Harbour y el Privacy Shield.

Estos dos acuerdos eran los principales medios de protección en las transferencias internacionales de datos, suponían una garantía suficiente para transmitir los datos desde la UE hasta terceros países, en especial EE. UU. Es cierto que los países miembros contaban con la Directiva 95/46/CE, pero servía para garantizar la protección de los derechos fundamentales de las personas físicas respecto a las transferencias de datos únicamente dentro de la UE. Por lo tanto, eran necesarias normas complementarias a esta directiva que se ajustaran al nuevo mercado globalizado, que incluía transferencias de datos desde la UE hasta países terceros.

El primer acuerdo fue el *Safe Harbor* o "Puerto Seguro", surgido en el año 2000 tras ser firmado entre la UE y EE. UU. De esta manera, se convirtió en la primera regulación internacional en materia de protección de datos, algo novedoso que facilitaba las relaciones comerciales entre la UE y EE. UU., y supuso un aumento del flujo de información transmitida. El *Safe Harbor* suponía contar con un marco normativo aplicable de manera genérica a todas las transferencias de datos entre los países miembros y terceros, sin necesidad de firmar un acuerdo independiente cada vez que se transmitían datos. Además, la intención era que ese acuerdo permaneciera vigente por muchos años, siendo el marco normativo de referencia, ya que proporcionaba numerosas ventajas que favorecían a ambas partes. El acuerdo de Puerto Seguro permitía que todos los acuerdos entre cualquier país de la UE y una empresa de EE. UU. fueran aceptados automáticamente sin tener que revisar los respectivos ordenamientos jurídicos. En el artículo 1 de la Decisión 2000/520/CE se indicaba que todas aquellas empresas que quisieran adherirse al acuerdo debían redactar y enviar una carta al Departamento de Comercio de Estados Unidos de América donde se reconociera expresamente que aceptan los principios del *Safe Harbor*, y se comprometen a actuar de acuerdo a ellos. También se recoge en el artículo 1 los documentos que debían acompañar a la carta: "…. habida cuenta de los siguientes documentos publicados por el Departamento de Comercio de Estados Unidos de América:

a) Estudio de aplicación, que figura en el anexo III;

b) Memorando sobre daños y perjuicios por violación de la vida privada y autorizaciones explícitas en la legislación estadounidense, que figura en el anexo IV;

c) Carta de la Comisión Federal de Comercio, que figura en el anexo V;

d) Carta del Departamento estadounidense de Transporte, que figura en el anexo VI."[45]

En el anexo de la Decisión 2000/520/CE se recogen los Principios del Puerto Seguro:

- **Notificación**: "Las entidades informarán a los particulares de los fines con los que cuales recogen y utilizan información sobre ellos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales se revelará la información; las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación."
- **Opción**: "Las entidades ofrecerán a los particulares la posibilidad de decidir si su información personal: a) puede divulgarse a un tercero o bien b) puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o no haya sido autorizado posteriormente por el particular. Se deben proporcionar a los particulares mecanismos claros y transparentes, fácilmente disponibles y asequibles para ejercer su derecho de opción."
- **Transferencia ulterior**: "Para revelar información a terceros, las entidades deberán aplicar los principios de notificación y opción. Cuando una entidad desee transferir los datos a un tercero que actué como agente, como se describe en la nota final, podrá hacerlo si previamente se asegura de que este suscribe los principios".
- **Seguridad**: "Las entidades que creen, mantengan, utilicen o difundan información personal tomarán precauciones razonables para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, su modificación y su destrucción."
- **Integridad de los datos**: "De acuerdo con los principios, la información personal debe ser pertinente para los fines con los que se utiliza."
- **Acceso**: "Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona; o cuando puedan vulnerarse los derechos de otras personas."

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

- **Aplicación**: "Una protección eficaz de la vida privada debe incluir mecanismos para garantizar la conformidad con los principios, una vía de recurso para las personas a que se refieran los datos y se vean afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora."[46]

Cuando se aprobó el acuerdo de Puerto Seguro, las empresas estadounidenses no estaban obligadas a cumplir con el acuerdo, sino que podían decidir si preferían mantener su propia regulación y negociar cada uno de los contratos; o, por otro lado, unirse al acuerdo, y con ello, conseguir una aprobación directa, presuponiendo que esas empresas cumplen con las garantías de protección adecuadas. En este caso la empresa Facebook Inc. se hallaba bajo el régimen del *Safe Harbor* al haber aceptado voluntariamente los principios del acuerdo mediante la presentación de la carta al Departamento de Comercio.

Todo parecía indicar que este acuerdo se mantendría en el tiempo y sería el marco regulatorio de las transferencias internacionales de datos, pero en 2013 comenzaron las dudas sobre la seguridad proporcionada por el acuerdo. En la sentencia del TJUE de 6 de octubre de 2015, el Abogado General del TJUE Yves Bot dio a conocer que las autoridades de EE. UU. tenían acceso a los datos personales procedentes de la UE, y, además, no se estaba cumpliendo con lo dispuesto en el artículo 25.1 de la Directiva 95/46: "1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado." Ese nivel de protección adecuado se garantiza en los países terceros cuando es equivalente al establecido en la UE, y en este caso no existían mecanismos de defensa para los ciudadanos afectados. Por todo ello, en la sentencia Schrems I, el TJUE declaró inválida la Decisión 2000/520/CE al no adecuarse a lo dispuesto en la Carta y en la Directiva 95/46.

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

Tras conocer esta sentencia y con el objetivo de proporcionar mayor seguridad a los ciudadanos, el Departamento de Comercio de EE. UU. junto con la Comisión Europea comenzaron a trabajar en un nuevo acuerdo de protección de datos que solucionara los principales problemas del *Safe Harbour*, es decir, frenar la excesiva capacidad de las autoridades publicas de EE. UU. para acceder a los datos europeos, y, por otro lado, incrementar los medios jurídicos de protección ofrecidos a los ciudadanos europeos. De esta manera, tras meses de negociación consiguió aprobarse un nuevo acuerdo en 2016, el *Privacy Shield*.

Si observamos ambos acuerdos detenidamente no existen grandes diferencias entre ellos, el *Privacy Shield* tiene las mismas bases normativas, incluye los siete *Principios del Safe Harbor*, solo que más enfocados en ampliar los derechos de los ciudadanos europeos y limitar las capacidades de las autoridades estadounidenses. Principalmente lo que se incluye en el *Privacy Shield* son nuevos métodos de control, organizaciones pertenecientes a EE. UU.[47] y la UE[48] que supervisarán el nivel de cumplimiento del acuerdo para que no ocurra como con el anterior. También se establecen requisitos más estrictos sobre los registros de los datos, se exige que las empresas que participen en el acuerdo que mantengan informados a las autoridades sobre su política de privacidad y el nivel de cumplimiento de esta.
Y, al igual que con el *Safe Harbor*, el *Privacy Shield* determina que cuando las empresas dejan de participar en el acuerdo deben mantener todos los registros de datos personales protegidos de la misma manera que cuando eran miembros del *Privacy Shield.* Si se realiza una revisión y se observa que están usando los datos de manera contraria a lo establecido en el acuerdo, se les obligará a destruir todos los datos afectados, o asegurar un nivel de protección superior al ofrecido hasta el momento, como, por ejemplo, incluyendo cláusulas contractuales tipo. En último lugar, la última innovación que incluyó el *Privacy Shield* está relacionada con la intención de mejorar los medios de defensa de los ciudadanos europeos. Este nuevo acuerdo incluye varias vías para que los ciudadanos de la UE presenten sus quejas y reclamaciones. Las opciones se basaban en dirigirse ante las propias autoridades de protección de datos de la UE, ante el Defensor del Pueblo de EE. UU., una figura creada a raíz del acuerdo, supuestamente independiente y encargada de resolver los casos en los que los datos personales se han puesto en peligro; por último, como vía excepcional se podía comenzar un proceso de arbitraje ante el *Privacy Shield Panel.*

[47] El Departamento de Comercio, o el Departamento de Transporte, quienes se comprometen a mantener un nivel de cooperación superior al existente con el *Safe Harbor* con las autoridades de la UE.
[48] El Supervisor Europeo de Protección de Datos.

Se pensaba que el Escudo de Privacidad sería el acuerdo definitivo para las transferencias internacionales de datos ya que se intentó superar los puntos débiles del *Safe Harbor*, los cuales se pusieron de relieve con la primera sentencia del TJUE Schrems I en 2015. Años más tarde, en 2018, Mrs. Schrems volvió a poner de relieve ante el Tribunal Supremo de Irlanda que se seguían violando sus derechos fundamentales de los ciudadanos con el *Privacy Shield* porque las autoridades de EE. UU. seguían teniendo acceso a los datos personales procedentes de la UE y, además, los medios de defensa ofrecidos a los ciudadanos europeos eran ineficaces por motivos como la falta de independencia del Defensor del Pueblo.

La High Court volvió a plantear una cuestión prejudicial ante el TJUE para que se juzgara tanto la situación como el acuerdo en sí. Finalmente, el TJUE dictaminó en la sentencia Schrems II que el Escudo de Privacidad quedaba anulado por no garantizar los medios de protección adecuados.

La declaración de invalidez del Privacy Shield trajo consigo el revuelo y la inseguridad en el mercado internacional, teniendo que buscar las alternativas que sustituyeran al Escudo de Privacidad para poder seguir transfiriendo datos a nivel internacional. Esto ha supuesto principalmente el tener que adaptarse a las exigencias del RGPD debido a que las empresas necesitan seguir transfiriendo datos y continuar con su actividad económica comercial. Las empresas también cuentan con las cláusulas contractuales tipo como medio de protección alternativo para transferir datos a nivel internacional, pero como veremos, no son del todo seguras, y no sirven como sustituto al *Privacy Shield*.

3.2.2 Las transferencias internacionales de datos con el Reglamento General de Protección de Datos

En 2016 se aprobó el Reglamento General de Protección de Datos (RGPD) con el objetivo de mejorar la protección y la seguridad en materia de intercambio de datos, y, además, establecer un régimen único de protección para todos los países miembros de la Unión Europea. El RGPD recoge unos nuevos principios de responsabilidad, de protección de datos, y de transparencia que favorecen la compresión para las partes intervinientes en el acuerdo y, también obligan a las empresas a demostrar que se está cumpliendo con las medidas de seguridad adecuadas a través de una serie de nuevas exigencias.

Entre estas exigencias se incluyen evaluaciones de impacto sobre la privacidad, para valorar los posibles riesgos e intentar reducirlos o eliminarlos, si es posible; unas garantías adicionales más severas para las transferencias internacionales de datos; o incluso sanciones económicas[49] para las situaciones donde no se cumplen las normas del RGPD.

Otro aspecto importante del RGPD consiste en tener en cuenta los derechos de los ciudadanos cuyos datos se están viendo perjudicados. Es un punto importante debido a que el anterior acuerdo de protección de datos[50] que fue declarado inválido no incluía los medios de protección a los ciudadanos.

Algunos de los derechos que aparecen en el RGPD son:

- Transparencia e información.
- Consentimiento expreso por parte del ciudadano para poder manejar sus datos personales.
- Derecho al olvido: supone otorgar al ciudadano la posibilidad de eliminar los datos personales que estén circulando por internet.
- Derecho a la limitación del tratamiento.
- Derecho a denunciar y exigir indemnizaciones por daños.[51]

El RGPD establece los medios a través de los cuales se pueden llevar a cabo de forma segura las transferencias internacionales de datos, y son los siguientes:

- Transferencias basadas en una decisión de adecuación, recogido en el artículo 45 RGPD: "Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica."

[49] "Las sanciones económicas que se aplican pueden llegar hasta los 20 millones de euros o el 4% de la facturación global anual" (AEPD.org, 2016).
[50] *Safe Harbor.*
[51] AEPD.org, 2016: *Análisis del RGPD.*

A la hora de elaborar el análisis del nivel de protección de un país, la Comisión atenderá a los requisitos establecido en el "Working document on Adequacy Referential"[52] aprobado en 2017. En él se explica que se examinará el nivel de protección adecuada atendiendo al ordenamiento jurídico propio del país; las competencias de las autoridades de control del país tercero, comprobando que se encargan de garantizar el cumplimiento de las normas relativas a la protección de datos, de facilitar el ejercicio de los derechos de los afectados, y colaboran en la medida de lo posible con las autoridades de la UE; y, por último se atiende a los tratados internacionales ratificados por el país tercero en materia de protección de datos, así como la pertenencia a un organismo internacional dedicado a la protección de datos.

Si la Comisión declara una decisión de adecuación respecto a un determinado país tercero, se permite realizar transferencias internacionales sin necesidad de una autorización expresa. Esto se entiende sin perjuicio de que la situación jurídica cambie y se revoque la decisión de adecuación por parte de la Comisión, lo que supondría la paralización de las transferencias hacia ese país. Algunos de los países que cuentan con estas decisiones son Suiza, Canadá, Argentina, Andorra o Uruguay.

- Transferencias mediante garantías adecuadas, artículo 46 RGPD:

"1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas."

En los siguientes apartados, el artículo 46 diferencia entre:

- Las garantías que no requieren autorización previa:
    - Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
    - Normas corporativas vinculantes de conformidad con el artículo 47.
    - Cláusulas tipo de protección de datos adoptadas por la Comisión.

[52] Se trata de un documento aprobado y redactado por el "Working Party" el 28 de Novimebre de 2018. El "Working Party" se creó con arreglo al artículo 29 de la Directiva 95/46/CE. Se trata de un organismo independiente cuya función es resolver consultas sobre protección de datos y privacidad. En el artículo 30 de la Directiva 95/46/CE se regulan las funciones específicas de este organismo.

- Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión.
- 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.
- 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 a los derechos de los interesados.

- Las garantías que requieren autorización previa:
  - Cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o
  - Disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.[53]

- Excepciones para situaciones específicas, artículo 49 del RGPD:

"1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

> a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

[53] Unión Europea. 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.

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero solo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta."

Es decir, que estas excepciones del artículo 49 del RGPD son aplicables en caso de exista un interés público reconocido con anterioridad por el derecho europeo o nacional, y además si esa transferencia de datos que se incluye en un contrato o reclamación tiene carácter ocasional y necesario. También se recoge en este mismo artículo la posibilidad de que el RGPD permita una determinada transmisión de datos cuando esta no es repetitiva, afecta a un número limitado de interesados y es necesaria respecto a los intereses legítimos del responsable del tratamiento.

3.2.3 Especial referencia a las transferencias internacionales de datos mediante las Cláusulas Contractuales Tipo y las Normas Corporativas Vinculantes del artículo 47 del RGPD.

- Las Cláusulas Contractuales Tipo:

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

La finalidad de las cláusulas contractuales tipo es servir como mecanismo para la transferencia de datos internacionales, en el artículo 1 de la Decisión de Ejecución (UE) 2021/914 se establece que:

"1. Se considera que las cláusulas contractuales tipo establecidas en el anexo ofrecen garantías adecuadas en el sentido del artículo 46, apartado 1 y apartado 2, letra c), del Reglamento (UE) 2016/679 para la transferencia de datos personales por parte de un responsable o encargado del tratamiento sujeto a dicho Reglamento (exportador de datos) a un responsable o (sub)encargado cuyo tratamiento de datos no esté sujeto a dicho Reglamento (importador de datos).

2. Las cláusulas contractuales tipo también establecen los derechos y obligaciones de los responsables y encargados del tratamiento con respecto a las cuestiones a que se refiere el artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 en lo que respecta a la transferencia de datos personales por parte de un responsable a un encargado, o de un encargado a un subencargado."[54]

Las cláusulas contractuales tipo parecen (a priori) una buena solución para la transferencia internacional de datos debido a que según establece la Comisión, estas cláusulas incluyen garantías adecuadas respecto a la vida privada y a los derechos fundamentales de los ciudadanos cuyos datos se transfieren, y por ello el TJUE decidió que seguían siendo válidas. Sin embargo, las cláusulas contractuales tipo, al igual que el *Privacy Shield* no incluyen un nivel de protección similar al ofrecido en la UE debido a que las autoridades estadounidenses pueden tener acceso a los datos.

[54] Unión Europea. Decisión (UE) 2021/914 de la Comisión, de 7 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Tras la sentencia Schrems II se decidió que si las empresas querían usar las cláusulas contractuales tipo como método de protección en las transferencias de datos entre la UE y EE. UU., debían incluir unas garantías adicionales que cubrieran esa intervención de las autoridades estadounidenses. La sentencia del TJUE de 16 de julio de 2020 ha provocado que cada vez se vuelvan más exigentes con las garantías de protección en las transferencias internacionales de datos, algo que se ha incluido en la última modificación de la normativa referente a las cláusulas contractuales tipo. Anteriormente, en la regulación de 2010 y 2016 se establecía una especial protección sobre los datos sensibles, se incluyó la figura de encargado del tratamiento y se exigía que el ciudadano estuviera protegido con las máximas garantías posibles. Actualmente, las novedades que incluye son:

- Cumplimiento y adecuación de los principios establecidos en el RGPD respecto al tratamiento de datos, como es el de transparencia, responsabilidad o exactitud.
- Nuevas formas de transferencia de datos en cuatro situaciones distintas:
    - De responsable a responsable del tratamiento (R – R)
    - De responsable a encargado (R – E)
    - De encargado a responsable (E – R)
    - De encargado a encargado (E – E)
- Las empresas que utilicen las cláusulas tienen la obligación de incluir y explicar en el anexo del contrato cuáles serán las garantías que van a ser utilizadas, es decir, cuál va a ser exactamente el nivel de protección ofrecido en las transferencias de datos internacionales.
- Además, las autoridades nacionales tendrán la competencia para suspender y anular transferencias de datos realizadas mediante cláusulas contractuales tipo cuando las empresas firmantes del contrato no cumplen con lo acordado y ponen el riesgo los derechos del interesado; y en el caso en el que la regulación de EE. UU. suprima las garantías ofrecidas por las cláusulas contractuales tipo.

Por lo tanto, es cierto que las empresas siguen usando las cláusulas contractuales tipo como mecanismo para transferir datos a nivel internacional pero ahora tendrán que tener más cuidado para cumplir con todos los requisitos, sobretodo especial atención sobre la legislación extranjera si no quieren que esa transferencia de datos se prohíba. Todas las transferencias internacionales de datos realizadas mediante cláusulas contractuales tipo deberán ser examinadas antes de ser aprobadas y asegurar que cumplen con todas las garantías.

- Las Normas Corporativas Vinculantes:

Al igual que las cláusulas contractuales tipo, las normas corporativas vinculantes aparecen como medio para transferir datos internacionalmente, se trata de una relación contractual "jurídicamente vinculante aplicable a los miembros de un grupo empresarial[55] o a la unión de empresas dedicadas a una actividad económica conjunta (incluidos los empleados)"[56]. Están reguladas en el artículo 47 del RGPD, donde se establece que se pueden utilizar las normas corporativas vinculantes para ofrecer las garantías adecuadas en la transferencia de datos sin que haga falta una autorización de la autoridad nacional competente en esta materia. Esto se debe a las normas corporativas vinculantes tienen que cumplir previamente con una serie de condiciones para poder ser aprobadas por la autoridad de protección de datos y así, posteriormente ser utilizadas como medios de garantía en las transferencias internacionales de datos[57]. El RGPD establece los elementos que como mínimo deben incluir esas normas corporativas vinculantes en el artículo 47.2, entre ellos se incluye:

- "La estructura y los datos de contacto".
- "Las transferencias o conjuntos de transferencias de datos".
- "La aplicación de los principios generales en materia de protección de datos".
- "La aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión"
- "Los procedimientos de reclamación".
- "Los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control".
- "La formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales".[58]

[55] Los grupos empresariales son son aquellos "constituidos por una empresa que ejerce el control y sus empresas controladas". (AEPD, 2016, "¿Qué son las normas corporativas vinculantes?")
[56] Artículo 47.1 a) RGPD.
[57] Deben cumplir con un nivel de protección tal que se asegure que los datos pueden ser transferidos desde la UE hasta cualquier país extranjero (no solamente EE. UU.) sin que se produzca ninguna violación de los derechos fundamentales de los ciudadanos europeos.
[58] Unión Europea. 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.

La utilidad de las normas corporativas vinculantes radica en la posibilidad de establecer de manera armonizada unos mecanismos referentes a la protección de datos aplicables a todos los contratos que realicen dentro del grupo empresarial. De esta manera se asegura que se están cumpliendo con las garantías exigidas en todas las transferencias de datos personales, sin tener que evaluarlo caso por caso, y, además, se reduce el volumen de trámites burocráticos realizados en cada transferencia realizada desde la UE hasta EE.UU. También van a ser útiles para las empresas del grupo empresarial, quienes tendrán una mejor reputación al incluir entre sus valores la preocupación por cumplir con la protección de los derechos fundamentales de los ciudadanos cuyos datos personales se transfieren.[59]

La sentencia Schrems II también tuvo influencia sobre las normas corporativas vinculantes debido a que se comprobó que la normativa estadounidense también pasaba por encima de las normas corporativas vinculantes y por ello no protegían de manera equivalente a la UE los derechos fundamentales de los ciudadanos durante las transferencias de datos personales. Esto ha derivado en la necesidad de evaluar contrato por contrato el nivel de protección que se está ofreciendo y comprobar que es suficiente y adecuado con respecto a las exigencias del RGPD. En caso de observar alguna posible fisura en el nivel de protección ofrecido, las partes intervinientes en el contrato deben incluir medidas complementarias de garantía, o serán suspendidas por las autoridades nacionales competentes.

A modo de resumen de este apartado podríamos decir siguiendo las palabras de Pedro A. De Miguel Asensio "que el uso de cláusulas contractuales tipo y de normas corporativas vinculantes no exime de la necesidad de valorar si, a la luz de las circunstancias que rodean la transferencia, estos medios de protección de datos cumplen o no con las garantías adecuadas en el país tercero, de manera equivalente a como lo hacen en la UE. En relación con las transferencias entre la UE y EE. UU., las carencias en el sistema jurídico estadounidense que sirven de fundamento en la sentencia a la declaración de invalidez de la Decisión de la Comisión sobre el Escudo de Privacidad parecen poner también en entredicho el que la transferencia pueda tener lugar de modo respetuoso con lo exigido en el RGPD mediante el empleo de clausulas contractuales tipo o normas corporativas vinculantes" [60].

[59] Delegado Protección de datos, 2017.
[60] A. De Miguel Asensio. P, 2020, "Implicaciones de la declaración de invalidez del Escudo de Privacidad", La Ley Unión Europea, Número 84. (p.6)

3.2.4 Una amenaza a las transferencias internacionales de datos: la ley Cloud Act 2018

Las transferencias internacionales de datos conllevan de manera intrínseca un almacenamiento de esos datos, ya que una vez que se transfieren hasta el país tercero se acumulan en la nube[61].

La normativa relativa al almacenamiento de datos ha sido siempre algo difícil de manejar debido a que la tecnología y los servicios digitales están en constante desarrollo, mientras que, la preparación y aprobación de una norma jurídica conlleva su tiempo. El gobierno de EE. UU. ha introducido en 2018 una nueva ley para regular el tratamiento de los datos procedentes de empresas situadas fuera del territorio americano, pero gestionadas por empresas de EE. UU. Esta ley se denomina *CLOUD Act*, siendo "CLOUD" las siglas de "Clarifying Lawful Overseas Use of Data"[62], es decir es una ley que no regula la nube como tal, sino la protección de datos que se da dentro de la nube.

Para la ley *Cloud Act* los datos procedentes de las empresas que están fuera de EE. UU. se tratarán igual que los datos de los servidores americanos, y por ello, dentro del territorio estadounidense pueden ser solicitados por las autoridades nacionales en base a la ley *Cloud Act* siempre que sea bajo alguno de los fines de custodia, control, o investigación de delitos graves. Esto significa que desde la policía local de EE. UU. hasta las agencias federales tienen la posibilidad de pedir a los proveedores de servicios datos de los usuarios y de las empresas tanto de EE. UU. como de fuera del país, y los proveedores deberán entregarlos sin necesidad de que se lo exija un juez.

Conociendo esta información se entiende que haya sido tan criticada puesto que el Privacy Shield fue declarado invalido por la falta de protección y la ley *Cloud Act* permite a cualquier autoridad tener de nuevo acceso a los datos personales. Por lo tanto, la ley *Cloud Act* estaría entrando en conflicto con el RGPD, concretamente con lo dispuesto en los artículos 46 y 48 del mismo donde se establece que "el responsable o encargado del tratamiento transmitirá datos personales solo si se ofrecen las garantías adecuadas, y además, será necesario un acuerdo internacional o un tratado de asistencia jurídica mutua entre la UE y el país tercero

[61] "El almacenamiento en la nube es un servicio que permite almacenar datos transfiriéndolos a través de Internet o de otra red a un sistema de almacenamiento externo que mantiene un tercero" (Microsoft Azure, 2021).

[62] En castellano significa "Aclarando el uso legal de datos en el extranjero". (Carisio, E. 2018).

para que se permita a una autoridad de un país tercero exigir que un responsable le transmita datos personales"[63].

La ley *Cloud Act* supone una clara amenaza para los derechos fundamentales de los ciudadanos europeos, sobre todo el derecho a la privacidad, desestabilizando la normativa de protección de datos de la UE. Las empresas europeas que transfieren datos a EE. UU. se encuentran en una situación tal que si cumplen con la ley *Cloud Act* estarían incumpliendo el RGPD, y viceversa. Para solucionar este problema y acabar con las injerencias de las autoridades estadounidenses en los datos personales de los ciudadanos europeos, lo mejor seria que dentro de la UE tuviéramos nuestra propia plataforma de almacenamiento de datos para las empresas de los países miembros sometida únicamente a las leyes europeas.

4. CASO MAILCHIMP

Desde que se publicó la sentencia Schrems II donde se ponen de relieve los posibles peligros derivados del uso del Privacy Shield como norma para realizar las transferencias de datos internacionales entre la UE y un país tercero, muchas empresas y usuarios europeos han comenzado a revisar detalladamente las políticas de protección de datos ofrecidas por las empresas de EE. UU. En este sentido, lo que buscan los usuarios europeos es que se cumplan con las exigencias del RGPD, es decir que se cumpla con el nivel de protección adecuado, asegurando sus derechos fundamentales.

El primer caso que ha salido a la luz por no cumplir con el RGPD es Mailchimp, una empresa estadounidense usada como herramienta para enviar *newsletter* por correo electrónico dentro de la UE procedentes de países terceros. Un suscriptor de la *newsletter* de *FOGS Magazin* procedente de Alemania denunció ante las autoridades que Mailchimp reenvíaba las direcciones de correo electrónico de los suscriptores sin su consentimiento. De esta manera comenzó un litigio entre *FOGS Magazin* y Mailchimp que finalizó en marzo de 2021 con la sentencia de la Autoridad de Protección de Datos de Baviera confirmando la ilegalidad de los hechos por contradecir lo dispuesto en el artículo 44 del RDGP. Las razones que llevaron a la Autoridad a tomar esa decisión se basan en que Mailchimp no tomó ninguna medida complementaria para acabar con las interferencias de las autoridades de EE. UU. en las transferencias de datos, a pesar de ser algo obligatorio desde la sentencia Schrems II.

[63] Unión Europea. 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.

Además, las transferencias de datos de Mailchimp desde la UE hasta EE. UU. se basaban en cláusulas contractuales tipo, las cuales necesitan garantías complementarias si no cumplen con un nivel de protección adecuado, y en este caso la revista alemana descubrió que no existía esa protección. Como de momento no se ha aprobado ninguna normativa internacional que sustituya al Privacy Shield como ley marco de protección de datos, las empresas europeas se basan en el RGPD en relación con la transferencia de datos seguras. Por ello, siguiendo este Reglamento deben asegurarse de que las empresas americanas están certificadas por el RGPD y que han establecido medidas complementarias para proteger los datos personales.

A raíz de la sentencia de la Autoridad de Protección de Datos de Baviera, Mailchimp ha decido introducir cambios en su empresa y mejorar su compromiso con el RGPD mediante formularios de consentimiento y herramientas como la administración de los perfiles para que los usuarios decidan que información quieren transmitir y cuál mantener al margen o eliminar. Dentro de la página web de Mailchimp se ha creado un apartado donde se explican todas las medidas que han introducido para cumplir con el RGPD:

"¿Qué hace Mailchimp para cumplir con el RGPD?

- Ha designado a un Delegado de Protección de Datos para supervisar nuestro programa de cumplimiento.
- Revisar continuamente nuestras medidas de seguridad para asegurarnos de que cualquier dato personal que recopilemos y tratemos en nuestros sistemas esté adecuadamente protegido.
- Asegurarnos de que nuestra Política de Privacidad explique claramente el compromiso de Mailchimp con el RGPD, sea transparente en cuanto a cómo utilizamos los datos personales y dé a las personas información sobre cómo pueden ejercer sus derechos como titulares de los datos.
- Proporcionar a nuestros clientes condiciones que cumplan con el RGPD en nuestro Anexo de Tratamiento de Datos y actualizar nuestros contratos con proveedores externos para garantizar que cumplen con el RGPD.
- Mantener procesos formales en torno a los derechos de los titulares de los datos para garantizar que podamos ayudar a los clientes a cumplir las solicitudes que reciben.
- Completar las evaluaciones del impacto de la protección de datos para identificar y minimizar cualquier riesgo derivado de nuestras actividades de tratamiento de datos.
- Mantener registros precisos de nuestras actividades de tratamiento de datos, tanto como encargados de los datos personales como responsables los mismos.

- Prestar mucha atención a las pautas normativas en torno al cumplimiento del RGPD y realizar cambios en las características de nuestros productos y contratos cuando sea necesario."[64]

Esta iniciativa de Mailchimp es un buen comienzo hacia el objetivo planteado en la sentencia Schrems II, conseguir que todas las transferencias de datos entre la UE y EE. UU. sean seguras y no violen ningún derecho fundamental. Todas las empresas americanas deberían seguir estos pasos e introducir nuevas medidas orientadas a cumplir con el RGPD, aunque por el momento es algo complicado debido a que la legislación estadounidense sigue permitiendo a las autoridades interferir en las transferencias de datos con leyes como la *Cloud Act*.

[64] Mailchimp, 2021. *Con Mailchimp es muy fácil cumplir con el RGPD.*

5. CONCLUSIONES

Gracias a la sentencia Schrems I y, en especial Schrems II hemos descubierto la verdadera realidad detrás de las transferencias internacionales de datos. Una realidad que no es favorable para los ciudadanos cuyos datos se transfieren ya que, como hemos visto al comienzo del trabajo la sentencia Shcrems I terminó con la declaración de invalidez del *Safe Harbor* y, Schrems II acabó con su sustituto, el *Privacy Shield*. Las razones que llevaron a la Gran Sala del TJUE a invalidar estas normas radican en la falta de protección ofrecida a los ciudadanos europeos por parte de los países terceros destinatarios de las transferencias de datos, en términos generales, el nivel de protección no era el adecuado, no se ajustaba al establecido en la UE. A pesar de que se intentaron superar las deficiencias del *Safe Harbor* con el *Privacy Shield*, el TJUE determinó que tampoco era suficiente como escudo de protección de datos. Estas normas no consiguieron cubrir los principales problemas, por un lado, la extrema vigilancia, control y manipulación de los datos personales de los ciudadanos europeos por parte de las autoridades de EE. UU. y, por otro lado, la falta de medios jurídicos ofrecidos en EE. UU. a los ciudadanos europeos afectados por la violación de su derecho a la privacidad, es decir, incumplimiento del derecho a la tutela judicial efectiva.

Del mismo modo, se puso de manifiesto que las cláusulas contractuales tipo y las normas corporativas vinculantes no son medios de protección suficientes por sí solos, necesitan medidas complementarias que garanticen un nivel de protección adecuado, equivalente al de la UE. En cuanto a las cláusulas contractuales tipo fueron declaradas válidas en la sentencia Schrems II, pero hemos visto como su regulación de 2010 se ha quedado obsoleta y ha sido necesaria una actualización, la cual se recoge en la regulación de 2021.

Es cierto que, crear una normativa que regule el derecho a la vida privada digital es muy complicado debido a que controlar todos los datos que se están transfiriendo continuamente es prácticamente imposible, además, el ritmo de desarrollo de las innovaciones tecnológicas es difícil de seguir desde un punto de vista jurídico. A pesar de ello, se ha intentado crear leyes para proteger la privacidad de los usuarios, y garantizar que su información personal siga manteniéndose dentro de su ámbito privado, sin que los servicios digitales se apropien de esa información.

Aparte de la dificultad derivada de las nuevas tecnologías, también hay que tener en cuenta las diferencias existentes entre la UE y EE. UU. en cuanto a la protección de datos. A nivel europeo se creó el RGPD para garantizar a las personas el derecho a la protección de la privacidad de los agentes comerciales y los gobiernos. Son conscientes del poder que tienen las autoridades nacionales estadounidenses para interferir en las transferencias de datos y también de la influencia de las grandes empresas como Facebook, con un gran control sobre el mercado, ya que tienen la capacidad de recopilar y transferir numerosos datos personales. Las intenciones de la UE se dirigen a frenar esas situaciones a través de la aplicación estricta del RGPD, el control aplicado por las Autoridades de Protección de Datos y, la aplicación de medidas como la Recomendación 01/2020.

Por su parte, EE. UU. ha combinado los avances en la protección de datos con una legislación que permite la vigilancia y el control sobre los datos personales procedentes de la UE como un medio para garantizar supuestamente la seguridad nacional de sus ciudadanos. Algo que podemos ver claramente en la ley *Cloud Act* de 2018 donde se permite a las autoridades nacionales tener competencias para exigir que se les entreguen datos personales procedentes de empresas de fuera del territorio estadounidense.

Por lo que vemos, aunque la protección del derecho a la vida privada es un objetivo para la UE y EE. UU., la iniciativa de la UE es más amplia que la de EE. UU. ya que, el país americano se centra en sus propios intereses y los de sus ciudadanos, sin tener en cuenta al resto. Si la intención de ambos territorios es continuar con las relaciones comerciales necesitan una nueva ley de protección de datos armonizada que asegure la protección de todos los ciudadanos y mejore la cooperación entre ambos territorios.

6. BIBLIOGRAFÍA

Anexo normativo:

Agencia Española de Protección de Datos. (2018). DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO. AEPD. Disponible en https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf [consulta: 06/20/2021]

Data Protection Working Party (2017). Article 29 Working Party Adequacy Referential. Adopted on 28 November *2017. WP 254 rev.01.* Disponible en https://ec.europa.eu/newsroom/article29/items/614108/en [consulta: 07/05/2021]

Unión Europea (2000). Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de la Unión Europea. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12016P/TXT&from=DE [consulta: 06/15/2021]

Unión Europea. (2000). Decisión 2000/520 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. Disponible en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32000D0520 [consulta: 06/15/2021]

Unión Europea. (2016). 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. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016D1250 [consulta: 06/16/2021]

Unión Europea. (2021). Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Disponible en https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80739 [consulta: 07/09/2021]

Unión Europea. (2016). 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. Disponible en https://eur-lex.europa.eu/eli/dec_impl/2016/2297/oj/spa [consulta: 06/17/2021]

Unión Europea. (1995) 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. Disponible en https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678 [consulta: 06/17/2021]

Unión Europea. (2020). Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE. European Data Protection Board. Disponible en https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf [consulta: 06/22/2021]

Unión Europea. (2016) 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). Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf [consulta: 06/22/2021]

Anexo jurisprudencial:

Curia Europa. (2019). *CONCLUSIONES DEL ABOGADO GENERAL SR. HENRIK SAUGMANDSGAARD ØE presentadas el 19 de diciembre de 2019*. EURLEX. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62018CC0311&from=ES [consulta: 06/15/2021]

Unión Europea. (2015). SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 6 de octubre de 2015. Asunto *C-362/14*. InfoCuria. Disponible en https://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES [consulta: 06/14/2021]

Unión Europea. (2019). Conclusiones del Abogado General en el asunto C-311/18 Data Protection Commissioner/Facebook Ireland Limited, Maximilian Schrems. Curia Europa. Disponible en https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165es.pdf [consulta: 06/15/2021]

Artículos y páginas web consultadas:

Agencia Española de Protección de Datos. (2021). *TRANSFERENCIAS INTERNACIONALES*. AEPD. Disponible en https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales [consulta: 06/22/2021]

Agencia Española de Protección de Datos. (2016). "¿Qué son las normas corporativas vinculantes?". Disponible en https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00050 [consulta: 06/22/2021]

Aparicio, J. (2020). *Las empresas deben resolver el problema de la sentencia de Schrems II*. Cotizalia. Disponible en https://blogs.elconfidencial.com/mercados/tribuna-mercados/2020-11-17/empresas-deben-resolver-problema-sentencia-schrems_2835016/ [consulta: 06/20/2021]

Asociación de Empresas de Protección de Datos (2016). *RGPD - Reglamento General de Protección de datos. Análisis del RGPD*. Disponible en https://rgpd.es [consulta: 07/05/2021]

Ayudaley. (2019). *Privacy Shield: ¿qué es y qué significa para los usuarios?* Ayuda ley protección de datos. Disponible en https://ayudaleyprotecciondatos.es/2020/07/09/privacy-shield/#Opiniones_sobre_Privacy_Shield [consulta: 06/15/2021]

Bevan, O., Mikkelsen, D. and Soller, H. (2021). *International personal-data transfer amid regulatory upheaval.* [online] McKinsey & Company. Disponible en: https://www.mckinsey.com/business-functions/risk/our-insights/international-personal-data-transfer-amid-regulatory-upheaval# [consulta 06/25/2021]

Carisio. E. (2018). *Qué es la CLOUD Act, y cómo afecta a la privacidad de los datos*. Blog MediaCloud. Disponible en https://blog.mdcloud.es/cloud-act/ [consulta: 07/08/2021]

ClickDatos. (2018). *El papel del Safe Harbor en las transferencias de datos*. ClickDatos. Disponible en https://clickdatos.es/el-papel-del-safe-harbor-en-las-transferencias-de-datos/ [consulta: 06/11/2021]

Cloud Computing. (2019). *¿Cómo afecta la Ley Cloud Act a las empresas europeas?* Computing. Disponible en https://www.computing.es/seguridad/noticias/1113879002501/afecta-ley-cloud-act-empresas-europeas.1.html [consulta 07/08/2021]

Comisión Europea (2016). *¿Qué son las autoridades de protección de datos (APD) y cómo puedo ponerme en contacto con ellas?* Web oficial de la Unión Europea. Disponible en https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/redress/what-are-data-protection-authorities-dpas-and-how-do-i-contact-them_es [consulta: 06/20/2021]

De Miguel Asensio. P. A., 2020, *Implicaciones de la declaración de invalidez del Escudo de Privacidad.* La Ley Unión Europea, Número 84. (p.6). Disponible en https://eprints.ucm.es/id/eprint/62504/1/PADemiguelAsensio%20LaLey%20UE%20n%2084%2009.20.pd [consulta: 07/08/2021]

Delegado Protección de datos. (2017). *Las normas corporativas vinculantes y el RGPD*. Disponible en https://www.delegadoprotecciondatos.com/normas-corporativas-vinculantes-rgpd/#Finalidad [consulta: 07/08/2021]

El delegado de protección de datos. (2019). *Autoridad de Control*. Obtenido de Protección de datos y privacidad. Disponible en https://www.eldelegadodeprotecciondedatos.com/autoridad-de-control/ [consulta: 06/20/2021]

European Data Protection Board. (2020). *Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 — Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems*. EDPB. Disponible en https://www.aepd.es/sites/default/files/2020-08/faqs-sentencia-SCHREMS-II-es.pdf [consulta: 07/08/2021]

European Data Protection Board. (2020). *CEPD. Quiénes somos*. Web oficial de la Unión Europea. Disponible en https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en [consulta: 06/22/2021]

European Data Protection Supervisor. (2020). *Strategy for EU institutions to comply with "Schrems II" Ruling*. Web oficial de la Unión Europea. Disponible en https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en [consulta: 06/22/2021]

Equipo PSN Sercon (2021). *USAR MAILCHIMP ES ILEGAL SEGÚN LA AUTORIDAD ALEMANA DE PROTECCIÓN DE DATOS*. Blog PSN. Disponible en https://blog.psnsercon.com/usar-mailchimp-es-ilegal-segun-la-autoridad-alemana-de-proteccion-de-datos/ [consulta: 07/09/2021]

Fuentes Máiquez, A. (2021). *Comentario de la STJUE de 16 de julio de 2020, C-311/18 (Schrems II)*. Revista Comillas. Disponible en https://revistas.comillas.edu/index.php/revistaicade/article/view/14901/13893#toc [consulta: 06/15/2021]

García Escobar. E & Ortega Giménez. A (2021). *Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 («Schrems II»)*. Laleydigital. Disponible en https://buc-uva.alma.exlibrisgroup.com/infra/docDeliveryDownload [consulta: 06/28/2021]

Gavetti. J.H. (2018). *La Cloud Act, una amenaza para la privacidad de los ciudadanos y las empresas europeas*. EL PAÍS. Disponible en https://elpais.com/retina/2018/08/01/tendencias/1533121170_040578.html [consulta: 07/08/2021]

Guías Jurídicas. (2020). *Transferencia internacional de datos (Protección de Datos)*. Guías Jurídicas. Disponible en https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjEwNjE7Wy1KLizPw8WyMDQwsDU0OwQGZapUt-ckhlQaptWmJOcSoA6fqAajUAAAA=WKE#I236 [consulta: 06/22/2021]

Internet Society. (n.d.). *¿Qué es el cifrado?* Internet Society. Disponible en https://www.internetsociety.org/es/encryption/what-is-encryption/ [consulta: 06/14/2021]

Johansson, L. (2014). *No Transfer, No Trade* [the Importance of Cross-Border Data Transfers for Companies Based in Sweden]. Kommerskollegium. The National Board of Trade. Disponible en https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf [consulta: 06/25/2021]

Kovacsics, P. (2018). *Everything you need to know about a Data Processing Agreement*. Tresorit. Disponible en https://tresorit.com/blog/everything-you-need-to-know-about-a-data-processing-agreement/ [consulta: 06/14/2021]

LaFever, G. (2021). *Schrems II: DPAs in Germany Begin Compliance Checks - Other Jurisdictions Soon to Follow*. Linkedin. Disponible en https://www.linkedin.com/pulse/schrems-ii-dpas-germany-begin-compliance-checks-other-gary-lafever [consulta: 06/20/2021]

Maldonado. E (2020): *Bridging the gap in transatlantic data protection*, Discussion Paper, No. 4/20, Europa-Kolleg Hamburg, Institute for European Integration, Hamburg. Disponible en https://www.econstor.eu/bitstream/10419/224928/1/1734852224.pdf [consulta: 07/08/2021]

Mailchimp (2021). *Con Mailchimp es muy fácil cumplir con el RGPD*. Mailchimp. Disponible en https://mailchimp.com/es/gdpr/ [consulta: 07/09/2021]

Méndez de Vigo. P & Monclús. J (2021). *TRANSFERENCIAS INTERNACIONALES DE DATOS: YA ESTÁN AQUÍ LAS NUEVAS CLÁUSULAS CONTRACTUALES TIPO*. Blog Cuatrecasas. Disponible en https://blog.cuatrecasas.com/propiedad-intelectual/transferencias-internacionales-datos-estan-aqui-clausulas-contractuales-tipo/ [consulta: 07/08/2021]

Mendoza Losana, A. I. (2015). *TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES: ESTADOS UNIDOS NO ES UN PUERTO SEGURO, PERO TAMPOCO UNA ISLA INALCANZABLE1*. Centro de Estudios de Consumo. Universidad de Castilla-La Mancha. Disponible en https://blog.uclm.es/cesco/files/2015/10/Transferencias-internacionales-de-datos-personales_Estados-Unidos-no-es-un-puerto-seguro-pero-tampoco-una-isla-inalcanzable.pdf [consulta: 06/13/2021]

Montero Díaz, E. (2020). *¿Qué son las SCC o Cláusulas Contractuales Tipo?*. Ilp ABOGADOS. Disponible en https://www.ilpabogados.com/que-son-las-scc-o-clausulas-contractuales-tipo/ [consulta: 07/08/2021]

Morales Martín, T. (2015). *El Puerto Seguro ya no es tan seguro*. PRODAT. Disponible en https://www.prodat.es/blog/el-puerto-seguro-ya-no-es-tan-seguro/ [consulta: 06/20/2021]

Microsoft Azure (2021). *¿Qué es el almacenamiento en la nube?* Microsoft Azure. Disponible en https://azure.microsoft.com/es-es/overview/what-is-cloud-storage/ [consulta: 07/08/2021]

Negro, A., & Méndez de Vigo, P. (2020). *SENTENCIA SCHREMS II: PRIMERAS DECLARACIONES DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS*. Cuatrecasas. Disponible en https://blog.cuatrecasas.com/propiedad-intelectual/sentencia-schrems-ii-primeras-declaraciones-autoridades-proteccion-datos/ [consulta: 06/27/2021]

Noyb. (2020). *Transferencias de datos entre la UE y los Estados Unidos*. Noyb. Disponible en https://noyb.eu/es/proyecto/transferencias%20de%20eeuu-us [consulta: 06/20/2021]

ONTIER. (2021, 10 02). *ASUNTO C-311/18 "SCHREMS II": GUÍA SOBRE TRANSFERENCIAS INTERNACIONALES E INTERROGANTES ACTUALES EN RELACIÓN CON LAS TRANSFERENCIAS A TERCEROS PAÍSES*. Boletín Digital Las. Disponible en https://es.ontier.net/ia/boletin-xvi-schrems-ii-y-faqs-tis.pdf [consulta: 06/11/2021]

Ortega Giménez, A. (2014). Privacidad y Seguridad en Internet. *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, (97). Disponible en https://telos.fundaciontelefonica.com/archivo/numero097/ [consulta: 06/20/2021]

Owen. (2019). *Safe Harbor Vs. The EU-US Privacy Shield*. Otava. Disponible en https://www.otava.com/reference/how-does-safe-harbor-compare-to-the-eu-us-privacy-shield/ [consulta: 06/20/2021]

Padín, A. (2020). *El Tribunal de Justicia de la Unión Europea anula el Escudo de Privacidad ('Privacy Shield')*. Garrigues. Disponible en https://www.garrigues.com/es_ES/noticia/tribunal-justicia-union-europea-anula-escudo-privacidad-privacy-shield [consulta: 06/29/2021]

Peruzzotti, M. (2020). *El caso Schrems II y sus implicancias en la región app*. Disponible en https://iapp.org/news/a/el-caso-schrems-ii-y-sus-implicancias-en-la-region/ [consulta: 06/22/2021]

Privacy Law & Business. (2020). *Finland queries businesses about their Schrems II compliance*. Privacy Law. Disponible en https://www.privacylaws.com/news/finland-queries-businesses-about-their-schrems-ii-compliance/ [consulta: 06/20/2021]

PymeLegal (2021). Nuevas clausulas contactuales tipo de la CE relativas a la Transferencia Internacional de Datos. PymeLegal. Disponible en https://www.pymelegal.es/noticias/rgpd/nuevas-clausulas-contractuales-tipo-de-la-ce-relativas-a-la-transferencia-internacional-de-datos [consulta: 07/08/2021]

R. Aguiar, A. (2021). *Europa abre una investigación sobre el uso que hacen sus instituciones de las nubes de Amazon o Microsoft por las transferencias de datos a EE. UU.*. Business Insider. Disponible en https://www.businessinsider.es/ue-investiga-como-estan-usando-nubes-microsoft-amazon-873123 [consulta: 06/22/2021]

Recio Gayo, M. (2020, 10 1). *Transferencias Internacionales de datos tras Schrems II, retos y conclusiones preliminares*. ELDERECHO.COM. Disponible en https://elderecho.com/transferencias-internacionales-datos-tras-schrems-ii-retos-conclusiones-preliminares [consulta: 06/11/2021]

Rojas Jiménez, L. (2021). *Las complicaciones derivadas de Schrems II*. Legal Army. Disponible en https://www.legalarmy.net/las-complicaciones-derivadas-de-schrems-ii/ [consulta: 06/22/2021]

Secure Privacy. (2020). *EDPB Schrems II Guidance: GDPR Data Transfers to Third Countries*. Secure Privacy. Disponible en https://secureprivacy.ai/blog/edpb-schrems-ii-guidanc [consulta: 06/22/2021]

Teguayco PInto. (2019, 10 09). *El legado de Snowden: las filtraciones que transformaron internet*. EL PAIS. Disponible en https://elpais.com/tecnologia/2019/10/07/actualidad/1570455695_974155.html [consulta: 06/11/2021]

Tribunal de Justicia de la Unión Europea. (2015). *El Tribunal de Justicia declara inválida la Decisión de la Comisión que declaró que Estados Unidos garantiza un nivel de protección adecuado de los datos personales transferidos*. COMUNICADO DE PRENSA no 117/15. Disponible en https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf [consulta: 06/14/2021]

Tripolis (2021). *Usar Mailchimp infringe el GDPR*. Tripolis. Disponible en https://www.tripolis.com/es/usar-mailchimp-infringe-el-gdpr/ [consulta: 07/09/2021]

Uría Gavilán, E. (2016). Derechos fundamentales *versus* vigilancia masiva. *Revista de Derecho Comunitario Europeo,* 53, 261-282. Disponible en http://dx.doi.org/10.18042/cepc/rdce.53.07 [consulta: 07/09/2021]