Icade. Revista de la Facultad de Derecho | nº 110 | 1-10 [julio-diciembre 2020] [ISSN 2341-0841]
DOI: 10.14422/icade.i110.y2020.009

COMENTARIO DE LA STJUE DE 16 DE JULIO DE 2020, C-311/18 (SCHREMS II)

Commentary on the Resolution of the Court of Justice of EU C-311/18 (Schrems II), 16th July 2020

Antonio Fuentes Máiquez
Alumno Colaborador en el Área de Derecho Internacional Privado
Universidad Pontificia Comillas
E-mail: afuentesmaiquez@alu.comillas.edu

Autor

Las empresas establecidas en la Unión Europea (UE) que transferían datos personales de ciudadanos europeos a entidades estadounidenses solían hacerlo empleando el *Privacy Shield* como marco legal, una decisión de la Comisión Europea que garantizaba la existencia de un nivel de protección de datos adecuado en Estados Unidos. Sin embargo, en julio de 2020 el Tribunal de Justicia de la Unión Europea (TJUE) invalidó esta decisión, generando incertidumbre en muchas de estas empresas. En este comentario se pretende analizar cuáles son las principales consecuencias de esta sentencia y qué alternativas tienen ahora las empresas de la UE.

Companies stablished in the European Union (EU) which used to transfer personal data of European citizens to American entities used to do so using the Privacy Shield as a legal framework, a decision of the European Commission that guaranteed the existence of an adequate level of data protection in the United States. However, in July 2020 the European Court of Justice invalidated this decision, creating uncertainty in many of these companies. This commentary aims to analyze what the main consequences of this ruling are and what alternatives EU companies now have.

Resumen

Privacy Shield; cláusulas tipo de protección de datos; datos personales; Schrems; transferencias; Unión Europea; Estados Unidos; nivel de protección

Privacy shield; standard data protection clauses; personal data; Schrems; transfers; European Union; United States; level of protection

Key words

Recibido: 20/11/2020. Aceptado: 03/12/2020

Fechas

1. Introducción

La Sentencia del Tribunal de Justicia de la UE (STJUE) de 16 de julio de 2020, C-311/18 (Schrems II) invalidó la Decisión 2016/1250 de la Comisión (conocida como *Privacy Shield*).

Esta decisión sustituía a la Decisión 2000/520 (conocida como *Safe Harbour*), que fue invalidada en la STJUE de 6 de octubre de 2015, C-362/14 (Schrems I). De esta forma, las transferencias de datos personales entre empresas establecidas en la UE[1] y entidades estadounidenses han quedado en cierto modo desprotegidas, al no existir una decisión de adecuación de la Comisión que garantice un nivel de protección adecuado en Estados Unidos.

Los efectos de la sentencia Schrems II recaen sobre un gran número de empresas de la UE que solían transferir datos personales a empresas estadounidenses bajo el amparo de este instrumento jurídico. Es por ello por lo que conviene identificar cuáles son las principales consecuencias de su invalidación y qué alternativas pueden ser utilizadas.

2. Hechos principales

Los hechos que dan origen a este litigio se remontan al 25 de junio de 2013, momento en el que el Sr. Schrems, nacional austriaco residente en Austria, interpuso una reclamación ante la Comisión solicitando que prohibiese a Facebook Ireland transferir datos personales a Facebook Inc., establecida en los Estados Unidos. Dicha pretensión se fundaba en la deficiente protección de los datos personales frente al acceso de las autoridades públicas estadounidenses. Inicialmente la reclamación fue desestimada por la Comisión basándose en la existencia del *Safe Harbour*, una decisión de adecuación dictada por la Comisión a la luz del artículo 45 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD), mediante la que garantizaba la existencia de un adecuado nivel de protección de los datos personales en Estados Unidos.

Sin embargo, el Sr. Schrems recurrió ante el Tribunal Superior de Irlanda y este planteó una cuestión prejudicial al TJUE en relación con la validez del *Safe Harbour*. Es entonces cuando se invalidó dicha Decisión mediante la sentencia Schrems I y se sustituyó por el *Privacy Shield*.

La consecuencia de Schrems I fue la anulación de la desestimación de la reclamación inicial ante la Comisión y la interposición de una reclamación modificada por parte del Sr. Schrems en diciembre de 2015, alegando, además del escaso nivel de protección, que la Decisión 2016/2297 (conocida como Decisión CPT), que incluye las cláusulas tipo de protección de datos empleadas por Facebook Ireland, no era una garantía suficiente para permitir la transferencia de datos a los Estados Unidos, pues en su territorio existen programas de vigilancia que permiten a sus autoridades acceder a los datos, lo que atentaría contra los artículos 7, 8 y 47 de la Carta de Derechos Fundamentales de la Unión Europea.

En mayo de 2016 la Comisión, ante la sospecha de una posible invalidez de la Decisión CPT, se personó ante el Tribunal Superior de Irlanda para que este plantease una cuestión prejudicial al TJUE, lo que finalmente hizo en mayo de 2018.

1 El Reglamento General de Protección de Datos (RGPD) se aplica a: el tratamiento de datos personales por parte de un responsable con establecimiento en la Unión Europea; al tratamiento de datos personales de interesados que residan en la Unión por parte de responsables establecidos fuera de esta cuando (a) se dé una oferta de bienes o servicios en la Unión (b) o se produzca un control de su comportamiento en la Unión; y al tratamiento que se dé en un lugar fuera de la Unión donde sea de aplicación el Derecho de la Unión en virtud del Derecho Internacional Público (artículo 3 RGPD).

Junto a la petición, el Tribunal Superior de Irlanda, adjuntó una sentencia de octubre de 2017 que contenía las claves de los posibles motivos de invalidez de la Decisión CPT en el ámbito del procedimiento nacional. En concreto, se refería a 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.

Además, el Tribunal Superior de Irlanda indicó que el acceso a los datos personales que pueden llevar a cabo las autoridades de los Estados Unidos encuentra como único límite que se busque la mayor adaptación posible del tratamiento al fin que se persigue. Por último, destacó la ausencia de una tutela judicial efectiva, pues el acceso a los tribunales estadounidenses por parte de ciudadanos europeos se hacía prácticamente imposible a causa de la legislación vigente.

En este contexto, el Tribunal Superior de Irlanda planteó once cuestiones prejudiciales que son resueltas por el TJUE en la sentencia Schrems II, tal y como veremos a continuación.

3. Cuestiones jurídicas

El Tribunal Superior de Irlanda pregunta, en primer lugar, si una transferencia de datos entre una empresa de la UE y otra establecida en un tercer país, cuando estos datos pueden ser tratados por las autoridades de este país, está comprendida dentro del ámbito de aplicación del RGPD, en base a su artículo 2.1. y 2.2.

El TJUE indica que, tal y como se afirmaba en la sentencia Schrems I, una transferencia de datos de un Estado de la UE a un tercer país ha de ser considerada un tratamiento de datos personales, ya que el concepto de *tratamiento* hace referencia a cualquier operación realizada sobre datos personales (art. 4.2 RGPD) (párrafo 41 Schrems I). Por otro lado, el hecho de que estos datos puedan ser tratados por las autoridades del país tercero por motivos de seguridad no lo excluye del ámbito de aplicación del Reglamento (párrafos 81 a 89, Schrems II).

En las cuestiones prejudiciales segunda, tercera y sexta el Tribunal Superior de Irlanda pregunta cuál es el nivel de protección exigido por el artículo 46.1 y 46.2 RGPD para una transferencia de datos personales basada en cláusulas tipo de protección de datos.

Ante esto, el TJUE indica que, por un lado, podrá determinarse el nivel de protección adecuado mediante una decisión de la Comisión Europea en la que se afirme que un tercer país ofrece un nivel de protección equivalente al garantizado por la UE en dicho Reglamento (art. 45.1 RGPD); y, por otro lado, en caso de no existir una Decisión de este tipo, el responsable o el encargado del tratamiento deberá añadir las garantías necesarias para poder asegurar, igualmente, que el nivel de protección de los datos transferidos será equivalente al ofrecido por la UE (párrafos 90 a 101, Schrems II).

Además, en cuanto a los elementos que se han de observar para comprobar si se da un adecuado nivel de protección, estos serán las estipulaciones contractuales entre el responsable o el encargado del tratamiento en la UE y el destinatario de la transferencia, así como la legislación del tercer país cuyas autoridades podrían acceder a los datos (párrafo 104, Schrems II).

Posteriormente, en la octava cuestión prejudicial se pregunta al TJUE si la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos entre un país de la UE y un país tercero basada en cláusulas tipo de protección de datos cuando considere que dichas cláusulas no se pueden cumplir.

En este sentido, la autoridad competente deberá suspender o prohibir una transferencia en dichas circunstancias si no lo hacen el responsable o el encargado del tratamiento establecidos en la UE y la protección garantizada por el RGPD para los tratamientos en la UE no puede lograrse por otros medios (párrafo 148 conclusiones Abogado General, Schrems II).

Por otro lado, mediante las cuestiones prejudiciales séptima y undécima, el Tribunal Superior de Irlanda pregunta acerca de la validez de la Decisión CPT, cuestionada por el hecho de que las cláusulas tipo de protección de datos que recoge no son vinculantes para las autoridades de terceros países, lo que impide un adecuado nivel de protección.

El TJUE indica que, si bien es cierto que las cláusulas tipo de protección de datos solo son vinculantes para el responsable del tratamiento de los datos en la UE y para el destinatario de un país tercero, y no para las autoridades de dicho país, esto no implica la invalidez de la Decisión CPT (párrafo 125, Schrems II). De hecho, el artículo 46.1 RGPD establece que, a falta de una decisión de adecuación, será el responsable o encargado de protección de datos el que decida si es necesario añadir garantías adicionales a las cláusulas tipo para garantizar el nivel de protección adecuado (párrafo 128, Schrems II).

Además, el responsable o encargado del tratamiento en la UE y el destinatario en el país tercero están obligados a comprobar que el cumplimiento de las cláusulas tipo de protección de datos y, en su caso, de las garantías adicionales es viable. Si el destinatario comprueba la imposibilidad de dicho cumplimiento deberá informar al encargado o responsable en la UE y este tendrá que suspender la transferencia o rescindir el contrato, tal y como establece la cláusula 5 b) de la propia Decisión CPT (párrafos 141 y 142, Schrems II).

Por último, en la cuestión prejudicial novena se solicita al TJUE que informe sobre si una autoridad de control de un Estado miembro está vinculada por el *Privacy Shield*. Además, las cuestiones prejudiciales cuarta, quinta y décima cuestionan la validez de esta Decisión, preguntando en concreto por el Defensor del Pueblo en el marco del *Privacy Shield*.

El TJUE indica que las autoridades de control estatales no tienen competencia para suspender o prohibir una transferencia de datos personales a una entidad adherida al *Privacy Shield* por considerar que no garantiza el nivel de protección suficiente mientras que no se declare la invalidez de este. No obstante, si un particular presenta una reclamación, la autoridad de control podrá interponer un recurso ante los tribunales nacionales y estos deberán plantear una cuestión prejudicial ante el TJUE (párrafos 156 y 157, Schrems II).

En cuanto a la validez del *Privacy Shield*, queda probado que la comunicación de los datos personales a una autoridad pública atenta contra los principios consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. En concreto, el artículo 8 exige el consentimiento del afectado o un fundamento legítimo previsto por ley para poder tratar los datos personales. Además, el artículo 52.1 establece que cualquier limitación a estos derechos deberá ser necesaria y de interés general. Por lo tanto, cualquier norma que limite estos derechos ha de especificar las circunstancias y las exigencias con las que se podría llevar a cabo un tratamiento de los datos de forma que no se sobrepase nunca lo estrictamente necesario (párrafo 176, Schrems II).

Si se atiende a las injerencias que pueden llevar a cabo las autoridades de los Estados Unidos mediante sus programas de vigilancia, se observa que no se establecen límites a las mismas ni garantías para no nacionales afectados. Por lo tanto, estas injerencias no cumplirían con los principios de proporcionalidad e irían más allá de lo estrictamente necesario (párrafo 184, Schrems II).

Además, el artículo 47 de la Carta garantiza la tutela judicial efectiva para cualquier persona que vea dañados los derechos y libertades que le proporciona el Derecho de la Unión, algo que pretende lograrse con la creación del Defensor del Pueblo en el marco del *Privacy Shield*. Sin embargo, esta figura es nombrada por el Secretario de Estado, al que informa directamente, lo que pone en entredicho su independencia. Unido a ello, tal y como indica el Abogado General en el punto 338 de sus conclusiones y el TJUE en el párrafo 196 de la sentencia, las decisiones del Defensor del Pueblo no son vinculantes, por lo que no se logra una tutela judicial efectiva mediante el mismo.

Aunque el Abogado General considera en el punto 186 de sus conclusiones que el TJUE no debe pronunciarse sobre la validez del *Privacy Shield*, decide hacer un examen de carácter subsidiario e indica en el punto 342 que existen serias dudas sobre la validez del *Privacy Shield*.

Finalmente, el TJUE sí decide pronunciarse, invalidando el *Privacy Shield*, así como sus efectos, ya que considera que esto no genera un vacío legal, pues el RGPD establece claramente la forma en la que se ha de producir una transferencia de datos de estas características cuando no existe una decisión de adecuación como el *Privacy Shield*.

4. Comentario

4.1. Las consecuencias prácticas de Schrems II

4.1.1. La invalidez inmediata del *Privacy Shield*

Tras la sentencia del TJUE, se produce una invalidez inmediata del *Privacy Shield* con carácter retroactivo. Por lo tanto, a partir de ese momento no podrán producirse transferencias de datos personales desde la UE a Estados Unidos bajo el amparo de dicha Decisión. Además, aquellas transferencias que se hubiesen llevado a cabo con base en el *Privacy Shield* exclusivamente, devienen ilegales de forma inmediata (García Micó & García-Perrote, 2020, p. 555).

Esto significa que Estados Unidos se encuentra en la misma posición que cualquier otro tercer Estado que no cuente con una decisión de adecuación para las transferencias de datos personales. De hecho, la Comisión Irlandesa de Protección de Datos ya ha advertido en una orden preliminar enviada a Facebook de que ha de cesar de inmediato cualquier transferencia llevada a cabo bajo la exclusiva protección del *Privacy Shield* (Costello, 2020, p. 12).

Hay que tener en cuenta que el *Privacy Shield* era la decisión que sustituía al anterior *Safe Harbour*, por lo que parece bastante probable que próximamente se elabore una nueva decisión de adecuación. En este sentido, el Departamento de Comercio de Estados Unidos ya ha

reconocido haber iniciado las negociaciones para adaptar el *Privacy Shield* a las exigencias de la sentencia Schrems II[2] (Tracol, 2020, p. 8).

Sin embargo, no se espera una nueva decisión hasta que Estados Unidos no lleve a cabo ciertas modificaciones en sus políticas de vigilancia (Chamber, 2020, p. 775). La Comisión tendrá que asegurarse de que el tratamiento de los datos que puedan llevar a cabo las autoridades estadounidenses cumpla con las exigencias del RGPD, algo que, tal y como ha aclarado la sentencia, no ocurre actualmente con la existencia de instrumentos de vigilancia como los recogidos en la FISA o en la *E.O.* 12333, en concreto los programas PRISM y Upstream (Butler, 2020, p. 112).

Además, esta sentencia no afecta solamente a una hipotética futura decisión de adecuación entre la UE y Estados Unidos, sino que tendrá que ser tenida en cuenta para cualquier decisión que la Comisión tome con respecto a un tercer Estado en el futuro (De Miguel, 2020, p. 5).

4.2. Los encargados de evaluar el nivel de protección

Una de las cuestiones más relevantes que surge a raíz de Schrems II es quién deberá evaluar el nivel de protección de terceros países, y en concreto de Estados Unidos, para determinar cuáles son las garantías que se han de implementar al realizar una transferencia de datos personales.

Esta tarea parece corresponder a la Comisión, pues es la que ha de alcanzar los acuerdos de privacidad oportunos, como era el caso del *Privacy Shield*. Sin embargo, a falta de estos acuerdos, se traslada la obligación a los responsables o encargados del tratamiento de los datos y, en su defecto, a las autoridades de control (Bennett, 2016, p. 62).

Por lo tanto, cuando una empresa de la UE pretenda llevar a cabo una transferencia de datos personales a otra empresa en un tercer país, tendrá que esperar a que sus responsables o encargados del tratamiento, junto a los de la empresa importadora, evalúen la legislación en materia de protección de datos en aquel país para determinar qué garantías han de ser aplicadas y hasta qué punto se podrá cumplir con estas.

Esto obliga a las empresas de la UE a evaluar minuciosamente la legislación del país al que pretenden transferir datos personales, algo que, llevado a la práctica, puede ser complicado y difícil de aplicar.

No obstante, ellos no son los únicos que han de estudiar el nivel de protección ofrecido, sino que las autoridades de control estatales en materia de protección de datos han de asegurarse de que cada transferencia que se lleva a cabo desde su Estado a un tercer país cumple con las exigencias del RGPD, coordinándose en todo momento con el Comité Europeo de Protección de Datos. Además, cuando comprueben que alguna de estas transferencias no alcanza un adecuado nivel de protección deberán suspenderla o prohibirla (Tracol, 2020, p. 10).

2 Comunicado de prensa conjunto del Comisario Europeo de Justicia Didier Reynders y el Secretario de Comercio de los Estados Unidos Wilbur Ross. Disponible en: https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en

En definitiva, lo que se crea es un sistema de control de tres niveles, pues la evaluación de la legislación y las políticas de terceros países en materia de protección de datos corresponde: en primer lugar, a la Comisión, que es la encargada de aprobar las decisiones de adecuación como el *Privacy Shield*; en segundo lugar, a los responsables y encargados de protección de datos, que han de desempeñar esta tarea cuando no exista una decisión de adecuación; y en tercer lugar, a las autoridades de control estatales, pues son las que han de evaluar en última instancia si realmente se ha alcanzado un nivel de protección adecuado y, de no ser así, suspender o prohibir las transferencias.

5. Las alternativas al *Privacy Shield*

5.1. Cláusulas tipo de protección de datos

Una vez invalidado el *Privacy Shield*, conviene analizar cuáles son los medios que se han de emplear para realizar transferencias de datos personales a terceros países. En este sentido, las cláusulas tipo de protección de datos parecen ser una opción, pues el TJUE mantiene la validez de la Decisión CPT, que permite usar estas cláusulas para transferir datos a terceros países.

No obstante, a pesar de que no se anule la Decisión CPT, las cláusulas tipo de protección de datos no son por sí mismas una alternativa al *Privacy Shield*. Esto se debe a que, tal y como indica el TJUE, una transmisión de datos personales a un tercer país solo podrá llevarse a cabo bajo la exclusiva protección de dichas cláusulas cuando en ese país se asegure un nivel de protección equivalente al que se garantiza en la UE (Tracol, 2020, p. 5).

Esto es lo que explica que las transferencias de datos personales entre Facebook Ireland y Facebook Inc. no pudiesen justificarse en las cláusulas tipo de protección de datos, pues al permitir la legislación estadounidense el acceso de las autoridades a estos datos, se alcanzaba un nivel de vigilancia tan elevado que hacía insuficientes estas garantías (Maldonado, 2020, p. 10).

De esta forma, cualquier empresa que pretenda llevar a cabo una transmisión de datos de este tipo a una entidad estadounidense, podrá utilizar las cláusulas de la Decisión CPT, pero deberá incluir además otras garantías que suplan la falta de protección de los Estados Unidos.

Por lo tanto, aunque esta vía puede ser empleada para efectuar transferencias de datos entre la UE y terceros Estados, habrá que asegurarse antes de que pueda garantizarse de esta forma el nivel de protección adecuado, pues de no ser así, la autoridad competente tendrá que suspender o prohibir la transferencia mientras no se incluyan garantías adicionales (De Miguel, 2020, p. 6).

5.2. Normas corporativas vinculantes

Las normas corporativas vinculantes se regulan en el artículo 47 RGPD y son políticas de protección de datos elaboradas por empresas de la UE para transferir datos personales a terceros países dentro de un mismo grupo empresarial. El TJUE no hace ninguna referencia a las mismas en su sentencia, aunque, posteriormente, el Comité Europeo de Protección de Datos afirmó que los efectos de la sentencia se extienden también a esta herramienta. Parece lógico que así sea, pues lo que fundamenta la invalidez del *Privacy Shield* es, como se ha indicado

anteriormente, el insuficiente nivel de protección garantizado por Estados Unidos en el tratamiento de los datos personales (Tracol, 2020, p. 9).

Por lo tanto, el hecho de incluir normas corporativas vinculantes no implica que haya una protección suficiente en un tercer país, sino que esto se tendrá que comprobar en cada caso y añadir garantías adicionales cuando fuese necesario, lo que sucederá en las transferencias a Estados Unidos. En este sentido no encontramos pues ninguna ventaja con respecto a las cláusulas tipo de protección de datos, cuya validez dependerá también del nivel de protección garantizado en ese Estado y de las garantías que se añadan.

5.3. Consentimiento explícito

El artículo 49 RGPD incluye, fundamentalmente, dos posibles alternativas para la transferencia de datos personales a terceros países. La primera de ellas es el consentimiento del interesado, mientras que la segunda es la existencia de algún supuesto de necesidad como el cumplimiento de un contrato o razones de interés público (Chander, 2020, p. 775).

Con respecto al consentimiento, este debe prestarse de forma explícita. Además, no bastaría con este primer requisito, sino que además será necesario informar previamente al interesado de los riesgos que puede conllevar una transferencia de datos personales que no está amparada por una decisión de adecuación ni por otras garantías suficientes como para alcanzar el nivel de protección adecuado (De Miguel, 2020, p. 7).

Aunque la sentencia Schrems II no trata el tema del consentimiento explícito, es relevante también en este ámbito, pues al invalidar el *Privacy Shield,* obliga a informar a los interesados de los riesgos que esto supone antes de llevar a cabo transferencias de datos por consentimiento explícito.

6. Las recomendaciones 01/2020 del Comité Europeo de Protección de Datos

El 10 de noviembre de 2020, el Comité Europeo de Protección de Datos adoptó las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para asegurar el cumplimiento del nivel de protección de datos personales de la UE[3]. El documento desarrolla una guía explicativa de seis niveles para orientar a los exportadores e importadores de datos personales sobre las garantías que han de ser aplicadas durante las transferencias de los datos.

En primer lugar, insta a los exportadores establecidos en la Unión a conocer en todo momento a qué lugar van a ser transferidos los datos personales de los que disponen, asegurándose también de que se usan tan solo para lo estrictamente necesario.

3 Comité Europeo de Protección de Datos (2020). Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (01/2020). Recuperado de https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

El segundo paso sería, una vez localizado el destino de los datos, escoger la herramienta jurídica que se va a emplear para transferirlos. En caso de existir una decisión de adecuación no habría que incluir otras garantías, mientras que si esta no existe será necesario incluir garantías adecuadas que aseguren un adecuado nivel de protección (artículo 46 RGPD), a no ser que sea de aplicación algún supuesto de consentimiento o necesidad (artículo 49 RGPD).

El siguiente nivel exige a los responsables del tratamiento evaluar la legislación y las políticas del Estado receptor para comprobar si existe alguna amenaza que ponga en riesgo la posibilidad de cumplir con las garantías proporcionadas por la herramienta utilizada para la transferencia. Es decir, se ha de evaluar si el nivel de protección de los datos pretendido puede ser alcanzado en ese país.

El cuarto paso requiere la implementación de garantías adicionales cuando en el anterior nivel se compruebe que las herramientas empleadas para la transferencia no aseguran un adecuado grado de protección. En el anexo 2 de las recomendaciones se incluyen algunos ejemplos de posibles garantías adicionales, no obstante, será el exportador de los datos el que tendrá que determinar cuál es la medida más adecuada para cada situación. En caso de no encontrar ninguna garantía suficiente, la transferencia tendrá que ser suspendida o cancelada.

El quinto paso es la inclusión de los requisitos de forma que exija la implementación de las garantías adicionales, para lo que habrá que consultar a las autoridades de control estatales en algunas ocasiones.

Finalmente, se tendrá que revisar periódicamente que las transferencias de datos personales llevadas a cabo continúan cumpliendo con los niveles de protección exigidos, algo que también supervisarán las autoridades de control.

7. Conclusiones

La sentencia Schrems II refleja perfectamente el elevado nivel de protección que ofrece a los ciudadanos europeos el RGPD. Comprobar cómo la normativa de la UE es capaz de condicionar la actividad de empresas de terceros países demuestra la gran eficacia de esta.

Queda probado que el acceso de las autoridades estadounidenses a los datos personales transferidos a empresas establecidas en su país por razones de vigilancia impide que su nivel de protección pueda ser equiparado con el europeo. Por lo tanto, el TJUE acierta al dejar sin validez el *Privacy Shield* que se creó para sustituir al *Safe Harbour*, así como al determinar la validez de la Decisión CPT, pero indicando que esta se tendrá que complementar con garantías adicionales que aseguren una adecuada protección de los datos personales.

Sin embargo, no se puede ignorar la incertidumbre que genera en empresarios y consumidores un fallo de este tipo, con un efecto tan inmediato que obliga a los responsables y encargados de protección de datos a evaluar minuciosamente la legislación y las políticas de cada Estado a cuyas empresas pretendan transferir datos, basándose en unos criterios que tampoco deja claros el TJUE.

Las recomendaciones publicadas el 10 de noviembre de 2020 por el Comité Europeo de Protección de Datos arrojan algo de luz en este sentido, aunque siguen siendo insuficientes, pues no hacen mucho más que ordenar las ideas que ya anticipaba la sentencia Schrems II, disparando la carga de trabajo de las empresas y, en ocasiones, generando grandes costes, en especial

para aquellas entidades que no dispongan de departamentos especializados en protección de datos.

En resumen, el hecho de dejar en manos de los responsables o encargados del tratamiento de los datos la evaluación del nivel de protección de terceros países les obliga a conocer en profundidad su legislación y sus políticas, trasladándoles grandes responsabilidades y dando lugar a opiniones dispares entre unas empresas y otras. Obliga así, además, a las autoridades de control estatales a revisar a su vez las conclusiones a las que llegan los responsables del tratamiento.

Sería más acertado, probablemente, que el Comité Europeo de Protección de Datos estableciera unas instrucciones claras y comunes para los diferentes Estados, unificando así el criterio a seguir por las empresas al efectuar transferencias de datos e implementar garantías que permitan el cumplimiento de las exigencias del RGPD.

Referencias

Bennett, S. C. (2016). Eu privacy shield: Practical implications for U.S. litigation. *Practical Lawyer*, *62*(2), 60-64. Recuperado de: http://files.ali-cle.org/thumbs/datastorage/lacidoirep/articles/TPL1604-Bennett_thumb.pdf

Butler, A. (2017). United States. Whither privacy shield in the Trump era. *European Data Protection Law Review (EDPL)*, *3*(1), 111-113. doi: 10.21552/edpl/2017/1/17.

Chander, A. (2020). Is Data Localization a Solution for Schrems II? *Journal of International Economic Law*, *23*(3), 771-784. doi: 10.1093/jiel/jgaa024.

Costello, R. A. (2020, Octubre 15). Schrems II: Everything is Illuminated? *European Papers*, *2020*(5), 1-15. doi: 10.15166/2499-8249/396.

García Micó, T. G., & García-Perrote, I. (2020). Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II. *Indret: Revista para el Análisis del Derecho*, *3*, 551-559. Recuperado de: https://raco.cat/index.php/InDret/article/view/375259/468645

Maldonado, E. (2020, Septiembre). Bridging the gap in transatlantic data protection, Discussion Paper, No. 4/20. *Europa-Kolleg Hamburg, Institute for European Integration*. doi: 10419/224928.

Miguel, P. A. de (2020). Implicaciones de la declaración de invalidez del Escudo de Privacidad. *La Ley Unión Europea*, *84*. Recuperado de: https://eprints.ucm.es/62504/1/PADemiguelAsensio%20LaLey%20UE%20n%2084%2009.20.pdf

Tracol, X. (2020). "Schrems II": The return of the Privacy Shield. *Computer Law & Security Review*, *39*. doi: 10.1016/j.clsr.2020.105484.