"SCHREMS II" Y LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES UE-EE.UU.

Alfonso Ortega Giménez
Profesor Titular de Derecho Internacional Privado
Universidad Miguel Hernández de Elche

I. PLANTEAMIENTO

La Sentencia del Tribunal de Justicia de la Unión Europea, en lo sucesivo, TJUE de 16 de julio de 2020, dictada en el Asunto C-311/18, (en adelante, Sentencia "Schrems II") constituye un hito esencial en una sucesión de hechos relacionados con una de las cuestiones que mayor debate ha generado en los últimos años en materia de protección de datos, como es la transferencia de datos personales protegidos por el Derecho de la Unión a terceros países extracomunitarios, especialmente, a los Estados Unidos de América.

Se trata de una cuestión cuya suma importancia resulta comprensible en un mundo en el que la globalización alcanza su máximo exponente en el campo de los datos personales protegidos; principalmente, debido a la existencia de redes sociales u otras plataformas digitales que operan a nivel mundial tratando datos personales protegidos de sus usuarios que, en muchos casos, se refieren a la esfera más íntima de su privacidad.[109]

---

[109] Vid., en sentido amplio, ORTEGA GIMÉNEZ, Alfonso (Dir.); HEREDIA SÁNCHEZ, Lerdys; y LORENTE MARTÍNEZ, Isabel (Coords.), Problemas que el COVID-19 plantea en el trinomio protección de datos, transferencia y movilidad. Aportación de soluciones prácticas desde la ciencia jurídica, Editorial Thomson Reuters Aranzadi, Cizur Menor (Navarra), abril 2021; ORTEGA GIMÉNEZ, Alfonso, Transferencias Internacionales de Datos de Carácter Personal Ilícitas, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017; y ORTEGA GIMÉNEZ, Alfonso y MARZO PORTERA, Ana, Empresa y transferencia internacional de datos personales, Instituto Español de Comercio Exterior (ICEX), Madrid, 2013.

Esta situación es de enorme importancia por cuanto que, de no establecerse los adecuados criterios de control del respeto a la normativa comunitaria en materia de protección de datos de carácter personal, en este tipo de transferencias a terceros países extracomunitarios, nos encontraríamos con que la protección de datos de carácter personal quedarían limitados a un ámbito territorial relativamente reducido, con lo que los ciudadanos de la Unión Europea (en adelante, UE) estarían desprotegidos en multitud de ocasiones en los que sus datos personales serán tratados en países ajenos al territorio comunitario.

Es por ello por lo que la normativa comunitaria de protección de datos de carácter personal, representada en la actualidad por el 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, que sustituyó a la Directiva 95/46/CE –en adelante, RGPD- [110], establece unos criterios reguladores de dichas transferencias a países extracomunitarios,[111] con la evidente finalidad de mantener, aún en estos casos, el debido nivel de protección de los datos de carácter personal de los ciudadanos de la UE.

De esta forma, a grandes rasgos, el RGPD establece un mecanismo de protección que se configura en tres niveles, debiendo considerarse, en primer lugar, lo establecido en su artículo 45[112], que regula la emi-

---

110 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://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&qid=1601305740744&from=ES.

111 Vid., en sentido amplio, ORTEGA GIMÉNEZ, Alfonso, "El impacto del Reglamento General de Protección de Datos de la Unión Europea y de la LOPDGDD en el régimen jurídico de las transferencias internacionales de datos de carácter personal", en GARCÍA MAHAMUT, Rosario y TOMÁS MALLÉN, Beatriz, El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de datos y garantía de los derechos digitales, Editorial Tirant lo Blanch, Valencia 2019, pp. 393-417.

112 Artículo 45 del RGPD: "Transferencias basadas en una decisión de adecuación. 1. 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. 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales. 3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2. 4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE. 5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que

sión de Decisiones de Adecuación por parte de la Comisión; en segundo lugar, lo dispuesto por su artículo 46, que establece un sistema de garantías sostenido, principalmente, por las normas corporativas vinculantes y las cláusulas tipo de protección de datos. Por último, lo dispuesto en su artículo 49 que, en defecto de los mecanismos dispuestos en los anteriores preceptos, establece una serie de supuestos relacionados taxativamente, en los que pueden realizarse transferencias de datos a terceros países comunitarios, que descansan, en general, en el expreso consentimiento del interesado, previa advertencia de los riesgos de la transferencia de sus datos, así como en razones de interés general que, en cualquier caso, deberán respetar las garantías del Derecho de la UE.

Teniendo en cuenta lo anterior, la Sentencia "Schrems II" es de enorme importancia por cuanto que, a pesar de referirse a las transferencias de datos personales protegidos a los Estados Unidos, establece con nitidez los parámetros que deberán ser tenidos en cuenta para las transferencias de datos a terceros países extracomunitarios, definiendo con claridad conceptos esenciales como es el nivel de protección adecuado de los datos personales que ha de ser tomado en consideración, o las obligaciones y facultades, tanto de las autoridades públicas de control, como de todos los sujetos implicados en la transferencia

---

se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2. Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3. 6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5. 7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49. 8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado. 9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo."

y tratamiento de datos personales protegidos con destino a terceros países extracomunitarios.[113]

Por esta razón, a pesar de que el objeto y alcance de la Sentencia "Schrems II" puede parecer limitado al caso de los Estados Unidos, lo cierto es que la misma ha marcado un antes y un después en las transferencias extracomunitarias de datos de carácter personal al definir elementos esenciales para garantizar que los derechos de los ciudadanos de la Unión Europea, afectados por estas transferencias, no quedan desprotegidos.

Estamos ante una cuestión enormemente importante, que hará correr ríos de tinta, por lo que, es evidente que, no llegaremos a alcanzar en el presente trabajo todas las implicaciones y matices que tiene la Sentencia. Sin perjuicio de ello, no cabe duda del interés jurídico del presente estudio, en el que se partirá de un breve relato de los antecedentes que nos han conducido a este hito, concretando el objeto de la cuestión prejudicial planteada, para llegar al concreto análisis de la decisión que, el TJUE, ha alcanzado con respecto a cada una de estas cuestiones controvertidas.

II. ANTECEDENTES: "SCHREMS I"

En cuanto a los pronunciamientos contenidos en la Sentencia "Schrems II" resulta pertinente la realización de un breve análisis de los antecedentes fácticos y jurídicos que nos llevan a la Sentencia objeto de estudio, constituyendo el punto de partida la reclamación que

---

113 Vid., en particular, ORTEGA GIMÉNEZ, Alfonso y GARCÍA ESCOBAR, Encarnación, "Réquiem por el Escudo de Privacidad (tras la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 "Schrems II")", en Revista Aranzadi Unión Europea, número 11, Editorial Aranzadi, S.A.U., Cizur Menor (Navarra), 02 de marzo de 2021; ORTEGA GIMÉNEZ, Alfonso y GARCÍA ESCOBAR, Encarnación, "Transferencias internacionales de datos personales UE-EE.UU. tras la STJUE "SCHREMS II", en Revista Lex Mercatoria, volumen 16, artículo 2, Universidad Miguel Hernández de Elche, Elche, 2020, pp. 9-15; y ORTEGA GIMÉNEZ, Alfonso y GARCÍA ESCOBAR, Encarnación, "Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 ("Schrems II")", en LA LEY Privacidad, número 6, Editorial Wolters Kluwer, Madrid, octubre-diciembre 2020, pp. 1-22.

el Sr. Schrems presentó, en fecha 25 de junio de 2013, ante el Comisario, en la que le solicitaba, en esencia, que prohibiera a Facebook Ireland transferir sus datos personales a los Estados Unidos, alegando el reclamante que el Derecho y las prácticas en vigor en dicho país no garantizaban una protección suficiente de los datos personales conservados en su territorio frente a las actividades de vigilancia llevadas a cabo, en dicho país, por las autoridades públicas. Esta reclamación fue desestimada basándose en que, en particular, la Comisión había declarado, en su Decisión 2000/520/CE de "Puerto Seguro"[114], que los Estados Unidos ofrecían un nivel adecuado de protección.

La High Court (Tribunal Superior, Irlanda), ante la que el Sr. Schrems había interpuesto un recurso contra la desestimación de su reclamación, planteó al TJUE una petición de decisión prejudicial relativa a la interpretación y a la validez de la Decisión 2000/520/CE, que dio lugar a la Sentencia de 6 de octubre de 2015, que se denominará como "Schrems I", en la que el TJUE declaró inválida la referida Decisión[115].Como consecuencia de dicha Sentencia, el órgano jurisdiccional remitente anuló la desestimación de la reclamación del Sr. Schrems, devolviendo la misma al Comisario.

Cabe señalar que, en el marco de la investigación abierta por este último, Facebook Ireland alegó que una gran parte de los datos personales se transfería a Facebook Inc. basándose en cláusulas tipo de protección de datos recogidas en el anexo de la Decisión 2010/87/UE[116], por lo que, teniendo en cuenta todos estos elementos, el Comisario instó al Sr. Schrems a modificar su reclamación.

Atendiendo el requerimiento del Comisario, el Sr. Schrems presentó, el 1 de diciembre de 2015, su reclamación modificada en base a la nuevas circunstancias acaecidas (Sentencia "Schrems I" y alegaciones

---

114 Decisión de la Comisión, de 26 de julio, 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 los Estados Unidos de América (DO 2000, L 215, p. 7)

115 Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Schrems, C-362/14.

116 2010/87/UE: Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

de Facebook Inc. ante la Comisión, acerca de su actuación conforme a la Decisión 2010/87/UE), alegando, principalmente, que el Derecho estadounidense obliga a Facebook Inc. a poner los datos personales que se le transfieren a disposición de las autoridades estadounidenses, como la National Security Agency (NSA) y la Federal Bureau of Investigation (FBI). La reclamación modificada afirmaba, además, que, al utilizarse esos datos en el marco de diferentes programas de vigilancia, de una manera incompatible con los artículos 7, 8 y 47 de la Carta[117] (que reconocen, respectivamente, el derecho a la vida privada y familiar, el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva, y a un juez imparcial para la obtención de la tutela de los derechos y libertades reconocidos en el marco de la Unión Europea), la Decisión 2010/87/UE no puede justificar la transferencia de esos datos a los Estados Unidos en base a las cláusulas tipo de protección de datos que se recogen en la misma. Teniendo en cuenta estos argumentos, el Sr. Schrems solicitó al Comisario que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.

Con posterioridad a la presentación de la reclamación modificada por el Sr. Schrems, el 24 de mayo de 2016, el Comisario publicó un "proyecto de decisión" en el que se resumían las conclusiones provisionales de su

---

117 Carta de los Derechos Fundamentales de la Unión Europea. 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."

investigación. En dicho proyecto, consideró con carácter provisional que los datos personales de ciudadanos de la Unión Europea transferidos a Estados Unidos corrían el riesgo de ser consultados y tratados por las autoridades estadounidenses de una manera incompatible con los artículos 7 y 8 de la Carta y que el Derecho estadounidense no ofrece a esos ciudadanos vías de recurso compatibles con el artículo 47 de la Carta. El Comisario estimó que las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT no subsanan esa deficiencia, en la medida en que sólo confieren a los interesados derechos contractuales contra el exportador o el importador de los datos, sin vincular a las autoridades estadounidenses.

De esta forma, al considerar que, en esas circunstancias, la reclamación modificada del Sr. Schrems planteaba la cuestión de la validez de la Decisión 2010/87/UE relativa a cláusulas contractuales tipo, el 31 de mayo de 2016, el Comisario inició un procedimiento ante la High Court (Tribunal Superior), apoyándose en la jurisprudencia resultante de la sentencia "Schrems I", de 6 de octubre de 2015, apartado 65, a efectos de que esta última pregunte al TJUE acerca de esta cuestión. Mediante resolución de 4 de mayo de 2018, la High Court (Tribunal Superior) planteó la petición de decisión prejudicial ante el TJUE que, finalmente, se resuelve por la Sentencia "Schrems II".

Es conveniente resaltar que, durante todo este *iter* procedimental se producen dos hechos que constituyen antecedentes a tener en cuenta. La primera de las circunstancias ocurridas durante toda la tramitación someramente reproducida es que, con posterioridad a la declaración de invalidez de la Decisión "Puerto seguro", por la Sentencia "Schrems I", la Comisión adoptó la Decisión "Escudo de Privacidad"[118] que tenía como vocación ocupar el vacío dejado por la declaración de invalidez contenida en la referida Sentencia, constituyendo su validez, como se verá, uno de los puntos fundamentales de la Sentencia que es objeto de análisis en el presente estudio. La segunda de estas circunstancias, con cierta relevancia para el análisis de la cuestión objeto del presente trabajo, es la entrada en vigor del RGPD,

---

118 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 Privacidad UE-EEUU (DO 2016, L 207, p.1).

que sustituyó a la Directiva 95/46/CE, manteniendo, no obstante, en lo sustancial, la regulación contenida en ésta sobre la transferencia de datos personales a terceros países extracomunitarios.

Con respecto a esta última circunstancia, considera el Tribunal que aunque las cuestiones prejudiciales planteadas se refieren a las disposiciones de la Directiva 95/46/CE, deberán responderse en base al RGPD, ya que el Comisario aún no había adoptado una decisión final sobre esa reclamación cuando la Directiva fue derogada y sustituida por el RGPD, con efecto a partir del 25 de mayo de 2018, por lo que es esta norma, y no la Directiva derogada, la que toma en consideración el Tribunal para la resolución de las cuestiones prejudiciales planteadas

III. LA SENTENCIA "SCHREMS II". OBJETO DE LA CUESTIÓN PREJUDICIAL PLANTEADA

Aunque el órgano judicial nacional formula un total de once cuestiones prejudiciales, el Tribunal agrupa sistemáticamente las mismas de manera que el objeto de decisión se reduce a cinco cuestiones que se relacionarán a continuación.

La primera cuestión prejudicial, tiene como objeto la determinación de la inclusión dentro del ámbito de aplicación del RGPD de las transferencias de datos personales realizada por un operador económico establecido en un Estado miembro, a otro operador económico establecido en un país tercero cuando, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades de ese país tercero con fines de seguridad nacional, defensa y seguridad del Estado.

El segundo grupo sistemático de la reclamación prejudicial formulada, en el que el Tribunal incluye las cuestiones prejudiciales segunda, tercera y sexta, es de suma importancia, por cuanto que se traduce en la delimitación de los elementos que han de tomarse en consideración a efectos de determinar si ese nivel de protección está garantizado en el contexto de una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos.

En tercer lugar, el TJUE se pronuncia sobre la cuestión prejudicial octava, que se refiere a la determinación de las facultades de las autoridades de control competentes y, concretamente, a si éstas están obligadas a suspender o prohibir una transferencia de datos personales a un país tercero, que esté basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando por parte de la correspondiente autoridad de control se considera que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero.

El cuarto grupo sistemático objeto de resolución por la Sentencia "Schrems II" comprende las cuestiones prejudiciales séptima y undécima, concretándose en el análisis de la validez de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo, bajo el prisma de la Carta de Derechos Fundamentales de la UE.

En quinto y último lugar, se valoran por el Tribunal, de forma conjunta, las cuestiones prejudiciales cuarta, quinta, novena y décima que, en suma, se refieren a una cuestión de vital importancia como es la validez de la Decisión "Escudo de Privacidad", así como el grado de garantía de la tutela judicial efectiva que, para los ciudadanos de la UE, ofrece la figura del Defensor del Pueblo mencionado en el Anexo III de la referida Decisión.

IV. LA SENTENCIA "SCHREMS II". DECISIÓN DEL TRIBUNAL

1. Sobre el ámbito de aplicación del RGPD

Como se ha expuesto, el objeto de la primera cuestión prejudicial se concreta en la inclusión, dentro del ámbito de aplicación del RGPD de una transferencia de datos personales realizada por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero cuando, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades de ese país tercero con fines de seguridad nacional, defensa y seguridad del Estado.

El TJUE resuelve esta cuestión considerando que este tipo de transferencias se encuentran dentro del ámbito de aplicación del RGPD, tras un acertado análisis del ámbito de aplicación del mismo, conforme a lo dispuesto en su artículo 2, apartado 1, que establece que el RGPD se aplica al tratamiento total, o parcialmente automatizado, de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Toma en consideración, también, el Tribunal la definición que el artículo 4, punto 2 del RGPD, realiza del concepto de "tratamiento" como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no", así como los ejemplos que, de dicho concepto, se citan en el referido precepto, como es la "comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso", debiendo tenerse en cuenta, además, a juicio del Tribunal, que el referido RGPD aplica, a las transferencias de datos personales a países terceros, normas particulares recogidas en su capítulo V, titulado "Transferencias de datos personales a terceros países u organizaciones internacionales", y confiere a las autoridades de control poderes específicos a ese efecto, que se recogen en el artículo 58[119], apartado 2, letra j), del RGPD.

No existiendo dudas con respecto a que el RGPD se aplica a las transferencias de datos personales a países terceros extracomunitarios, pasa el Tribunal a analizar si, el supuesto de hecho de la cuestión prejudicial planteada resulta incardinable a alguna de las excepciones que establece el Reglamento en cuanto a su ámbito de aplicación establecidas en el artículo 2[120], apartado 2

---

119 Artículo 58, apartado 2, letra j) del RGPD: "Poderes. Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional."

120 Artículo 2, apartado 2 del RGPD: "Ámbito de aplicación material 2. El presente Reglamento no se aplica al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines

del RGPD que, como recuerda el TJUE, deben interpretarse en sentido estricto[121].

Así las cosas, el Tribunal concluye que, en el caso de autos, al haber sido realizada la transferencia de datos personales que es objeto del litigio principal, por Facebook Ireland hacia Facebook Inc., es decir, entre dos personas jurídicas, dicha transferencia no está comprendida dentro del ámbito del artículo 2, apartado 2, letra c) del RGPD, que tiene por objeto el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. A la referida transferencia tampoco pueden aplicársele las excepciones recogidas en el artículo 2[122], apartado 2, letras a), b) y d), del antedicho Reglamento, ya que las actividades que allí se enumeran a título de ejemplo son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares.

Por todo ello concluye el Tribunal, con respecto a la primera de las cuestiones prejudiciales planteadas, que la posibilidad de que los datos personales transferidos entre dos operadores económicos con fines comerciales sean objeto, en el transcurso de la transferencia o tras ella, de un tratamiento con fines de seguridad pública, defensa o seguridad del Estado por parte de las autoridades del país tercero de que se trate, no puede excluir a la referida transferencia del ámbito de aplicación del RGPD.

---

de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."

121 *Vid*. en lo que se refiere al artículo 3, apartado 2, de la Directiva 95/46/CE, la sentencia de 10 de julio de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, apartado 37.

122 Artículo 2, apartado 2, letras a), b) y d) del RGPD: "Ámbito de aplicación material: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."

2. *Sobre el nivel de protección adecuado para la transferencia de datos a terceros países*

Como se ha avanzado, el segundo grupo de cuestiones analizadas por el TJUE se centra en la delimitación de los elementos que han de tomarse en consideración a efectos de determinar si ese nivel de protección está garantizado en el contexto de una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos.

En relación con esta cuestión, analiza el TJUE, en primer lugar, lo dispuesto por el artículo 46[123], apartados 1 y 2, letra c) del RGPD, tras una lectura conjunta de esas disposiciones, concluyendo que, cuando no existe una decisión de adecuación adoptada en virtud del artículo 45[124], apartado 3, del referido Reglamento, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país si hubiera ofrecido "garantías adecuadas", siempre que se cumpla la condición de que los interesados cuenten "con derechos exigibles y acciones legales efectivas", pudiendo proporcionarse esas

---

123 Artículo 46, apartados 1 y 2, letra c) del RGPD: "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."

124 Artículo 45, apartado 3 del RGPD: "Transferencias basadas en una decisión de adecuación. 3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2."

garantías adecuadas, en particular, mediante cláusulas tipo de protección de datos adoptadas por la Comisión.

Afirma el Tribunal que el artículo 45[125], apartado 1, primera frase del RGPD establece que podrá autorizarse una transferencia de datos personales a un tercer país mediante una decisión adoptada por la Comisión, conforme a la cual se atestigua que ese tercer país, un territorio o uno o varios sectores específicos de ese tercer país garantizan un nivel de protección adecuado. A este respecto, sin exigir que el país tercero de que se trate garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la UE, debe entenderse que la expresión "nivel de protección adecuado", tal como queda confirmado en el considerando 104 del referido Reglamento, exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y de los derechos fundamentales sustancialmente equivalente al garantizado en la Unión Europea en virtud del antedicho Reglamento, interpretado a la luz de la Carta. En efecto, a falta de esa exigencia, el objetivo mencionado en el anterior apartado se frustraría[126].

En este sentido, concluye el Tribunal que las garantías adecuadas deben asegurar que las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gocen, como en el marco de una transferencia basada en una decisión de adecuación, de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión.

En relación con el marco sobre el que ha de interpretarse el alcance del nivel de protección sustancialmente equivalente al garantizado dentro de la UE, analiza el Tribunal si el análisis del nivel de protección debía determinarse a la luz del Derecho de la Unión, en particular, de los derechos garantizados por la Carta y/o a la luz de los

---

125 Artículo 45, apartado 1 del RGPD: "Transferencias basadas en una decisión de adecuación 1. 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."

126 *Vid*., en lo que respecta al artículo 25, apartado 6, de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 73.

derechos fundamentales reconocidos en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, o también a la luz del Derecho nacional de los Estados miembros. Con respecto a esta cuestión, concluye el Tribunal que el nivel de protección de los derechos fundamentales exigido en el artículo 46, apartado 1, del antedicho Reglamento debe determinarse sobre la base de las disposiciones del mismo Reglamento, interpretadas a la luz de los derechos fundamentales garantizados por la Carta.

Por último, determina el Tribunal los elementos que han de tomarse en consideración para determinar la adecuación del nivel de protección en el contexto de una transferencia de datos personales a un país tercero sobre la base de las cláusulas tipo de protección de datos adoptadas en virtud del artículo 46, apartado 2, letra c) del RGPD, respondiendo el Tribunal que han de tenerse en cuenta, por una parte, las estipulaciones contractuales objeto de acuerdo entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate y, por otra parte, en lo que respecta al hipotético acceso de las autoridades públicas del país tercero, a los datos personales transferidos, se han de tener en cuenta los elementos mencionados, de modo no exhaustivo, en el artículo 45, apartado 2 del RGPD, que precisa que los interesados deben gozar de garantías adecuadas y contar con derechos exigibles y acciones legales efectivas.

Por tanto, teniendo en cuenta todo lo anterior, el Tribunal interpreta el nivel de protección adecuado para la transferencia de datos a terceros países en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de

las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45[127], apartado 2 del RGPD.

3. Sobre las obligaciones de control de las autoridades

Como se ha visto, el TJUE analiza, de forma independiente, la cuestión prejudicial octava, que se refiere a la determinación de las facultades de las autoridades de control competentes y, concretamente, a si éstas están obligadas a suspender o prohibir una transferencia de datos personales a un país tercero, basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando por parte de la correspondiente autoridad de control se considera que dichas cláusulas no se respetan, o no pueden respetarse en ese país tercero, así como que la protección de los datos transferidos exigida por el Derecho de la Unión Europea, en particular, por los artículos 45 y 46 del RGPD y

---

127 Artículo 45, apartado 2 del RGPD: "Transferencias basadas en una decisión de adecuación. 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales."

por la Carta, no puede garantizarse, o si, por el contrario, el ejercicio de esas facultades de suspensión o prohibición de las transferencias están limitadas a supuestos excepcionales[128].

Esta cuestión prejudicial es resuelta por el mencionado Tribunal en el sentido de considerar dos escenarios diferentes dependiendo de la existencia o no de una decisión de adecuación dictada por la Comisión. En el caso de que exista una decisión de adecuación, y mientras que la misma no haya sido objeto de invalidación por el TJUE, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciará con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado ni, por consiguiente, suspender o prohibir transferencias de datos personales a ese tercer país.

No obstante, aclara el Tribunal que incluso habiendo adoptado la Comisión una decisión de adecuación, la autoridad nacional de control competente, a la que una persona haya presentado una reclamación para proteger sus derechos y libertades frente al tratamiento de datos personales que la conciernen, debe poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por el RGPD y, en su caso, interponer un recurso ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de adecuación, planteen al TJUE una cuestión prejudicial sobre esta validez[129].

Por el contrario, en el caso de que no exista una decisión de adecuación emitida por la Comisión, el Tribunal resuelve que la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando esa autoridad de control

---

128 *Vid.*, en relación con la traslación de la responsabilidad hacia el responsable del tratamiento, Rodríguez Ayuso, J. F., "Anulación del Privacy Shield en las transferecnias internacionales de datos: ¿presenciamos un desplazamiento fáctico de la responsabilidad?", en *Revista Boliviana de Derecho*, N.º 31, enero 2021, pp. 426-503.

129 *Vid.*, en lo que respecta al artículo 25, apartado 6, y al artículo 28 de la Directiva 95/46/CE, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartados 57 y 65.

considera, a la luz de todas las circunstancias específicas de la referida transferencia, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión Europea, en particular, por los artículos 45 y 46[130] del RGPD y por la Carta, no puede garantizarse mediante otros medios, en especial si el responsable o el encargado del tratamien-

---

130 Artículo 46 del RGPD: "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: a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; b) normas corporativas vinculantes de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2; e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados. 3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante: a) 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 b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. 4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo. 5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo."

to establecidos en la Unión Europea no han suspendido la transferencia o puesto fin a esta por sí mismos.

4. Sobre la validez de la Decisión 2010/87/UE

Como se ha señalado, el cuarto grupo sistemático objeto de resolución por la Sentencia "Schrems II" comprende las cuestiones prejudiciales séptima y undécima que, en esencia, tratan sobre el análisis de la validez de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo bajo el prisma de la Carta de Derechos Fundamentales de la Unión Europea.

El TJUE hace depender la validez de la Decisión 2010/87/UE a si, de conformidad con la exigencia resultante de los artículos 46, apartado 1 y 2, letra c), del RGPD, interpretados a la luz de los artículos 7, 8 y 47 de la Carta[131], tal decisión incluye mecanismos efectivos que permitan, en la práctica, garantizar que el nivel de protección exigido por el Derecho de la Unión Europea sea respetado, así como que las transferencias de datos personales basadas en esas cláusulas sean suspendidas o prohibidas en caso de violación de dichas cláusulas, o de que resulte imposible su cumplimiento.

---

131 Carta de los Derechos Fundamentales de la Unión Europea. 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."

El referido Tribunal analiza los concretos mecanismos efectivos de protección de datos que se recogen en el anexo de la Decisión 2010/87/UE concluyendo que, de las cláusulas 4, letras a) y b), 5, letra a), 9 y 11, apartado 1, de dicho anexo se desprende que el responsable del tratamiento establecido en la UE, el destinatario de la transferencia de datos personales y el eventual encargado de este último, se comprometen mutuamente a que el tratamiento de esos datos, incluida su transferencia, ha sido efectuado y seguirá efectuándose de conformidad con la legislación de protección de datos aplicable, que, conforme al artículo 3, letra f) de la antedicha Decisión se corresponde con la legislación que protege los derechos y libertades fundamentales de las personas y, en particular, su derecho a la vida privada respecto del tratamiento de los datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos.

Asimismo, se analizan por el TJUE las obligaciones del destinatario de la transferencia de datos personales establecido en un país tercero, que se concretan en una información inmediata, al responsable del tratamiento establecido en la UE, de su eventual incapacidad para cumplir con las obligaciones que le incumben con arreglo al contrato celebrado, teniendo la posibilidad, en este caso, el responsable del tratamiento establecido de suspender la transferencia de los datos o rescindir el contrato interpretando el TJUE que esta facultad es obligatoria para el responsable del tratamiento cuando el destinatario de la transferencia establecido en un país extracomunitario no cumple, o ya no puede cumplir, las cláusulas tipo de protección de datos, por lo que, más que una facultad, se convierte en una obligación del responsable de tratamiento establecido en la Unión Europea.

Por tanto, concluye el TJUE que la interpretación de los mecanismos incluidos en la Decisión 2010/87/UE, obligan al responsable del tratamiento establecido en la Unión Europea y al destinatario de la transferencia de datos personales a asegurarse de que la legislación del país tercero de destino permita al antedicho destinatario cumplir con las cláusulas tipo de protección de datos recogidas en la propia Decisión 2010/87/UE, antes de llevar a cabo una transferencia de datos personales a ese país tercero.

En lo que se refiere al alcance de dicha comprobación a efectuar por los sujetos intervinientes en la transferencia de datos, o lo que es lo mismo, cuando debe considerarse por éstos que la legislación del país extracomunitario es incompatible con las cláusulas, señala el TJUE que, las obligaciones impuestas por esa legislación que no vayan más allá de las restricciones necesarias en una sociedad democrática para la salvaguardia, en particular, de la seguridad del Estado, la defensa y la seguridad pública no están en contradicción con las cláusulas tipo de protección de datos, por lo que, *sensu* contrario, el hecho de acatar una obligación dictada por el Derecho del país tercero de destino que vaya más allá de lo necesario para la consecución de tales fines debe considerarse una violación de las antedichas cláusulas.

Conforme a lo establecido en el anexo de la Decisión 2010/87/UE, el responsable del tratamiento establecido en la UE está obligado, cuando el destinatario de la transferencia de datos personales le notifica, que la legislación que le es de aplicación ha sido objeto de una modificación que puede tener un importante efecto negativo sobre las garantías ofrecidas y las obligaciones impuestas por las cláusulas tipo de protección de datos, a enviar esa notificación a la autoridad de control competente en caso de que, a pesar de dicha notificación por parte del destinatario establecido en el país extracomunitario, el responsable de tratamiento establecido en la UE, decida proseguir la transferencia, o levantar una suspensión previamente acordada. El envío de la referida notificación a la autoridad de control competente, y la facultad de ésta de auditar al destinatario de la transferencia de datos personales, permiten a la mencionada autoridad de control comprobar si es preciso proceder a la suspensión o la prohibición de la transferencia prevista para garantizar un nivel de protección adecuado.

Por lo tanto, advierte el Tribunal que, incluso teniendo en cuenta las obligaciones de notificación e información del destinatario extracomunitario, y la obligación de suspensión o finalización de la transferencia de datos por parte del responsable del tratamiento las partes, en el caso de que éste decida no suspender o no finalizar la transferencia, tiene una obligación de notificación a la autoridad de control competente que podrá suspender o prohibir, en su caso, una transferencia de datos personales a un país tercero basada en las cláusulas tipo de protección de datos recogidas en el anexo de dicha Decisión

2010/87/UE, debiendo la autoridad de control ejercer las facultades que le corresponden conforme a lo resuelto en la propia Sentencia "Schrems II".

Por todo lo expuesto, concluye el TJUE que la Decisión 2010/87/UE prevé mecanismos efectivos que permiten, en la práctica, garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas, incluyendo la posibilidad de control por las autoridades en el caso de que por el responsable del tratamiento no se suspenda o prohíba la transferencia, por lo que entiende que no se presenta ningún elemento que pueda afectar a la validez de dicha Decisión.

5. Sobre la validez de la Decisión "Escudo de Privacidad"

Por último, el TJUE entra a valorar la validez de la Decisión "Escudo de Privacidad", atendiendo a si el Derecho de los Estados Unidos garantiza efectivamente el nivel de protección adecuado exigido en el artículo 45 del RGPD, interpretado a la luz de los derechos fundamentales garantizados en los artículos 7, 8 y 47 de la Carta teniendo en cuenta que, el órgano jurisdiccional que plantea la cuestión prejudicial considera que el Derecho de los Estados Unidos no prevé las limitaciones y garantías necesarias con respecto a las injerencias autorizadas por su normativa nacional, así como que tampoco garantiza una tutela judicial efectiva a los interesados, contra tales injerencias, sin que el mecanismo del Defensor del Pueblo previsto ofrezca la debida protección a la tutela judicial efectiva.

Partiendo de este planteamiento se analiza por parte del TJUE la validez de la Decisión "Escudo de Privacidad" teniendo en cuenta, por una parte, la incidencia que las injerencias de las autoridades de Estados Unidos, conforme al Derecho de aquel país, tiene en el nivel de protección adecuado y, por otra, la validez de la figura de Defensor del Pueblo regulado por la Decisión "Escudo de Privacidad" para garantizar la tutela judicial efectiva de los ciudadanos comunitarios en defensa de sus datos personales protegidos.

Con respecto a la primera de las cuestiones, considera el Tribunal que las injerencias resultantes de los programas de vigilancia basados en la FISA[132] y en la E.O. 12333[133] no están sujetas a exigencias que garanticen, un nivel de protección sustancial, considerando el TJUE que las limitaciones que establecen las referidas normas de los Estados Unidos no respetan el principio de proporcionalidad, que establece básicamente que las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario.

En este sentido, añade el TJUE que la comunicación de datos de carácter personal a un tercero, como una autoridad pública, constituye una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta (derecho al respeto a la vida privada y familiar, así como derecho a la protección de datos personales), cualquiera que sea la utilización posterior de la información comunicada, considerando una injerencia similar la conservación de los datos de carácter personal y del acceso a esos datos con vistas a su utilización por parte de las autoridades públicas, con independencia de que la información relativa a la vida privada de que se trate tenga o no carácter sensible o de que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia[134].

Aunque el TJUE pone de manifiesto que los anteriores derechos no gozan de carácter absoluto, incide en que cualquier limitación de los mismos, derivada del tratamiento de datos de carácter personal, debe realizarse para fines concretos, sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto en la Ley, que deberá definir con absoluta claridad el alcance de la limitación prevista en los derechos y libertades, estableciendo reglas claras y precisas que regulen el alcance y la aplicación de la medida

---

132 Foreign Intelligence Surveillance Act of 1978 (Ley de Vigilancia de la Inteligencia Extranjera) (*Pub.L.* 95–511, 92 Stat. 1783, 50 U.S.C. cap. 36).

133 Executive Order 12333.

134 Se remite el TJUE en este punto a las sentencias de 20 de mayo de 2003, Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartados 74 y 75; de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 33 a 36, y el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126.

en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario ya que, de lo contrario, no se respetaría el citado principio de proporcionalidad.

En el caso objeto de la Sentencia "Schrems II", el TJUE advierte que las injerencias resultantes de los programas de vigilancia basados en la FISA y en la E.O. 12333 exceden de los límites impuestos por la normativa europea de protección de datos de carácter personal, principalmente debido a que los programas de vigilancia autorizados por la normativa de los Estados Unidos no se fundamentan en una vigilancia individual sino en programas de vigilancia masivos e indiscriminados y, en definitiva, ilimitados, basados en sistemas de recopilación "en bloque" de los datos personales protegidos que, evidentemente, exceden notablemente de las exigencias de concreción y determinación del alcance de la limitación de los derechos y libertades que derivan del principio de proporcionalidad, por lo que, concluye el Tribunal, que no puede considerarse que los programas de vigilancia basados en esas disposiciones se limiten a lo estrictamente necesario.

Con respecto a la segunda de las cuestiones, es decir, sobre la debida garantía del derecho a la tutela judicial efectiva de los interesados, y sobre si la figura del Defensor del Pueblo a la que se refiere la Decisión "Escudo de Privacidad" garantiza este derecho, el TJUE recuerda que el primer párrafo del referido artículo 47 de la Carta requiere que toda persona cuyos derechos y libertades garantizados por el Derecho de la UE hayan sido violados tenga derecho a la tutela judicial efectiva respetando las condiciones establecidas en el mencionado artículo. A tenor del párrafo segundo del antedicho artículo, toda persona tiene derecho a que su causa sea oída por un juez independiente e imparcial, lo que hace necesaria, en todo caso, la existencia de recursos administrativos y acciones judiciales que sean efectivos y accesibles para las personas cuyos datos personales son objeto de tratamiento.

En el caso de autos, la constatación contenida en la Decisión "Escudo de Privacidad", según la cual los Estados Unidos garantizan un nivel de protección sustancialmente equivalente al previsto en el artículo 47 de la Carta, fue puesta en entredicho basándose, en particular, en que la creación del Defensor del Pueblo en el ámbito del "Escudo de Privacidad" no puede subsanar las lagunas en lo que respecta a la tutela judicial de las personas cuyos datos personales son transferidos a ese país tercero, considerando el TJUE que esta exigencia no se cumple en este caso, por cuanto la normativa de los Estados Unidos, en especial en los casos de programas de vigilancia basados en la E.O. 12333, no ofrecen ninguna vía de recurso, por lo que no garantizan la debida tutela judicial efectiva para los ciudadanos cuyos datos son objeto de tratamiento.

Entiende el TJUE que la existencia del mecanismo del Defensor del Pueblo no subsana las limitaciones al derecho a la tutela judicial efectiva, poniendo en entredicho la independencia del Defensor del Pueblo con respecto al poder ejecutivo de los Estados Unidos y su facultad para emitir decisiones vinculantes para las autoridades estadounidenses sin que, además, constata que no existe ninguna garantía legal que pueda ser invocada por los ciudadanos ante dicho Defensor del Pueblo, por lo que no se cumple con la exigencia de una vía de recurso efectivo garante del derecho a la tutela judicial efectiva en materia de protección de datos.

Por lo tanto, concluye el TJUE que la Comisión, al declarar, en el artículo 1, apartado 1, de la Decisión "Escudo de Privacidad", que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a entidades establecidas en ese país tercero en el marco del Escudo de la Privacidad UE-EE. UU., no tuvo en cuenta las exigencias resultantes del artículo 45, apartado 1, del RGPD, interpretado a la luz de los artículos 7, 8 y 47 de la Carta por lo que declara la invalidez de dicha Decisión.

Por último, se pronuncia el TJUE sobre si es preciso mantener los efectos de la antedicha Decisión "Escudo de Privacidad" para evitar la creación de un vacío legal, concluyendo que en este caso no se produce tal vacío legal por cuanto que teniendo en cuenta el artículo 49 del RGPD, que establece, de manera precisa, las condiciones en las que pueden tener lugar transferencias de datos personales a países terceros

en ausencia de una decisión de adecuación en virtud del artículo 45, apartado 3, del referido Reglamento o de garantías adecuadas con arreglo al artículo 46 del mismo Reglamento.

V. CONCLUSIONES

PRIMERA.- La Sentencia "Schrems II" resuelve un total de once cuestiones prejudiciales planteadas por la High Court (Tribunal Superior, Irlanda), que el TJUE agrupa, para su resolución, en cinco cuestiones que se refieren a la aplicabilidad del RGPD a las transferencia de datos a terceros países extracomunitarios, cuando en dichos países los datos pueden ser tratados por las autoridades con fines de seguridad nacional, defensa y seguridad del Estado; a los elementos integrantes del nivel de protección adecuado en terceros países; a las competencias y facultades de las autoridades de control en dichas transferencias; así como a la validez tanto de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo bajo el prisma de la Carta de Derechos Fundamentales de la UE, como de la Decisión "Escudo de Privacidad", así como el grado de garantía de la tutela judicial efectiva que, para los ciudadanos de la Unión Europea, ofrece la figura del Defensor del Pueblo mencionado en esta última Decisión.

SEGUNDA.- El TJUE interpreta el nivel de protección adecuado para la transferencia de datos a terceros países en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas las disposiciones normativas de los terceros países deben garantizar que los derechos de las personas cuyos datos personales se transfieren a dicho país, sobre la base de cláusulas tipo de protección de datos, gozan de un nivel de protección, sustancialmente, equivalente al garantizado dentro de la Unión Europea por el RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

TERCERA.- En cuanto a las facultades de las autoridades de control competentes en el caso de transferencias de datos protegidos a terceros países extracomunitarios, diferencia el TJUE entre si existe o no de una decisión de adecuación dictada por la Comisión. En el caso de que exista una decisión de adecuación, y mientras que la misma no haya sido objeto de invalidación por el TJUE, los Estados miembros

y sus órganos, entre ellos las autoridades de control independientes, no pueden adoptar medidas contrarias a esa decisión, aunque tienen la potestad de interponer recurso ante los tribunales nacionales para que éstos formulen una cuestión prejudicial, ante el TJUE, sobre la validez de la decisión de adecuación. Por el contrario, en el caso de que no exista una decisión de adecuación emitida por la Comisión, el Tribunal resuelve que la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando esa autoridad de control considera, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero.

CUARTA.- El TJUE, en la Sentencia "Schrems II", declara la validez de la Decisión 2010/87/UE por cuanto que ésta prevé mecanismos efectivos que permiten en la práctica garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas, incluyendo la posibilidad de control por las autoridades en el caso de que por el responsable del tratamiento no se suspenda o prohíba la transferencia.

QUINTA.- El TJUE declara la invalidez de la Decisión "Escudo de Privacidad" teniendo en cuenta, por una parte, que las injerencias resultantes de los programas de vigilancia basados en la normativa de los Estados Unidos no ofrecen un nivel de protección, sustancialmente, equivalente al garantizado dentro de la Unión Europea por el RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea y, por otra parte, que el mecanismo del Defensor del Pueblo previsto en la Decisión "Escudo de Privacidad", no subsana las limitaciones al derecho a la tutela judicial efectiva, poniendo en entredicho la independencia del Defensor del Pueblo con respecto al poder ejecutivo de los Estados Unidos, poniendo de manifiesto, además, que no existe ninguna garantía legal que pueda ser invocada por los ciudadanos ante dicho Defensor del Pueblo, por lo que no se cumple con la exigencia de una vía de recurso efectivo garante del derecho a la tutela judicial efectiva en materia de protección de datos.