BASE DE DATOS DE Norma CEF.-
Referencia: NCJ064918

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
Sentencia de 16 de julio de 2020
Gran Sala
Asunto n.º C-311/18

SUMARIO:

Protección de datos personales. Transferencia de datos a un tercer país con fines comerciales. Tratamiento de los datos transferidos por las autoridades públicas de ese tercer país con fines de seguridad nacional. Nivel de protección en el tercer país. Cláusulas tipo. Garantías.
El Tribunal de Justicia declara que:

1) El artículo 2, apartados 1 y 2, del 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), debe interpretarse en el sentido de que está comprendida dentro del ámbito de aplicación de ese Reglamento una **transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero**, a pesar de que, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado.
2) El artículo 46, apartados 1 y apartado 2, letra c), del Reglamento 2016/679 debe interpretarse 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 de los Derechos Fundamentales de la Unión Europea. 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, apartado 2, del referido Reglamento.
3) El artículo 58, apartado 2, letras f) y j), del Reglamento 2016/679 debe interpretarse en el sentido de que, a no ser que exista una **decisión de adecuación válidamente adoptada por la Comisión Europea**, 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, 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, en particular, por los artículos 45 y 46 del mencionado Reglamento y por la Carta de los Derechos Fundamentales, no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismos.
4) El examen de la **Decisión 2010/87/UE** 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, en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016, a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales **no ha puesto de manifiesto la existencia de ningún elemento que pueda afectar a la validez de dicha Decisión**.
5) La Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU., **es inválida**.

PRECEPTOS:

Directiva 95/46/CE (Protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de esos datos), arts. 3.2, 25, 26.2 y .4 y 28.3.
Reglamento (UE) 2016/679 (tratamiento de datos personales), arts. 2.1 y .2, 4, 23, 44, 45, 46, 49, 51.1, 55.1, 57.1, 58.2 y .4, 64.2, 65.1, 77, 78, 94 y 99.
Decisión de la Comisión 2010/87/UE (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), arts. 1, 2, 3 y 4 y Anexo.
Decisión de Ejecución (UE) 2016/1250 (con arreglo a la Directiva 95/46 sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU), art. 1 y Anexos II, III y VI.

PONENTE:

Don T. von Danwitz.

En el asunto C-311/18,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la High Court (Tribunal Superior, Irlanda), mediante resolución de 4 de mayo de 2018, recibida en el Tribunal de Justicia el 9 de mayo de 2018, en el procedimiento entre

Data Protection Commissioner

y

Facebook Ireland Ltd,

Maximillian Schrems,

con intervención de:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. K. Lenaerts, Presidente, la Sra. R. Silva de Lapuerta, Vicepresidenta, el Sr. A. Arabadjiev, la Sra. A. Prechal, los Sres. M. Vilaras, M. Safjan, S. Rodin y P. G. Xuereb, la Sra. L. S. Rossi y el Sr. I. Jarukaitis, Presidentes de Sala, y los Sres. M. Ilešič, T. von Danwitz (Ponente) y D. Šváby, Jueces;

Abogado General: Sr. H. Saugmandsgaard Øe;

Secretaria: Sra. C. Strömholm, administradora;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 9 de julio de 2019;

consideradas las observaciones presentadas:

- en nombre del Data Protection Commissioner, por el Sr. D. Young, Solicitor, los Sres. B. Murray y M. Collins, SC, y la Sra. C. Donnelly, BL;
- en nombre de Facebook Ireland Ltd, por el Sr. P. Gallagher y la Sra. N. Hyland, SC, la Sra. A. Mulligan y el Sr. F. Kieran, BL, y los Sres. P. Nolan, C. Monaghan, C. O'Neill y R. Woulfe, Solicitors;
- en nombre del Sr. Schrems, por el Sr. H. Hofmann, Rechtsanwalt, los Sres. E. McCullough, J. Doherty y S. O'Sullivan, SC, y el Sr. G. Rudden, Solicitor;
- en nombre de The United States of America, por la Sra. E. Barrington, SC, la Sra. S. Kingston, BL, y los Sres. S. Barton y B. Walsh, Solicitors;
- en nombre de Electronic Privacy Information Centre, por la Sra. S. Lucey, Solicitor, la Sra. G. Gilmore y el Sr. A. Butler, BL, y el Sr. C. O'Dwyer, SC;
- en nombre de BSA Business Software Alliance Inc., por los Sres. B. Van Vooren y K. Van Quathem, advocaten;
- en nombre de Digitaleurope, por la Sra. N. Cahill, Barrister, el Sr. J. Cahir, Solicitor, y el Sr. M. Cush, SC;
- en nombre de Irlanda, por el Sr. A. Joyce y la Sra. M. Browne, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;
- en nombre del Gobierno belga, por los Sres. J.-C. Halleux y P. Cottin, en calidad de agentes;
- en nombre del Gobierno checo, por los Sres. M. Smolek, J. Vláčil y O. Serdula y por la Sra. A. Kasalická, en calidad de agentes;
- en nombre del Gobierno alemán, por los Sres. J. Möller, D. Klebs y T. Henze, en calidad de agentes;
- en nombre del Gobierno francés, por la Sra. A.-L. Desjonquères, en calidad de agente;
- en nombre del Gobierno neerlandés, por los Sras. C. S. Schillemans, M. K. Bulterman y M. Noort, en calidad de agentes;
- en nombre del Gobierno austriaco, por la Sra. J. Schmoll y el Sr. G. Kunnert, en calidad de agentes;
- en nombre del Gobierno polaco, por el Sr. B. Majczyna, en calidad de agente;
- en nombre del Gobierno portugués, por el Sr. L. Inez Fernandes y las Sras. A. Pimenta y C. Vieira Guerra, en calidad de agentes;
- en nombre del Gobierno del Reino Unido, por el Sr. S. Brandon, en calidad de agente, asistido por el Sr. J. Holmes, QC, y el Sr. C. Knight, Barrister;
- en nombre del Parlamento Europeo, por la Sra. M. J. Martínez Iglesias y el Sr. A. Caiola, en calidad de agentes;
- en nombre de la Comisión Europea, por los Sres. D. Nardi, H. Krämer y H. Kranenborg, en calidad de agentes;
- en nombre del Comité Europeo de Protección de Datos (EDPB), por la Sra. A. Jelinek y el Sr. K. Behn, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 19 de diciembre de 2019;

dicta la siguiente

Sentencia

1. La petición de decisión prejudicial tiene, en esencia, por objeto:

- la interpretación del artículo 3, apartado 2, primer guion, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO 1995, L 281, p. 31), en relación con el artículo 4 TUE, apartado 2, y los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).
- la interpretación y la validez de la Decisión de la Comisión 2010/87/UE, 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 (DO 2010, L 39, p. 5), en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016 (DO 2016, L 344, p. 100) (en lo sucesivo, «Decisión CPT»), así como

- la interpretación y la validez de la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46 sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU. (DO 2016, L 207, p. 1; en lo sucesivo, «Decisión EP»).

2. Esta petición se ha presentado en el contexto de un litigio entre, por una parte, el Data Protection Commissioner (Comisario para la Protección de Datos, Irlanda) (en lo sucesivo, «Comisario») y, por otra parte, Facebook Ireland Ltd y el Sr. Maximillian Schrems en relación con una reclamación presentada por este por lo que respecta a la transferencia de sus datos personales por parte de Facebook Ireland a Facebook Inc. en los Estados Unidos.

Marco jurídico

Directiva 95/46

3. El artículo 3 de la Directiva 95/46, titulado «Ámbito de aplicación», establecía en su apartado 2:

«Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

- efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

[…]».

4. El artículo 25 de la citada Directiva disponía lo siguiente:

«1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales […] únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; […]

[…]

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.»

5. El artículo 26, apartados 2 y 4, de la antedicha Directiva establecía:

«2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

[…]

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.»

6 A tenor del artículo 28, apartado 3, de la misma Directiva:

«La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;
- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

[…]»

RGPD

7. La Directiva 95/46 fue derogada y sustituida 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 y por el que se deroga la Directiva 95/46 (Reglamento general de protección de datos) (DO 2016, L 119, p. 1; en lo sucesivo, «RGPD»).

8. Los considerandos 6, 10, 101, 103, 104, 107 a 109, 114, 116 y 141 del RGPD tienen el siguiente tenor:

«(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

[…]

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales (“datos sensibles”). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

[…]

(101) Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

[…]

(103) La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.

(104) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país […] el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

[…]

(107) La Comisión puede reconocer que un tercer país, un territorio o sector específico en un tercer país, o una organización internacional ya no garantiza un nivel de protección de datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación.

(108) En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en

el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. […]

(109) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

[…]

(114) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías.

[…]

(116) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. […]

[…]

(141) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. […]»

9. El artículo 2, apartados 1 y 2, de dicho Reglamento establece:

«1. El presente Reglamento 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.

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 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.»

10. El artículo 4 del referido Reglamento dispone:

«A efectos del presente Reglamento se entenderá por:

[…]
2) "tratamiento": cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;
[…]
7) "responsable del tratamiento" o "responsable": la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;
8) "encargado del tratamiento" o "encargado": la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;
9) "destinatario": la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;
[…]».

11. El artículo 23 del mismo Reglamento establece:

«1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o [al] encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;
b) la defensa;
c) la seguridad pública;
d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;
[…]

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;
b) las categorías de datos personales de que se trate;
c) el alcance de las limitaciones establecidas;
d) las garantías para evitar accesos o transferencias ilícitos o abusivos;
e) la determinación del responsable o de categorías de responsables;
f) los plazos de conservación y las garantías aplicables, habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento;
g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.»

12. El capítulo V del RGPD, titulado «Transferencias de datos personales a terceros países u organizaciones internacionales», comprende los artículos 44 a 50 de dicho Reglamento. A tenor del artículo 44 de este, titulado «Principio general de las transferencias»:

«Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.»

13. El artículo 45 del antedicho Reglamento, titulado «Transferencias basadas en una decisión de adecuación», establece, en sus apartados 1 a 3:

«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.»

14. El artículo 46 del referido Reglamento, titulado «Transferencias mediante garantías adecuadas», dispone, en sus apartados 1 a 3:

«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.»

15. El artículo 49 del mismo Reglamento, titulado «Excepciones para situaciones específicas», establece:

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

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;
c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;
d) la transferencia sea necesaria por razones importantes de interés público;
e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otra persona, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;
g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero solo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos

imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.»

16. A tenor del artículo 51, apartado 1, del RGPD:

«Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante “autoridad de control”) supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.»

17. Con arreglo al artículo 55, apartado 1, de este Reglamento, «cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro».

18. El artículo 57, apartado 1, del citado Reglamento, establece:

«Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;
[…]
f) tratar las reclamaciones presentadas por un interesado […], e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;
[…]».

19. A tenor del artículo 58, apartados 2 y 4, del mismo Reglamento:

«2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

[…]
f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
[…]
j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

[…]

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.»

20. El artículo 64, apartado 2, del RGPD establece:

«Cualquier autoridad de control, el presidente del Comité [Europeo de Protección de Datos (EDPB)] o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.»

21. A tenor del artículo 65, apartado 1, de dicho Reglamento:

«Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

[…]
c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.»

22. El artículo 77 del referido Reglamento, titulado «Derecho a presentar una reclamación ante una autoridad de control», dispone:

«1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.»

23. El artículo 78 del mismo Reglamento, titulado «Derecho a la tutela judicial efectiva contra una autoridad de control», establece, en sus apartados 1 y 2:

«1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.»

24. El artículo 94 del RGPD dispone:

«1. Queda derogada la Directiva [95/46] con efecto a partir del 25 de mayo de 2018.

2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva [95/46] se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.»

25. Con arreglo al artículo 99 de dicho Reglamento:

«1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.

2. Será aplicable a partir del 25 de mayo de 2018.»

Decisión CPT

26. El considerando 11 de la Decisión CPT tiene el siguiente tenor:

«Las autoridades de control de los Estados miembros desempeñan una función esencial en este mecanismo contractual al garantizar la adecuada protección de los datos personales una vez realizada la transferencia. En casos excepcionales en que los exportadores de datos no quieran o no puedan informar adecuadamente a los importadores de datos y exista un riesgo inminente de que los interesados sufran un daño grave, las cláusulas contractuales tipo permitirán a las autoridades de control realizar la auditoría de los importadores de datos y los subencargados del tratamiento de datos y, en su caso, adoptar decisiones vinculantes para estos. Las autoridades de control tendrán la facultad de prohibir o suspender una transferencia o serie de transferencias que se fundamenten en las cláusulas contractuales tipo, en aquellos casos excepcionales en que se demuestre que una transferencia de este género podría tener efectos negativos considerables en las garantías y obligaciones de prestar la adecuada protección al interesado.»

27. El artículo 1 de dicha Decisión dispone:

«Se considera que las cláusulas contractuales tipo incluidas en el anexo ofrecen las garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos, según exige el artículo 26, apartado 2, de la Directiva [95/46].»

28. Con arreglo al artículo 2, párrafo segundo, de la antedicha Decisión, esta «se aplicará a la transferencia de datos personales por responsables del tratamiento establecidos en la Unión Europea a destinatarios establecidos fuera del territorio de la Unión Europea que actúen solamente como encargados del tratamiento».

29. El artículo 3 de la misma Decisión dispone lo siguiente:

«A efectos de la presente Decisión, serán aplicables las siguientes definiciones:

[…]
c) “exportador de datos”: el responsable del tratamiento que transfiera los datos personales;
d) “importador de datos”: el encargado del tratamiento establecido en un tercer país que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de este, de conformidad con sus instrucciones y los términos de la presente Decisión, y que no esté sujeto al sistema de un tercer país que garantice la protección adecuada en el sentido del artículo 25, apartado 1, de la Directiva [95/46];
[…]
f) “legislación de protección de datos aplicables”: 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;

[…]».

30. En su versión inicial, anterior a la entrada en vigor de la Decisión de Ejecución 2016/2297, el artículo 4 de la Decisión 2010/87 establecía:

«Las autoridades competentes de los Estados miembros, sin perjuicio de su facultad para iniciar acciones destinadas a garantizar el cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a los capítulos II, III, V y VI de la Directiva [95/46], podrán ejercer sus facultades para prohibir o suspender los flujos de datos hacia terceros países con objeto de proteger a las personas físicas en relación con el tratamiento de sus datos personales en los casos siguientes:

a) si se determina que la legislación a la que está sujeto el importador de datos o un subencargado del tratamiento le impone desviaciones de la legislación de protección de datos aplicable que vayan más allá de las restricciones necesarias en una sociedad democrática, como establece el artículo 13 de la Directiva [95/46], cuando tales exigencias puedan tener un importante efecto negativo sobre las garantías proporcionadas por las cláusulas contractuales tipo, o

b) si una autoridad competente decide que el importador de datos o un subencargado del tratamiento no ha respetado las cláusulas contractuales tipo del anexo, o

c) si existe la probabilidad sustancial de que las cláusulas contractuales tipo contenidas en el anexo no se estén respetando, o no se respeten en el futuro, y la continuación de la transferencia provoque un riesgo inminente de daños graves para los interesados.

2. La prohibición o suspensión con arreglo al apartado 1 se levantará tan pronto como desaparezcan las razones para dicha prohibición o suspensión.

3. Cuando los Estados miembros adopten medidas de conformidad con los apartados 1 y 2, informarán inmediatamente de ello a la Comisión, que remitirá la información a los demás Estados miembros.»

31. El considerando 5 de la Decisión de Ejecución 2016/2297, adoptada a raíz de la sentencia de 6 octubre de 2015, Schrems (C-362/14, EU:C:2015:650), tiene el siguiente tenor:

«*Mutatis mutandis*, una decisión de la Comisión adoptada de conformidad con el artículo 26, apartado 4, de la Directiva [95/46] es vinculante para todos los órganos de los Estados miembros a los que se dirige, incluidas sus autoridades de supervisión independientes, en la medida en que tiene el efecto de reconocer que las transferencias realizadas sobre la base de cláusulas contractuales tipo como las contempladas en dicha Directiva ofrecen garantías suficientes según lo establecido en su artículo 26, apartado 2. Ello no impide que una autoridad de supervisión nacional ejerza sus facultades para supervisar los flujos de datos, incluida la facultad de prohibir o suspender una transferencia de datos personales cuando constate que la transferencia se está realizando en infracción del Derecho de la Unión o de la legislación nacional en materia de protección de datos, como ocurre, por ejemplo, cuando el importador de datos no respeta las cláusulas contractuales tipo.»

32. En su versión actual, resultante de la Decisión de Ejecución 2016/2297, el artículo 4 de la Decisión CPT dispone:

«Cuando las autoridades competentes de los Estados miembros ejerzan sus facultades con arreglo al artículo 28, apartado 3, de la Directiva [95/46], y ello dé lugar a la suspensión o la prohibición definitiva de los flujos de datos hacia terceros países con el fin de proteger a las personas en lo que respecta al tratamiento de sus datos personales, el Estado miembro afectado informará inmediatamente a la Comisión, que remitirá la información a los demás Estados miembros.»

33. El anexo de la Decisión CPT, titulado «Cláusulas contractuales tipo (“encargados del tratamiento”)», comprende doce cláusulas tipo. La cláusula 3 de ese anexo, que, por su parte, tiene por título «Cláusula de tercero beneficiario», establece:

«1. Los interesados podrán exigir al exportador de datos el cumplimiento de la presente cláusula, las letras b) a i) de la cláusula 4, las letras a) a e) y g) a j) de la cláusula 5, los apartados 1 y 2 de la cláusula 6, la cláusula 7, el apartado 2 de la cláusula 8 y las cláusulas 9 a 12, como terceros beneficiarios.

2. Los interesados podrán exigir al importador de datos el cumplimiento de la presente cláusula, las letras a) a e) y g) de la cláusula 5, la cláusula 6, la cláusula 7, el apartado 2 de la cláusula 8 y las cláusulas 9 a 12, cuando el exportador de datos haya desaparecido de facto o haya cesado de existir jurídicamente, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley y a resultas de lo cual asuma los derechos y las obligaciones del exportador de datos, en cuyo caso los interesados podrán exigirlos a dicha entidad.

[…]»

34. A tenor de la cláusula 4 del referido anexo, titulada «Obligaciones del exportador de datos»:

«El exportador de datos acuerda y garantiza lo siguiente:

a) el tratamiento de los datos personales, incluida la propia transferencia, ha sido efectuado y seguirá efectuándose de conformidad con las normas pertinentes de la legislación de protección de datos aplicable (y, si procede, se ha notificado a las autoridades correspondientes del Estado miembro de establecimiento del exportador de datos) y no infringe las disposiciones legales o reglamentarias en vigor en dicho Estado miembro;

b) ha dado al importador de datos, y dará durante la prestación de los servicios de tratamiento de los datos personales, instrucciones para que el tratamiento de los datos personales transferidos se lleve a cabo exclusivamente en nombre del exportador de datos y de conformidad con la legislación de protección de datos aplicable y con las cláusulas;

[…]

f) si la transferencia incluye categorías especiales de datos, se habrá informado a los interesados, o serán informados antes de que se efectúe aquella, o en cuanto sea posible, de que sus datos podrían ser transferidos a un tercer país que no proporciona la protección adecuada en el sentido de la Directiva [95/46];

g) enviará la notificación recibida del importador de datos o de cualquier subencargado del tratamiento de datos a la autoridad de control de la protección de datos, de conformidad con la letra b) de la cláusula 5 y el apartado 3 de la cláusula 8, en caso de que decida proseguir la transferencia o levantar la suspensión;

[…]».

35. La cláusula 5 del mencionado anexo, titulada «Obligaciones del importador de datos […]», dispone:

«El importador de datos acuerda y garantiza lo siguiente:

a) tratará los datos personales transferidos solo en nombre del exportador de datos, de conformidad con sus instrucciones y las cláusulas. En caso de que no pueda cumplir estos requisitos por la razón que fuere, informará de ello sin demora al exportador de datos, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;

b) no tiene motivos para creer que la legislación que le es de aplicación le impida cumplir las instrucciones del exportador de datos y sus obligaciones a tenor del contrato y que, en caso de modificación de la legislación que pueda tener un [importante] efecto negativo sobre las garantías y obligaciones estipuladas en las cláusulas, notificará al exportador de datos dicho cambio en cuanto tenga conocimiento de él, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;

[…]

d) notificará sin demora al exportador de datos sobre:

i) toda solicitud jurídicamente vinculante de divulgar los datos personales presentada por una autoridad encargada de la aplicación de ley a menos que esté prohibido, por ejemplo, por el Derecho penal para preservar la confidencialidad de una investigación [llevada] a cabo por una de dichas autoridades,

ii) todo acceso accidental o no autorizado,

iii) toda solicitud sin respuesta recibida directamente de los interesados, a menos que se le autorice;

[…]».

36. La nota a pie de página a la que se remite el título de la referida cláusula 5 tiene el siguiente tenor:

«Las obligaciones impuestas por la legislación nacional aplicable al importador de datos que no vayan más allá de las restricciones necesarias en una sociedad democrática con arreglo a los intereses recogidos en el artículo 13, apartado 1, de la Directiva [95/46], es decir, si dichas obligaciones constituyen una medida necesaria para la salvaguardia de la seguridad del Estado; la defensa; la seguridad pública; la prevención, investigación, detección y enjuiciamiento de delitos o infracciones de la deontología en las profesiones reguladas; un interés económico o financiero importante del Estado o la protección del interesado o de los derechos y libertades de otras personas, no están en contradicción con las cláusulas contractuales tipo. […]»

37. La cláusula 6 del anexo de la Decisión CPT, titulada «Responsabilidad», establece:

«1. Las partes acuerdan que los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones mencionadas en la cláusula 3 o en la cláusula 11 por cualquier parte o subencargado del tratamiento tendrán derecho a percibir una indemnización del exportador de datos para el daño sufrido.

2. En caso de que el interesado no pueda interponer contra el exportador de datos la demanda de indemnización a que se refiere el apartado 1 por incumplimiento por parte del importador de datos o su subencargado de sus obligaciones impuestas en la cláusula 3 o en la cláusula 11, por haber desaparecido de facto, cesado de existir jurídicamente o ser insolvente, el importador de datos acepta que el interesado pueda demandarle a él en el lugar del exportador de datos […]
[…]».

38. La cláusula 8 del referido anexo, titulada «Cooperación con las autoridades de control», dispone, en su apartado 2:

«Las partes acuerdan que la autoridad de control está facultada para auditar al importador, o a cualquier subencargado, en la misma medida y condiciones en que lo haría respecto del exportador de datos conforme a la legislación de protección de datos aplicable.»

39. La cláusula 9 del antedicho anexo, titulada «Legislación aplicable», precisa que las cláusulas se regirán por la legislación del Estado miembro de establecimiento del exportador de datos.

40. A tenor de la cláusula 11 del mismo anexo, titulada «Subtratamiento de datos»:

«1. El importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas […]

2. El contrato escrito previo entre el importador de datos y el subencargado del tratamiento contendrá asimismo una cláusula de tercero beneficiario, tal como se establece en la cláusula 3, para los casos en que el interesado no pueda interponer la demanda de indemnización a que se refiere el apartado 1 de la cláusula 6 contra el exportador de datos o el importador de datos por haber estos desaparecido de facto, cesado de existir jurídicamente o ser insolventes, y ninguna entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos o del importador de datos en virtud de contrato o por ministerio de la ley. Dicha responsabilidad civil del subencargado del tratamiento se limitará a sus propias operaciones de tratamiento de datos con arreglo a las cláusulas.
[…]»

41. La cláusula 12 del anexo de la Decisión CPT, titulada «Obligaciones una vez finalizada la prestación de los servicios de tratamiento de los datos personales», dispone, en su apartado 1:

«Las partes acuerdan que, una vez finalizada la prestación de los servicios de tratamiento de los datos personales, el importador y el subencargado deberán, a discreción del exportador, o bien devolver todos los datos personales transferidos y sus copias, o bien destruirlos por completo y certificar esta circunstancia al exportador, a menos que la legislación aplicable al importador le impida devolver o destruir total o parcialmente los datos personales transferidos. […]»

Decisión EP

42. En su sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), el Tribunal de Justicia invalidó la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO 2000, L 215, p. 7), en la que la Comisión había declarado que ese país tercero garantizaba un nivel adecuado de protección.

43. A raíz de esta sentencia, la Comisión adoptó la Decisión EP, tras haber procedido, a efectos de su adopción, a una evaluación de la normativa de los Estados Unidos, como se precisa en el considerando 65 de la antedicha Decisión:

«La Comisión ha evaluado las limitaciones y salvaguardias existentes en el Derecho de los Estados Unidos con respecto al acceso a los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. y la utilización de los mismos por los poderes públicos estadounidenses a efectos de seguridad nacional, aplicación de la ley y otros fines de interés público. Asimismo, el Gobierno estadounidense, a través de su Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) […], ha proporcionado a la Comisión una serie de declaraciones y compromisos detallados que se exponen en el anexo VI de la presente Decisión. Mediante carta firmada por el secretario de Estado y adjunta como anexo III a la presente Decisión, el Gobierno de los Estados Unidos se ha comprometido asimismo a crear un nuevo mecanismo de supervisión de las injerencias con fines de seguridad nacional, a saber, el Defensor del Pueblo en el ámbito del Escudo de la privacidad, que será independiente de los servicios de inteligencia. Por último, la declaración del Departamento de Justicia de los Estados Unidos contenida en el anexo VII de la presente Decisión describe las limitaciones y salvaguardias aplicables al acceso a los datos y a su utilización por parte de los poderes públicos a efectos de aplicación de la ley y otros fines de interés público. Con vistas a mejorar la transparencia y reflejar la naturaleza jurídica de estos compromisos, cada uno de los documentos enumerados y adjuntos a la presente Decisión se publicará en el Registro Federal de los Estados Unidos.»

44. El examen realizado por la Comisión sobre esas limitaciones y salvaguardias se resume en los considerandos 67 a 135 de la Decisión EP, mientras que las conclusiones de esta institución acerca del nivel de protección adecuado en el marco del Escudo de la Privacidad UE-EE. UU. se recogen en los considerandos 136 a 141 de la referida Decisión.

45. En particular, los considerandos 68, 69, 76, 77, 109, 112 a 116, 120, 136 y 140 de la antedicha Decisión tienen el siguiente tenor:

«(68) De conformidad con la Constitución de los Estados Unidos, corresponde al presidente, en su calidad de jefe de Estado y de Gobierno y capitán general de las Fuerzas Armadas, garantizar la seguridad nacional y, por lo que respecta a la inteligencia exterior, administrar los asuntos exteriores del país […]. Si bien el Congreso está facultado para imponer limitaciones, y así lo ha hecho en diversos aspectos, el presidente podrá dirigir dentro de estos límites las actividades de los servicios de inteligencia estadounidenses, en particular mediante *executive orders* (decretos) o *presidential directives* (directivas presidenciales). […] En la actualidad, los dos principales instrumentos jurídicos en este sentido son [la] Executive Order 12333 (en lo sucesivo, “EO 12333”) […] y la Presidential Policy Directive 28 (en lo sucesivo, “PPD-28”).

(69) La PPD-28, adoptada el 17 de enero de 2014, impone una serie de limitaciones a las operaciones de “inteligencia de señales” […] Esta directiva presidencial es vinculante para los servicios de inteligencia de los

Estados Unidos […] y permanece en vigor aunque se produzcan cambios en el Gobierno estadounidense […]. La PPD-28 reviste especial importancia para los ciudadanos no estadounidenses, entre ellos los interesados de la UE. […]

[…]

(76) Aunque no se formule en tales términos jurídicos, estos principios [de la PPD-28] captan la esencia de los principios de necesidad y proporcionalidad. […]

(77) Al estar contenidos en una directiva adoptada por el presidente en calidad de Jefe de Gobierno, estos requisitos vinculan a la totalidad de los servicios de inteligencia y se han aplicado asimismo a través de una serie de normas y procedimientos institucionales que incorporan los principios generales a las instrucciones específicas aplicables a sus operaciones cotidianas. […]

[…]

(109) En cambio, con arreglo al artículo 702 de la [Foreign Intelligence Surveillance Act (FISA)], el [United States Foreign Intelligence Surveillance Court (FISC) (Tribunal de Vigilancia de la Inteligencia Exterior de los Estados Unidos)] no autoriza medidas de vigilancia individuales, sino programas de vigilancia (como PRISM o Upstream) sobre la base de certificaciones anuales elaboradas por el [United States Attorney General (fiscal general)] y el [Director of National Intelligence (DNI) (director de Inteligencia Nacional)]. […] Según se indica, las certificaciones que han de recibir el visto bueno del FISC no contienen información sobre las personas objetivo propiamente dichas, sino que identifican categorías de información de inteligencia exterior […]. Aunque el FISC no valora -sobre la base de la existencia de indicios razonables o de cualquier otra norma- si [las personas objetivo seleccionadas son adecuadas] para recabar información de inteligencia exterior […], su control abarca la condición de que uno de los principales fines de la recopilación de datos sea obtener ese tipo de información […]

[…]

(112) En primer lugar, la FISA contempla una serie de recursos, también a disposición de los ciudadanos no estadounidenses, para impugnar la vigilancia electrónica ilegal […]. Esto incluye la posibilidad para las personas de interponer una demanda de indemnización por daños y perjuicios económicos contra los Estados Unidos cuando se haya utilizado o divulgado información sobre ellas de manera intencionada y no autorizada […]; de demandar a funcionarios públicos estadounidenses a título personal (“con apariencia de legalidad”) por daños y perjuicios económicos […]; y de impugnar la legalidad de la vigilancia (y solicitar la supresión de la información) en el supuesto de que el Gobierno de los Estados Unidos pretenda utilizar o divulgar cualquier información obtenida o derivada de la vigilancia electrónica en contra del interesado en diligencias judiciales o administrativas emprendidas en dicho país […]

(113) En segundo lugar, el Gobierno estadounidense indicó a la Comisión una serie de vías adicionales que los interesados de la UE podían utilizar para presentar un recurso contra determinados funcionarios por el acceso no autorizado a datos personales y la utilización de estos por parte [d]el Gobierno, incluso con presuntos fines de seguridad nacional […]

(114) Por último, el Gobierno de los Estados Unidos ha señalado la [Freedom of information Act (FOIA) (Ley de Libertad de Información)] como instrumento a disposición de los ciudadanos no estadounidenses para solicitar acceso a los registros que obran en poder de los servicios federales, en particular cuando estos contengan datos personales del interesado […]. Tal como está planteada, la FOIA no ofrece una vía de recurso individual propiamente dicha contra las injerencias en los datos personales, si bien podría, en principio, permitir a los interesados obtener acceso a la información pertinente que poseen los servicios de inteligencia nacional. […]

(115) Si bien las personas, incluidos los interesados de la UE, disponen, por tanto, de una serie de vías de recurso cuando han sido objeto de vigilancia (electrónica) no autorizada a efectos de seguridad nacional, también es evidente que no están cubiertas todas las bases jurídicas que pueden invocar los servicios de inteligencia estadounidenses (por ejemplo, [la] EO 12333). Además, aunque los ciudadanos no estadounidenses dispongan, en

principio, de la posibilidad de recurso jurisdiccional, como en el caso de la vigilancia en virtud de la FISA, los medios de acción previstos son limitados […] y las demandas interpuestas por personas físicas (incluidos los ciudadanos estadounidenses) se declararán improcedentes cuando estas no puedan demostrar su legitimación […], lo que restringe el acceso a los órganos jurisdiccionales ordinarios […]

(116) Con miras a proporcionar una vía complementaria de recurso accesible a todos los interesados de la UE, el Gobierno de los Estados Unidos ha decidido crear una nueva figura, a saber, el Defensor del Pueblo, tal como se describe en la carta del Secretario de Estado a la Comisión, contenida en el anexo III de la presente Decisión. Dicha figura se basa en la designación, en virtud de la PPD-28, de un coordinador superior (con la categoría de subsecretario) en el seno del Departamento de Estado como punto de contacto para los gobiernos extranjeros que planteen cuestiones con respecto a las actividades de inteligencia de señales de los Estados Unidos, pero su cometido es mucho más amplio que el concepto original.

[…]

(120) […] El Gobierno de los EE. UU. se compromete a garantizar que, en el ejercicio de sus funciones, el Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá apoyarse en la cooperación de otros mecanismos de verificación del cumplimiento y de supervisión previstos en el Derecho estadounidense. […] En los casos en que se haya detectado algún incumplimiento por parte de uno de estos organismos de supervisión, el servicio de inteligencia en cuestión (por ejemplo, una agencia de inteligencia) deberá corregir el incumplimiento, ya que solo de este modo podrá el Defensor del Pueblo garantizar una respuesta "positiva" a la persona (es decir, que se ha subsanado el incumplimiento), con arreglo al compromiso del Gobierno de los EE. UU. […]

[…]

(136) A la luz de las constataciones anteriormente expuestas, la Comisión considera que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades autocertificadas en el marco del Escudo de la privacidad UE-EE. UU.

[…]

(140) Por último, sobre la base de la información disponible acerca del ordenamiento jurídico de los Estados Unidos, incluidas las declaraciones y compromisos prestados por el Gobierno estadounidense, la Comisión opina que las injerencias de los poderes públicos de los Estados Unidos en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a dicho país en el marco del Escudo de la privacidad a efectos de seguridad nacional, aplicación de la ley u otros fines de interés público, y las consiguientes restricciones impuestas a las entidades autocertificadas con respecto a su adhesión a los principios de privacidad, se limitarán a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que existe una tutela judicial efectiva frente a tales injerencias.»

46. A tenor del artículo 1 de la Decisión EP:

«1. A los efectos del artículo 25, apartado 2, de la Directiva [95/46], los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en los Estados Unidos en el marco del Escudo de la privacidad UE-EE. UU.

2. El Escudo de la privacidad UE-EE. UU. se compone de los principios establecidos por el Departamento de Comercio de los Estados Unidos el 7 de julio de 2016, tal como se exponen en el anexo II, y en los compromisos y declaraciones oficiales recogidos en los documentos enumerados en los anexos I y III a VII.

3. A los efectos del apartado 1, se considerarán datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. aquellos que hayan sido transferidos desde la Unión a entidades establecidas en los Estados Unidos que figuren en la denominada "lista del Escudo de la privacidad", mantenida y puesta a disposición del público por el Departamento de Comercio de los Estados Unidos, de conformidad con las secciones I a III de los principios expuestos en el anexo II.»

47. El anexo II de la Decisión EP, titulado «Principios del marco del Escudo de la privacidad UE-EE. UU. publicados por el Departamento de Comercio estadounidense», dispone, en su punto I.5., que la adhesión a estos principios puede verse limitada, en particular, por «exigencias de seguridad nacional, interés público y cumplimiento de la ley».

48. El anexo III de la referida Decisión contiene una carta del Sr. John Kerry, entonces Secretary of State (secretario de Estado, Estados Unidos), a la comisaria de Justicia, Consumidores e Igualdad de Género, de 7 de julio de 2016, a la que se adjunta, como anexo A, un memorando titulado «La figura del Defensor del Pueblo en el ámbito del Escudo de la privacidad UE-EE. UU. con relación a la inteligencia de señales», que contiene el siguiente pasaje:

«En reconocimiento a la importancia del marco del Escudo de la Privacidad UE-EE. UU., este memorando establece el procedimiento para la implantación de un nuevo mecanismo, en virtud de la Presidential Policy Directive 28 (PPD-28), que contempla la inteligencia de señales.

[…] El presidente Obama anunció la publicación de una nueva directiva presidencial, la PPD-28, para "exponer con claridad lo que hacemos y lo que no hacemos en lo que se refiere a nuestra vigilancia en el extranjero".

El artículo 4(d) de la PPD-28 exige que el secretario de Estado designe un "Senior Coordinator for International Information Technology Diplomacy" [(coordinador superior de la diplomacia internacional en materia de tecnología de la información)] (coordinador superior) "para […] que actúe como punto de contacto con los gobiernos extranjeros que deseen plantear sus dudas con respecto a las actividades de la inteligencia de señales llevadas a cabo por los Estados Unidos".

[…]

1) [El coordinador superior] actuará de defensor del pueblo en el ámbito del Escudo de la Privacidad y […] trabajará estrechamente con los funcionarios de otros departamentos y organismos responsables del tratamiento de las solicitudes de conformidad con la legislación y la política aplicable de los Estados Unidos. El defensor del pueblo es independiente de los servicios de inteligencia. El defensor del pueblo informará directamente al secretario de Estado, que garantizará que aquel desempeñe sus funciones de manera objetiva y sin ninguna influencia indebida que pueda afectar a la respuesta que debe proporcionarse.

[…]»

49. El anexo VI de la Decisión EP contiene una carta de la Oficina del Director de Inteligencia Nacional (Office of the Director of National Intelligence) al Departamento de Comercio de los Estados Unidos y a la Administración del Comercio Internacional, de 21 de junio de 2016, en la que se precisa que la PPD-28 permite llevar a cabo una «recopilación "en bloque" […] de una cantidad relativamente grande de información o datos de inteligencia de señales en circunstancias en las que los servicios de inteligencia no puedan utilizar un identificador asociado a un criterio de selección específico […] para orientar la recopilación».

Litigio principal y cuestiones prejudiciales

50. El Sr. Schrems, nacional austriaco residente en Austria, es usuario de la red social Facebook (en lo sucesivo, «Facebook») desde 2008.

51. Toda persona residente en el territorio de la Unión que desee utilizar Facebook debe celebrar, en el momento de su inscripción, un contrato con Facebook Ireland, filial de Facebook Inc., que a su vez está establecida en los Estados Unidos. Los datos personales de los usuarios de Facebook residentes en el territorio de la Unión se transfieren total o parcialmente a servidores pertenecientes a Facebook Inc., situados en el territorio de Estados Unidos, donde son objeto de tratamiento.

52. El 25 de junio de 2013, el Sr. Schrems presentó ante el Comisario una reclamación en la que le solicitaba, en esencia, que prohibiera a Facebook Ireland transferir sus datos personales a los Estados Unidos, alegando que el Derecho y las prácticas en vigor en ese 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, que los Estados Unidos ofrecían un nivel adecuado de protección.

53. La High Court (Tribunal Superior, Irlanda), ante la que el Sr. Schrems había interpuesto un recurso contra la desestimación de su reclamación, planteó al Tribunal de Justicia una petición de decisión prejudicial relativa a la interpretación y a la validez de la Decisión 2000/520. Mediante sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), el Tribunal de Justicia declaró inválida la referida Decisión.

54. A raíz de dicha sentencia, el órgano jurisdiccional remitente anuló la desestimación de la reclamación del Sr. Schrems y se la devolvió al Comisario. En el marco de la investigación abierta por este último, Facebook Ireland explicó 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 CPT. Habida cuenta de esos elementos, el Comisario instó al Sr. Schrems a modificar su reclamación.

55. En su reclamación modificada, presentada el 1 de diciembre de 2015, el Sr. Schrems alegó, en particular, 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). Esgrimió que, al utilizarse esos datos en el marco de diferentes programas de vigilancia de una manera incompatible con los artículos 7, 8 y 47 de la Carta, la Decisión CPT no puede justificar la transferencia de esos datos a los Estados Unidos. En esas condiciones, el Sr. Schrems solicitó al Comisario que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.

56. El 24 de mayo de 2016, el Comisario publicó un «proyecto de decisión» en el que se resumían las conclusiones provisionales de su investigación. En dicho proyecto, consideró con carácter provisional que los datos personales de ciudadanos de la Unión 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 solo confieren a los interesados derechos contractuales contra el exportador o el importador de los datos, sin vincular a las autoridades estadounidenses.

57. Al considerar que, en esas circunstancias, la reclamación modificada del Sr. Schrems planteaba la cuestión de la validez de la Decisión CPT, 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 de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), apartado 65, a efectos de que esta última pregunte al Tribunal de Justicia acerca de esta cuestión. Mediante resolución de 4 de mayo de 2018, la High Court (Tribunal Superior) planteó la presente petición de decisión prejudicial ante el Tribunal de Justicia.

58. La High Court (Tribunal Superior) ha adjuntado a dicha petición de decisión prejudicial una sentencia dictada el 3 de octubre de 2017, en la que había reseñado el resultado del examen de las pruebas que se le habían aportado en el marco del procedimiento nacional, procedimiento en el que había participado el Gobierno estadounidense.

59. En esa sentencia, a la que la petición de decisión prejudicial hace referencia en varias ocasiones, el órgano jurisdiccional remitente señaló que, en principio, no solo tiene el derecho, sino también la obligación de examinar la totalidad de los hechos y argumentos invocados ante ella para decidir, basándose en ellos, si una remisión prejudicial es necesaria o no. En cualquier caso, señaló, que estaba obligado a tener en cuenta las posibles modificaciones del Derecho que tuviesen lugar entre la interposición del recurso y la vista que se organizase ante él. Dicho órgano jurisdiccional precisó que, en el marco del procedimiento principal, su propia apreciación no se limitaba a los motivos de invalidez invocados por el Comisario, sino que también podía plantear de oficio otros motivos de invalidez y, basándose en ellos, proceder a una remisión prejudicial.

60. Conforme a las apreciaciones efectuadas en la referida sentencia, las actividades de inteligencia de las autoridades estadounidenses por lo que atañe a los datos personales transferidos a los Estados Unidos se basan, en particular, en el artículo 702 de la FISA y en la E.O. 12333.

61. Por lo que respecta al artículo 702 de la FISA, el órgano jurisdiccional remitente precisa, en la misma sentencia, que dicho artículo permite al fiscal general y al director de los Servicios de Inteligencia Nacionales autorizar conjuntamente, previa aprobación del FISC, con el fin de obtener «información en materia de inteligencia exterior», la vigilancia de personas no nacionales de los Estados Unidos que se encuentren fuera del territorio de ese país y sirve, en particular, de fundamento a los programas de vigilancia PRISM y Upstream. En el marco del programa PRISM, los proveedores de servicios de Internet están obligados, según las apreciaciones del referido órgano jurisdiccional, a proporcionar a la NSA todas las comunicaciones enviadas y recibidas por un «selector», de las cuales una parte se transmite también al FBI y a la Central Intelligence Agency (CIA) (Agencia Central de Inteligencia).

62. En lo que se refiere al programa Upstream, el antedicho órgano jurisdiccional ha observado que, en el marco de este programa, las empresas de telecomunicaciones que explotan la «red troncal» de Internet -es decir, la red de cables, conmutadores y enrutadores- están obligadas a permitir a la NSA copiar y filtrar los flujos de tráfico de Internet con el fin de recabar comunicaciones enviadas o recibidas por el nacional no americano al que corresponda un «selector» o que estén relacionadas con esa persona. En el marco de ese programa, conforme a las apreciaciones de ese mismo órgano jurisdiccional, la NSA tiene acceso tanto a los metadatos como al contenido de las comunicaciones de que se trate.

63. Por lo que se refiere a la E.O. 12333, el órgano jurisdiccional remitente observa que esta permite a la NSA acceder a datos «en tránsito» hacia los Estados Unidos, accediendo a los cables submarinos situados en el lecho del Atlántico, así como recabar y conservar esos datos antes de que lleguen a los Estados Unidos y estén sujetos a las disposiciones de la FISA. El órgano jurisdiccional remitente precisa que las actividades basadas en la E.O. 12333 no se rigen por la ley.

64. Por lo que atañe a los límites establecidos con respecto a las actividades de inteligencia, el órgano jurisdiccional remitente pone de relieve el hecho de que a las personas que no son nacionales de Estados Unidos únicamente se les aplica la PPD-28 y que esta se limita a indicar que las actividades de inteligencia deben ser «lo más adaptadas posible» (*as tailored as feasible*). Basándose en estas apreciaciones, el antedicho órgano jurisdiccional considera que los Estados Unidos llevan a cabo un tratamiento de datos en masa, sin garantizar una protección sustancialmente equivalente a la garantizada por los artículos 7 y 8 de la Carta.

65. En lo que se refiere a la tutela judicial, ese mismo órgano jurisdiccional expone que los ciudadanos de la Unión no tienen acceso a los mismos recursos de los que disponen los nacionales estadounidenses contra el tratamiento de datos personales por parte de las autoridades estadounidenses, ya que la cuarta enmienda de la Constitution of the United States (Constitución de los Estados Unidos), que constituye, en el Derecho estadounidense, la protección más importante contra la vigilancia ilegal, no es aplicable a los ciudadanos de la Unión. A este respecto, el órgano jurisdiccional remitente precisa que los recursos de que disponen estos últimos se enfrentan a obstáculos importantes, en particular, la obligación -a su juicio, excesivamente difícil de cumplir- de justificar su legitimación activa. Asimismo, según las apreciaciones del referido órgano jurisdiccional, las actividades de la NSA basadas en la E.O. 12333 no son objeto de control jurisdiccional y no pueden interponerse contra ellas recursos judiciales. Finalmente, el antedicho órgano jurisdiccional considera que, en la medida en que, a su entender, el Defensor del Pueblo en el ámbito del Escudo de la Privacidad no constituye un tribunal, en el sentido del artículo 47 de la Carta, el Derecho estadounidense no garantiza a los ciudadanos de la Unión un nivel de protección sustancialmente equivalente al garantizado por el derecho fundamental reconocido en ese artículo.

66. En su petición de decisión prejudicial, el órgano jurisdiccional remitente precisa, además, que las partes en el procedimiento principal discrepan, en particular, sobre la cuestión de la aplicabilidad del Derecho de la Unión a las transferencias a un país tercero de datos personales que puedan ser tratados por las autoridades de ese país, concretamente, con fines de seguridad nacional, así como sobre los elementos que deben tenerse en cuenta para la apreciación del nivel de protección adecuado garantizado por el referido país. En particular, el antedicho órgano jurisdiccional señala que, según Facebook Ireland, las constataciones de la Comisión relativas a la adecuación del nivel de protección garantizado por un país tercero, como las recogidas en la Decisión EP, vinculan a las autoridades de control también en el contexto de una transferencia de datos personales basada en las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT.

67. Por lo que atañe a las cláusulas tipo de protección de datos, el referido órgano jurisdiccional se pregunta si la Decisión CPT puede considerarse válida, dado que, según ese mismo órgano jurisdiccional, las mencionadas cláusulas no tienen carácter vinculante para las autoridades estatales del país tercero de que se trata y, por tanto, no pueden subsanar una eventual falta de nivel de protección adecuado en ese país. A este respecto, estima que la posibilidad, reconocida a las autoridades competentes de los Estados miembros, en el artículo 4, apartado 1, letra a), de la Decisión 2010/87, en su versión anterior a la entrada en vigor de la Decisión de Ejecución 2016/2297, de prohibir las transferencias de datos personales a un país tercero que imponga al importador obligaciones incompatibles con las garantías contenidas en esas mismas cláusulas demuestra que la situación del Derecho del país tercero puede justificar la prohibición de una transferencia de datos, aunque esta se realice sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT y, por tanto, pone de manifiesto que estas pueden ser insuficientes para garantizar una protección adecuada. No obstante, el órgano jurisdiccional remitente plantea sus dudas acerca del alcance de la facultad del Comisario de prohibir una transferencia de datos basada en esas cláusulas, considerando al mismo tiempo que una potestad discrecional no es suficiente para garantizar una protección adecuada.

68. En estas circunstancias, la High Court (Tribunal Superior) decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

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

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

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

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

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

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

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

o bien

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sobre la admisibilidad de la petición de decisión prejudicial

69. Facebook Ireland y los Gobiernos alemán y del Reino Unido alegan que la petición de decisión prejudicial es inadmisible.

70. En lo que se refiere a la excepción propuesta por Facebook Ireland debe señalarse que esta sociedad considera que las disposiciones de la Directiva 95/46 en las que se basan las cuestiones prejudiciales fueron derogadas por el RGPD.

71. A este respecto, es preciso observar que, si bien, en virtud del artículo 94, apartado 1, del RGPD, la Directiva 95/46 fue derogada con efecto a partir del 25 de mayo de 2018, dicha Directiva estaba todavía en vigor en el momento de la formulación, el 4 de mayo de 2018, de la presente petición de decisión prejudicial recibida en el Tribunal de Justicia el 9 de mayo de 2018. Asimismo, los artículos 3, apartado 2, primer guion, 25, 26 y 28, apartado 3, de la Directiva 95/46, a los que se refieren las cuestiones prejudiciales, fueron, en esencia, reproducidos en los artículos 2, apartado 2, 45, 46 y 58 del RGPD, respectivamente. Por otra parte, hay que recordar que el Tribunal de Justicia tiene la misión de interpretar cuantas disposiciones del Derecho de la Unión sean necesarias para que los órganos jurisdiccionales nacionales puedan resolver los litigios que se les hayan sometido, aun cuando tales disposiciones no se mencionen expresamente en las cuestiones remitidas por dichos órganos jurisdiccionales (sentencia de 2 de abril de 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, apartado 43 y jurisprudencia citada). Por esos distintos motivos, el hecho de que el órgano jurisdiccional remitente haya formulado las cuestiones prejudiciales refiriéndose únicamente a las disposiciones de la Directiva 95/46 no puede dar lugar a la inadmisibilidad de la presente petición de decisión prejudicial.

72. Por su parte, el Gobierno alemán basa su excepción de inadmisibilidad, por un lado, en que el Comisario solo ha expuesto dudas, y no una opinión definitiva, sobre la cuestión de la validez de la Decisión CPT y, por otro lado, en que el órgano jurisdiccional remitente se abstuvo de comprobar si el Sr. Schrems había dado su consentimiento de forma indubitada a las transferencias de datos de que se trata en el procedimiento principal, lo que, en caso de haber sido así, tendría como efecto hacer innecesaria una respuesta a esa cuestión. Finalmente, según el Gobierno del Reino Unido, las cuestiones prejudiciales tienen carácter hipotético, dado que el referido órgano jurisdiccional no ha constatado que esos datos hubiesen sido efectivamente transferidos sobre la base de la antedicha Decisión.

73. De reiterada jurisprudencia se desprende que corresponde exclusivamente al juez nacional que conoce del litigio y que debe asumir la responsabilidad de la decisión jurisdiccional que se ha de pronunciar apreciar, a la luz de las particularidades del asunto, tanto la necesidad de una decisión prejudicial para poder dictar sentencia como la pertinencia de las cuestiones que plantea al Tribunal de Justicia. Por consiguiente, cuando las cuestiones planteadas se refieren a la interpretación o a la validez de una norma del Derecho de la Unión, en principio, el Tribunal de Justicia está obligado a pronunciarse. De ello se deduce que las cuestiones planteadas por los órganos jurisdiccionales nacionales disfrutan de una presunción de pertinencia. La negativa del Tribunal de Justicia a pronunciarse sobre una cuestión prejudicial planteada por un órgano jurisdiccional nacional solo es posible cuando resulta evidente que la interpretación solicitada no tiene relación alguna con la realidad o con el objeto del litigio principal, cuando el problema sea de naturaleza hipotética o cuando el Tribunal de Justicia no disponga de los elementos de hecho y de Derecho necesarios para responder adecuadamente a las cuestiones que se le hayan planteado (sentencias de 16 de junio de 2015, Gauweiler y otros, C-62/14, EU:C:2015:400, apartados 24 y 25; de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, apartado 45, y de 19 de diciembre de 2019, Dobersberger, C-16/18, EU:C:2019:1110, apartados 18 y 19).

74. En el caso de autos, la petición de decisión prejudicial contiene elementos de hecho y Derecho suficientes para comprender el alcance de las cuestiones prejudiciales. Asimismo, y ante todo, ningún elemento de los autos que obran en poder del Tribunal de Justicia permite considerar que la interpretación del Derecho de la Unión que se solicita no tenga relación con la realidad o con el objeto del litigio principal o sea de naturaleza hipotética, en particular, debido al hecho de que la transferencia de datos personales de que se trata en el litigio principal se fundamentase en el consentimiento explícito de la persona afectada por esa transferencia, y no en la Decisión CPT. En efecto, según las indicaciones que figuran en la referida petición de decisión prejudicial, Facebook Ireland reconoció que transfiere a Facebook Inc. los datos personales de sus abonados residentes en la Unión y

que una gran parte de esas transferencias, cuya legalidad impugna el Sr. Schrems, se realiza sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT.

75. Por otra parte, no tiene relevancia por lo que atañe a la admisibilidad de la presente petición de decisión prejudicial que el Comisario no haya dado una opinión definitiva sobre la validez de la referida Decisión, ya que el órgano jurisdiccional remitente considera que la respuesta a las cuestiones prejudiciales relativas a la interpretación y a la validez de las normas del Derecho de la Unión es necesaria para resolver el litigio principal.

76. De las anteriores consideraciones se desprende que la petición de decisión prejudicial es admisible.

Sobre las cuestiones prejudiciales

77. Con carácter preliminar, debe recordarse que la presente petición de decisión prejudicial tiene su origen en una reclamación del Sr. Schrems que tiene por objeto que el Comisario ordene la suspensión o la prohibición, para el futuro, de la transferencia por parte de Facebook Ireland de sus datos personales a Facebook Inc. Pues bien, aunque las cuestiones prejudiciales se refieren a las disposiciones de la Directiva 95/46, ha quedado acreditado 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.

78. Esta ausencia de decisión nacional diferencia la situación de que se trata en el procedimiento principal de las que dieron lugar a las sentencias de 24 de septiembre de 2019, Google (Alcance territorial del derecho a la retirada de enlaces), (C-507/17, EU:C:2019:772), y de 1 de octubre de 2019, Planet49 (C-673/17, EU:C:2019:801), en las que eran objeto de litigio decisiones adoptadas con anterioridad a la derogación de la referida Directiva.

79. Por tanto, procede dar respuesta a las cuestiones prejudiciales a la luz de las disposiciones del RGPD, y no de las disposiciones de la Directiva 95/46.

Sobre la primera cuestión prejudicial

80. Mediante la primera cuestión prejudicial, el órgano jurisdiccional remitente solicita, en esencia, que se dilucide si el artículo 2, apartados 1 y 2, letras a), b) y d), del RGPD, en relación con el artículo 4 TUE, apartado 2, debe interpretarse en el sentido de que está comprendida dentro del ámbito de aplicación de ese Reglamento 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.

81. A este respecto, procede señalar, para empezar, que la disposición recogida en el artículo 4 TUE, apartado 2, según la cual, en la Unión, la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro, atañe únicamente a los Estados miembros de la Unión. Por consiguiente, esa disposición no es pertinente, en el caso de autos, para interpretar el artículo 2, apartados 1 y 2, letras a), b) y d), del RGPD.

82. A tenor de su artículo 2, apartado 1, 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. El artículo 4, punto 2, de dicho Reglamento define el 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» y cita, como ejemplos, la «comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso», sin hacer ninguna distinción en función de que esas operaciones se realicen en el interior de la Unión o tengan un vínculo con un país tercero. Asimismo, el referido Reglamento 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, además, a las autoridades de control poderes específicos a ese efecto, que se recogen en el artículo 58, apartado 2, letra j), del mismo Reglamento.

83. De ello se desprende que la operación consistente en hacer transferir datos personales desde un Estado miembro a un tercer país constituye por sí misma un tratamiento de datos personales, en el sentido del artículo 4, punto 2, del RGPD, realizado en el territorio de un Estado miembro, tratamiento al que dicho Reglamento se aplica en virtud de su artículo 2, apartado 1 [véase por analogía, por lo que respecta a los artículos 2, letra b), y 3, apartado 1, de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 45 y jurisprudencia citada].

84. Por lo que atañe a la cuestión de si una operación de ese tipo puede considerarse excluida del ámbito de aplicación del RGPD en virtud del artículo 2, apartado 2, de este, debe recordarse que dicha disposición establece excepciones al ámbito de aplicación de dicho Reglamento, tal como se define en su artículo 2, apartado 1, y que esas excepciones deben interpretarse en sentido estricto (véase por analogía, por lo que respecta al artículo 3, apartado 2, de la Directiva 95/46, la sentencia de 10 de julio de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, apartado 37 y jurisprudencia citada).

85. En el caso de autos, al haber sido realizada la transferencia de datos personales de que se trata en el 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, 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 (véase por analogía, por lo que respecta al artículo 3, apartado 2, de la Directiva 95/46, la sentencia de 10 de julio de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, apartado 38 y jurisprudencia citada).

86. Pues bien, 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.

87. Asimismo, al obligar explícitamente a la Comisión, cuando esta evalúa la adecuación del nivel de protección ofrecido por un país tercero, a tener en cuenta, en particular, «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», el propio tenor del artículo 45, apartado 2, letra a), del referido Reglamento pone de manifiesto el hecho de que el eventual tratamiento por un país tercero de los datos en cuestión con fines de seguridad pública, defensa y seguridad del Estado no pone en entredicho la aplicabilidad del antedicho Reglamento a la transferencia de que se trata.

88. De lo anterior se desprende que esa transferencia no puede quedar excluida del ámbito de aplicación del RGPD basándose en que los datos de que se trata pueden ser tratados, en el transcurso de la transferencia o tras ella, por las autoridades del país tercero en cuestión con fines de seguridad pública, defensa y seguridad del Estado.

89. Por tanto, procede responder a la primera cuestión prejudicial que el artículo 2, apartados 1 y 2, del RGPD debe interpretarse en el sentido de que está comprendida dentro del ámbito de aplicación de ese Reglamento una transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, a pesar del hecho de que, en el transcurso de dicha transferencia o tras ella, esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado.

Sobre las cuestiones prejudiciales segunda, tercera y sexta

90. En sus cuestiones prejudiciales segunda, tercera y sexta, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia acerca del nivel de protección exigido en el artículo 46, apartados 1 y 2, letra c), del RGPD en el marco de una transferencia de datos personales a un país tercero basada en cláusulas tipo de

protección de datos. En particular, dicho órgano jurisdiccional solicita al Tribunal de Justicia que precise los elementos que han de tomarse en consideración a efectos de determinar si ese nivel de protección está garantizado en el contexto de tal transferencia.

91. Por lo que atañe al nivel de protección exigido, de una lectura conjunta de esas disposiciones se desprende que, cuando no existe una decisión de adecuación adoptada en virtud del artículo 45, 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» y a condición de que los interesados cuenten «con derechos exigibles y acciones legales efectivas», pudiendo proporcionarse esas garantías adecuadas, en particular, mediante cláusulas tipo de protección de datos adoptadas por la Comisión.

92. Si bien el artículo 46 del RGPD no precisa la naturaleza de las exigencias que se derivan de esa referencia a las «garantías adecuadas», a los «derechos exigibles» y a las «acciones legales efectivas», debe señalarse que el antedicho artículo se encuentra en el capítulo V del referido Reglamento y, por tanto, debe interpretarse a la luz del artículo 44 del mencionado Reglamento, titulado «Principio general de las transferencias», que dispone que «todas las disposiciones [de dicho capítulo» se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el [mismo] Reglamento no se vea menoscabado». Por tanto, ese nivel de protección debe garantizarse con independencia de cuál sea la disposición del referido capítulo sobre cuya base se realice una transferencia de datos personales a un país tercero.

93. En efecto, como ha señalado el Abogado General en el punto 117 de sus conclusiones, las disposiciones del capítulo V del RGPD tienen como finalidad garantizar la continuidad del elevado nivel de esa protección cuando se produzca una transferencia de datos personales a un país tercero, de conformidad con el objetivo precisado en el considerando 6 del antedicho Reglamento.

94. El artículo 45, 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 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 Unión, 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 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 (véase por analogía, por 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).

95. En este contexto, el considerando 107 del RGPD dispone que, cuando «un tercer país, un territorio o sector específico en un tercer país […] ya no garantiza un nivel de protección de datos adecuado […], debe prohibirse la transferencia de datos personales a dicho tercer país […], salvo que se cumplan los requisitos [de dicho Reglamento] relativos a las transferencias basadas en garantías adecuadas». A tal efecto, el considerando 108 del referido Reglamento precisa que, en ausencia de una decisión por la que se constate la adecuación de la protección de los datos, las garantías adecuadas que corresponda adoptar al responsable o el encargado del tratamiento con arreglo al artículo 46, apartado 1, del mismo Reglamento deben «compensar la falta de protección de datos en un tercer país» para «asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión».

96. De ello se desprende, como ha señalado el Abogado General en el punto 115 de sus conclusiones, que esas 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.

97. El órgano jurisdiccional remitente se pregunta también si ese nivel de protección sustancialmente equivalente al garantizado dentro de la Unión debe 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 derechos fundamentales reconocidos en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en lo sucesivo, «CEDH») o también a la luz del Derecho nacional de los Estados miembros.

98. A este respecto, debe recordarse que, si bien, como confirma el artículo 6 TUE, apartado 3, los derechos fundamentales reconocidos por el CEDH forman parte del Derecho de la Unión como principios generales y el artículo 52, apartado 3, de la Carta dispone que los derechos contenidos en ella que correspondan a derechos garantizados por el CEDH tienen el mismo sentido y alcance que les confiere dicho Convenio, este no constituye, dado que la Unión no se ha adherido a él, un instrumento jurídico integrado formalmente en el ordenamiento jurídico de la Unión (sentencias de 26 de febrero de 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, apartado 44 y jurisprudencia citada, y de 20 de marzo de 2018, Menci, C-524/15, EU:C:2018:197, apartado 22).

99. En estas circunstancias, el Tribunal de Justicia ha declarado que la interpretación del Derecho de la Unión y el examen de la validez de los actos de la Unión deben basarse en los derechos fundamentales garantizados por la Carta (véase, por analogía, la sentencia de 20 de marzo de 2018, Menci, C-524/15, EU:C:2018:197, apartado 24).

100. Asimismo, es de reiterada jurisprudencia que la validez de las disposiciones del Derecho de la Unión y, a falta de una remisión expresa al Derecho nacional de los Estados miembros, su interpretación no pueden apreciarse a la luz de dicho Derecho nacional, incluso de rango constitucional y, en particular, de los derechos fundamentales tal y como están formulados en su constitución nacional (véanse, en este sentido, las sentencias de 17 de diciembre de 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, apartado 3; de 13 de diciembre de 1979, Hauer, 44/79, EU:C:1979:290, apartado 14, y de 18 de octubre de 2016, Nikiforidis, C-135/15, EU:C:2016:774, apartado 28 y jurisprudencia citada).

101. De lo anterior se deriva que, cuando, por una parte, una transferencia de datos personales, como aquella de que se trata en el litigio principal, realizada con fines comerciales por un operador económico establecido en un Estado miembro, con destino a otro operador económico establecido en un país tercero, está comprendida, como se desprende de la respuesta a la primera cuestión prejudicial, dentro del ámbito de aplicación del RGPD y cuando, por otra parte, dicho Reglamento tiene como finalidad, en particular, tal y como se desprende de su considerando 10, garantizar un nivel uniforme y elevado de protección de las personas físicas dentro de la Unión y, a tal efecto, garantizar en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de esas personas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea, 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.

102. El órgano jurisdiccional remitente desea asimismo saber qué elementos deben 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.

103. A este respecto, si bien esa disposición no enumera los diferentes elementos que han de tenerse en cuenta para evaluar la adecuación del nivel de protección que debe respetarse en el marco de una transferencia de esas características, el artículo 46, apartado 1, del referido Reglamento precisa que los interesados deben gozar de garantías adecuadas y contar con derechos exigibles y acciones legales efectivas.

104. La evaluación requerida a tal efecto 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 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 transferidos, los elementos pertinentes del sistema jurídico de dicho país. En lo que a este último aspecto se refiere, los elementos que deben tomarse en consideración en el contexto del artículo 46 del antedicho Reglamento se corresponden con los mencionados, de modo no exhaustivo, en el artículo 45, apartado 2, de este.

105. Por tanto, procede responder a las cuestiones prejudiciales segunda, tercera y sexta que el artículo 46, apartados 1 y 2, letra c), del RGPD debe interpretarse 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 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 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, apartado 2, del referido Reglamento.

Sobre la octava cuestión prejudicial

106. Mediante la octava cuestión prejudicial, el órgano jurisdiccional remitente solicita, en esencia, que se dilucide si el artículo 58, apartado 2, letras f) y j), del RGPD debe interpretarse en el sentido de que la autoridad de control competente está obligada 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 esa autoridad de control considera 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, en particular, por los artículos 45 y 46 del RGPD y por la Carta, no puede garantizarse, o en el sentido de que el ejercicio de esas facultades está limitado a supuestos excepcionales.

107. Conforme al artículo 8, apartado 3, de la Carta y al artículo 51, apartado 1, y al artículo 57, apartado 1, letra a), del RGPD, las autoridades nacionales de control están encargadas del control del cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales. Por tanto, cada una de ellas está investida de la competencia para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad hacia un tercer país respeta las exigencias establecidas por el antedicho Reglamento (véase por analogía, por lo que respecta al artículo 28 de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 47).

108. De las anteriores disposiciones se deriva que las autoridades de control tienen como misión principal controlar la aplicación del RGPD y velar por su cumplimiento. El ejercicio de esta misión tiene una especial importancia en el contexto de una transferencia de datos personales a un país tercero, dado que, como se desprende del propio tenor del considerando 116 del referido Reglamento, «cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información». En ese supuesto, tal como se precisa en ese mismo considerando, «es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras».

109. Asimismo, en virtud del artículo 57, apartado 1, letra f), del RGPD, incumbirá a cada autoridad de control, en su territorio, tratar las reclamaciones que cualquier persona, de conformidad con el artículo 77, apartado 1, del antedicho Reglamento, pueda presentar si considera que el tratamiento de datos personales que le conciernen infringe el referido Reglamento y examinar su objeto en la medida en que sea necesario. La autoridad de control debe proceder al tratamiento de esas reclamaciones con toda la diligencia exigible (véase por analogía, por lo que respecta al artículo25, apartado 6, de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 63).

110. El artículo 78, apartados 1 y 2, del RGPD reconoce a toda persona el derecho a la tutela judicial efectiva, en particular, cuando la autoridad de control no da curso a su reclamación. El considerando 141 del antedicho Reglamento hace también referencia a ese «derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta» en caso de que la mencionada autoridad de control «no actúe cuando sea necesario para proteger los derechos del interesado».

111. Para permitirles tratar las reclamaciones presentadas, el artículo 58, apartado 1, del RGPD confiere a cada autoridad de control importantes poderes de investigación. Cuando una de esas autoridades considera, al finalizar su investigación, que el interesado cuyos datos personales se transfirieron a un país tercero no goza en ese país de un nivel de protección adecuado, está obligada, en aplicación del Derecho de la Unión, a reaccionar de modo adecuado con el fin de subsanar la insuficiencia constatada, con independencia del origen o la naturaleza de dicha insuficiencia. A tal efecto, el artículo 58, apartado 2, del referido Reglamento enumera los diferentes poderes correctivos de que dispone la autoridad de control.

112. Aunque la elección del medio adecuado y necesario corresponde a la autoridad de control y es esta la que debe proceder a esa elección tomando en consideración todas las circunstancias de la transferencia de datos personales de que se trate, dicha autoridad sigue estando obligada a llevar a cabo con toda la diligencia exigible su misión de velar por el pleno cumplimiento del RGPD.

113. A este respecto, como el Abogado General ha señalado también en el punto 148 de sus conclusiones, la referida autoridad está obligada, en virtud del artículo 58, apartado 2, letras f) y j), del mencionado Reglamento, a suspender o prohibir una transferencia de datos personales a un país tercero si considera, a la luz de todas las circunstancias que rodean a esa transferencia, que las cláusulas tipo de protección de datos no se respetan o no pueden ser respetadas en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no ha suspendido la transferencia o puesto fin a esta por sí mismos.

114. La interpretación realizada en el apartado anterior no se ve desvirtuada por la argumentación del Comisario según la cual el artículo 4 de la Decisión 2010/87, en su versión anterior a la entrada en vigor de la Decisión 2016/2297, entendida a la luz del considerando 11 de dicha Decisión, limitaba a ciertos supuestos excepcionales la facultad de las autoridades de control de suspender o prohibir una transferencia de datos personales a un país tercero. En efecto, en su versión resultante de la Decisión de Ejecución 2016/2297, el artículo 4 de la Decisión CPT hace alusión a la facultad que tienen esas autoridades, en lo sucesivo, en virtud del artículo 58, apartado 2, letras f) y j), del RGPD, de suspender o prohibir esa transferencia, sin limitar en modo alguno el ejercicio de la antedicha facultad a circunstancias excepcionales.

115. En cualquier caso, el poder de ejecución que el artículo 46, apartado 2, letra c), del RGPD reconoce a la Comisión para que adopte cláusulas tipo de protección de datos no le confiere la competencia para restringir las facultades de que disponen las autoridades de control en virtud del artículo 58, apartado 2, del antedicho Reglamento (véase por analogía, por lo que respecta a los artículos 25, apartado 6, y 28 de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartados 102 y 103). Por otra parte, el considerando 5 de la Decisión de Ejecución 2016/2297 confirma que la Decisión CPT «no impide que una [autoridad de control] ejerza sus facultades para supervisar los flujos de datos, incluida la facultad de prohibir o suspender una transferencia de datos personales cuando constate que la transferencia se está realizando en infracción del Derecho de la Unión o de la legislación nacional en materia de protección de datos».

116. Sin embargo, es importante señalar que las facultades de la autoridad de control competente están sujetas al pleno cumplimiento de la Decisión mediante la cual la Comisión constata, en su caso, en aplicación del artículo 45, apartado 1, frase primera, del RGPD, que un tercer país determinado garantiza un nivel de protección adecuado. En efecto, en ese supuesto, del artículo 45, apartado 1, segunda frase, del referido Reglamento, en relación con el considerando 103 del mismo, se desprende que las transferencias de datos personales al tercer país de que se trate pueden realizarse sin que sea necesario obtener una autorización específica.

117. En virtud del artículo 288 TFUE, párrafo cuarto, una decisión de adecuación de la Comisión tiene, en todos sus elementos, carácter obligatorio para todos los Estados miembros destinatarios y vincula, por tanto, a todos su órganos, en la medida en que constate que el país tercero de que se trate garantiza un nivel de protección adecuado y tenga el efecto de autorizar las antedichas transferencias de datos (véase por analogía, por 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 51 y jurisprudencia citada).

118. Así pues, mientras la decisión de adecuación no haya sido declarada inválida por el Tribunal de Justicia, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden ciertamente 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 (sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 52 y jurisprudencia citada) ni, por consiguiente, suspender o prohibir transferencias de datos personales a ese tercer país.

119. No obstante, una decisión de adecuación de la Comisión adoptada en virtud del artículo 45, apartado 3, del RGPD no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten, en aplicación del artículo 77, apartado 1, del RGPD, a la autoridad nacional de control competente una reclamación para la protección de sus derechos y libertades frente al tratamiento de esos datos. De igual forma, una decisión de esa naturaleza no puede dejar sin efecto ni limitar las facultades expresamente reconocidas a las autoridades nacionales de control por el artículo 8, apartado 3, de la Carta y por los artículos 51, apartado 1, y 57, apartado 1, letra a), del antedicho Reglamento (véase por analogía, por lo que respecta a los artículos 25, apartado 6, y 28 de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 53).

120. Por tanto, 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 Tribunal de Justicia una cuestión prejudicial sobre esta validez (véase por analogía, por lo que respecta al artículo 25, apartado 6, y al artículo 28 de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 57 y 65).

121. Habida cuenta de las consideraciones anteriores, procede responder a la octava cuestión prejudicial que el artículo 58, apartado 2, letras f) y j), del RGPD debe interpretarse en el sentido de que, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión, 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, 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, en particular, por los artículos 45 y 46 del RGPD y por la Carta, no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismos.

Sobre las cuestiones prejudiciales séptima y undécima

122. Mediante sus cuestiones prejudiciales séptima y undécima, que es preciso examinar conjuntamente, el órgano jurisdiccional remitente pregunta, en esencia, al Tribunal de Justicia acerca de la validez de la Decisión CPT a la luz de los artículos 7, 8 y 47 de la Carta.

123. En particular, tal como se desprende del propio tenor de la séptima cuestión prejudicial y de las explicaciones referentes a dicha cuestión contenidas en la petición de decisión prejudicial, el órgano jurisdiccional remitente se pregunta si la Decisión CPT puede garantizar un nivel de protección adecuado de los datos personales transferidos a países terceros, en la medida en que las cláusulas tipo de protección de datos que prevé no son vinculantes para las autoridades de esos países terceros.

124. El artículo 1 de la Decisión CPT dispone que se considera que las cláusulas tipo de protección de datos incluidas en el anexo de esta ofrecen garantías suficientes con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, de conformidad con las exigencias del artículo 26, apartado 2, de la Directiva 95/46. Esta última disposición ha sido recogida, en esencia, en el artículo 46, apartados 1 y 2, letra c), del RGPD.

125. Sin embargo, aunque esas cláusulas son obligatorias para el responsable del tratamiento establecido en la Unión y el destinatario de la transferencia de datos personales establecido en un país tercero, en el supuesto de que hayan celebrado un contrato que haga referencia a esas cláusulas, ha quedado acreditado que dichas cláusulas no vinculan a las autoridades de ese país tercero, dado que estas últimas no son partes del contrato.

126. Si bien existen, por tanto, situaciones en las que, en función del estado del Derecho y de las prácticas en vigor en el país de que se trate, el destinatario de una transferencia de esas características puede garantizar la protección de datos necesaria basándose únicamente en las cláusulas tipo de protección de datos, existen otras situaciones en las que las estipulaciones contenidas en esas cláusulas podrían no constituir un medio suficiente para garantizar en la práctica la protección efectiva de los datos personales transferidos al país tercero de que se trate. Eso es lo que sucede, en particular, cuando el Derecho de ese país tercero permite a sus autoridades públicas llevar a cabo injerencias en los derechos de los interesados relativos a esos datos.

127. Por tanto, es preciso dilucidar si una decisión de la Comisión relativa a cláusulas tipo de protección de datos, adoptada sobre la base del artículo 46, apartado 2, letra c), del RGPD, es inválida si la referida decisión no contiene garantías exigibles a las autoridades públicas de los países terceros a los que se transfieran o puedan transferirse datos personales sobre la base de las antedichas cláusulas.

128. El artículo 46, apartado 1, del RGPD establece que, a falta de una decisión de adecuación, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Según el artículo 46, apartado 2, letra c), del antedicho Reglamento, esas garantías podrán ser aportadas mediante cláusulas tipo de protección de datos adoptadas por la Comisión. Pues bien, las anteriores disposiciones no establecen que la totalidad de las referidas garantías deban estar necesariamente previstas en una decisión de la Comisión como la Decisión CPT.

129. A este respecto, es preciso señalar que una decisión de esas características es distinta de una decisión de adecuación adoptada en virtud del artículo 45, apartado 3, del RGPD, la cual tiene por objeto declarar con efecto vinculante, tras un examen de la normativa del tercer país de que se trate que tenga en cuenta, en particular, la legislación pertinente en materia de seguridad nacional y de acceso de las autoridades públicas a los datos personales, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país garantizan un nivel de protección adecuados y que, por tanto, el acceso de las autoridades públicas de ese tercer país a esos datos no impide su transferencia a ese mismo tercer país. Por consiguiente, tal decisión de adecuación solo puede ser adoptada por la Comisión si ha constatado que la legislación pertinente del país tercero en la materia recoge efectivamente todas las garantías exigibles para poder considerar que asegura un nivel de protección adecuado.

130. En cambio, cuando se trata de una decisión de la Comisión que adopta cláusulas tipo de protección de datos, como la Decisión CPT, en la medida en que tal decisión no tiene por objeto un tercer país, un territorio o uno o varios sectores específicos de un tercer país, no puede inferirse del artículo 46, apartados 1 y 2, letra c), del RGPD que la Comisión esté obligada a llevar a cabo, antes de la adopción de dicha decisión, una evaluación de la adecuación del nivel de protección garantizado por los países terceros a los que podrían transferirse datos personales sobre la base de las referidas cláusulas.

131. A este respecto, debe recordarse que, a tenor del artículo 46, apartado 1, del mencionado Reglamento, a falta de decisión de adecuación de la Comisión, incumbe al responsable o al encargado del tratamiento establecidos en la Unión ofrecer, en particular, garantías adecuadas. Los considerandos 108 y 114 del antedicho Reglamento confirman que, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o, en su caso, el encargado del tratamiento «deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado» y que «esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas […] en la Unión o en un tercer país».

132. Dado que, como se desprende del apartado 125 de la presente sentencia, es inherente al carácter contractual de las cláusulas tipo de protección de datos que estas no pueden vincular a las autoridades públicas de

países terceros, pero que los artículos 44 y 46, apartados 1 y 2, letra c), del RGPD, interpretados a la luz de los artículos 7, 8 y 47 de la Carta, exigen que el nivel de protección de las personas físicas garantizado por dicho Reglamento no se vea comprometido, puede resultar necesario completar las garantías recogidas en esas cláusulas tipo de protección datos. A ese respecto, el considerando 109 del referido Reglamento dispone que «la posibilidad de que [los] responsable[s] […] del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión […] no debe obstar a que los responsables […] añadan otras cláusulas o garantías adicionales» y precisa, en particular, que «se debe alentar a los responsables […] a ofrecer garantías adicionales […] que complementen las cláusulas tipo de protección de datos».

133. Resulta, por tanto, evidente que las cláusulas tipo de protección de datos adoptadas por la Comisión en virtud del artículo 46, apartado 2, letra c), del mismo Reglamento tienen únicamente como finalidad proporcionar a los responsables o encargados del tratamiento establecidos en la Unión garantías contractuales que se apliquen de manera uniforme en todos los países terceros y, por tanto, independientemente del nivel de protección garantizado en cada uno de ellos. En la medida en que esas cláusulas tipo de protección de datos no pueden proporcionar, debido a su naturaleza, garantías que vayan más allá de una obligación contractual de velar por que se respete el nivel de protección exigido por el Derecho de la Unión, tales cláusulas pueden necesitar, en función de cuál sea la situación de un país tercero determinado, la adopción de medidas adicionales por parte del responsable del tratamiento con el fin de garantizar el respeto de ese nivel de protección.

134. A este respecto, tal como ha señalado el Abogado General en el punto 126 de sus conclusiones, el mecanismo contractual previsto en el artículo 46, apartado 2, letra c), del RGPD se basa en la responsabilización del responsable o del encargado del tratamiento establecidos en la Unión, así como, con carácter subsidiario, de la autoridad de control competente. Corresponde, por tanto, ante todo, a ese responsable o encargado del tratamiento comprobar, caso por caso y, si es preciso, en colaboración con el destinatario de la transferencia, si el Derecho del tercer país de destino garantiza una protección adecuada, a la luz del Derecho de la Unión, de los datos personales transferidos sobre la base de cláusulas tipo de protección de datos, proporcionado, cuando sea necesario, garantías adicionales a las ofrecidas por dichas cláusulas.

135. Si el responsable o el encargado del tratamiento establecidos en la Unión no pueden adoptar medidas adicionales suficientes para garantizar esa protección, estos o, con carácter subsidiario, la autoridad de control competente están obligados a suspender o poner fin a la transferencia de datos personales al país tercero de que se trate. En particular, eso es lo que ocurre cuando el Derecho de ese país tercero impone al destinatario de una transferencia de datos personales procedentes de la Unión obligaciones que son contrarias a las referidas cláusulas y que, por tanto, pueden poner en entredicho la garantía contractual de un nivel de protección adecuado contra el acceso de las autoridades públicas del mencionado país tercero a esos datos.

136. Por consiguiente, el mero hecho de que las cláusulas tipo de protección de datos recogidas en una decisión de la Comisión adoptada en aplicación del artículo 46, apartado 2, letra c), del RGPD, como las recogidas en el anexo de la Decisión CPT, no vinculen a las autoridades del país tercero al que pueden transferirse datos personales no afecta a la validez de dicha Decisión.

137. Esa validez depende, en cambio, de 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, tal decisión incluye mecanismos efectivos que permitan en la práctica garantizar que el nivel de protección exigido por el Derecho de la Unión sea respetado y 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.

138. Por lo que atañe a las garantías contenidas en las cláusulas tipo de protección de datos que se recogen en el anexo de la Decisión CPT, 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 Unión, 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», es decir, según la definición recogida en el artículo 3, letra f) de la antedicha Decisión, «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». Pues bien, las disposiciones del RGPD, interpretadas a la luz de la Carta, forman parte de esa legislación.

139. Asimismo, el destinatario de la transferencia de datos personales establecido en un país tercero se compromete, en virtud de la referida cláusula 5, letra a), a informar sin demora al responsable del tratamiento establecido en la Unión de su eventual incapacidad para cumplir con las obligaciones que le incumben con arreglo al contrato celebrado. En particular, según la mencionada cláusula 5, letra b), el antedicho destinatario certificará que no tiene motivos para creer que la legislación que le es de aplicación le impida cumplir las obligaciones que le incumben con arreglo al contrato celebrado y se comprometerá a notificar al responsable del tratamiento, en cuanto tenga conocimiento de ello, cualquier modificación de la legislación nacional que le ataña que pueda tener un importante efecto negativo sobre las garantías y obligaciones estipuladas en las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT. Por otra parte, si bien la misma cláusula 5, letra d), inciso i), permite al destinatario de la transferencia de datos personales, en caso de que exista una legislación que se lo impida, como una prohibición de carácter penal para preservar la confidencialidad de una investigación llevada a cabo por la policía, no notificar al responsable del tratamiento establecido en la Unión una solicitud jurídicamente vinculante de divulgar los datos personales presentada por una autoridad encargada de la aplicación de la ley, el referido destinatario sigue estando obligado, de conformidad con la cláusula 5, letra a), del anexo de la Decisión CPT, a informar al responsable del tratamiento de que no puede cumplir las cláusulas tipo de protección de datos.

140. En los dos supuestos que contempla, la antedicha cláusula 5, letras a) y b), confiere al responsable del tratamiento establecido en la Unión la facultad de suspender la transferencia de los datos o rescindir el contrato. Habida cuenta de las exigencias resultantes del artículo 46, apartados 1 y 2, letra c), del RGPD, interpretado a la luz de los artículos 7 y 8 de la Carta, la suspensión de la transferencia de los datos o la rescisión del contrato es obligatoria para el responsable del tratamiento cuando el destinatario de la transferencia no cumple, o ya no puede cumplir, las cláusulas tipo de protección de datos. Si no actuase así, el responsable del tratamiento incumpliría las exigencias que le incumben en virtud de la cláusula 4, letra a), del anexo de la Decisión CPT interpretada a la luz de las disposiciones del RGPD y de la Carta.

141. Por tanto, es evidente que las cláusulas 4, letra a), y 5, letras a) y b), del referido anexo obligan al responsable del tratamiento establecido en la Unión 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 el anexo de la Decisión CPT, antes de llevar a cabo una transferencia de datos personales a ese país tercero. Por lo que atañe a esta comprobación, la nota a pie de página relativa a la mencionada cláusula 5 precisa 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 el contrario, tal como ha subrayado el Abogado General en el punto 131 de sus conclusiones, 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. La apreciación, por parte de esos operadores, del carácter necesario de esa obligación deberá, en su caso, tener en cuenta la constatación de la adecuación del nivel de protección garantizado por el país tercero de que se trate que se recoja en una decisión de adecuación de la Comisión, adoptada en virtud del artículo 45, apartado 3, del RGPD.

142. De lo anterior se desprende que el responsable del tratamiento establecido en la Unión y el destinatario de la transferencia de datos personales están obligados a comprobar, previamente, el respeto, en el país tercero de que se trate, del nivel de protección exigido por el Derecho de la Unión. El destinatario de esa transferencia tiene, en su caso, la obligación, en virtud de la misma cláusula 5, letra b), de informar al responsable del tratamiento de su eventual incapacidad para cumplir con esas cláusulas, incumbiendo entonces a este último suspender la transferencia de datos o rescindir el contrato.

143. Si el destinatario de la transferencia de datos personales a un país tercero pone en conocimiento del responsable del tratamiento, en virtud de la cláusula 5, letra b), del anexo de la Decisión CPT, que la legislación del país tercero de que se trate no le permite cumplir con las cláusulas tipo de protección de datos recogidas en dicho anexo, de la cláusula 12 del antedicho anexo se deriva que los datos que ya hayan sido transferidos a ese país tercero y sus copias deben ser devueltos o destruidos en su totalidad. En cualquier caso, la cláusula 6 del mismo

anexo castiga el incumplimiento de esas cláusulas tipo confiriendo al interesado el derecho a percibir una indemnización por el daño sufrido.

144. Debe añadirse que, conforme a la cláusula 4, letra f), del anexo de la Decisión CPT, el responsable del tratamiento establecido en la Unión se compromete, en el caso de que categorías especiales de datos pudieran ser transferidas a un tercer país que no proporcione un nivel de protección adecuado, a informar de ello al interesado antes de que se efectúe la transferencia o en cuanto sea posible. Esa información puede permitir a esa persona ejercer el derecho de recurso contra el responsable del tratamiento que le reconoce la cláusula 3, apartado 1, del antedicho anexo con el fin de que ese responsable suspenda la transferencia prevista, rescinda el contrato celebrado con el destinatario de la transferencia de datos personales o, en su caso, solicite a este último la devolución o la destrucción de los datos transferidos.

145. Finalmente, en virtud de la cláusula 4, letra g), del referido anexo, el responsable del tratamiento establecido en la Unión está obligado, cuando el destinatario de la transferencia de datos personales le notifica, con arreglo a la cláusula 5, letra b), del anexo, 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, decida proseguir la transferencia o levantar la suspensión. El envío de la referida notificación a esa autoridad de control y la facultad de esta de auditar al destinatario de la transferencia de datos personales en aplicación de la cláusula 8, apartado 2, del mismo anexo 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.

146. En este contexto, el artículo 4 de la Decisión CPT, interpretado a la luz del considerando 5 de la Decisión de Ejecución 2016/2297, confirma que en modo alguno la Decisión CPT impide a la autoridad de control competente 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. A este respecto, tal como se desprende de la respuesta a la octava cuestión prejudicial, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión, la autoridad de control competente está obligada, en virtud del artículo 58, apartado 2, letras f) y j), del RGPD, a suspender o prohibir esa transferencia cuando considere, a la luz de 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 no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismos.

147. Por lo que atañe a la circunstancia, puesta de relieve por el Comisario, de que las transferencias de datos personales a tal país tercero podría ser eventualmente objeto de decisiones divergentes de las autoridades de control en diferentes Estados miembros, debe añadirse que, como se desprende de los artículos 55, apartado 1, y 57, apartado 1, letra a), del RGPD, la función de velar por el cumplimiento de dicho Reglamento se confía, en principio, a cada autoridad de control en el territorio del Estado miembro al que pertenece. Asimismo, para evitar decisiones divergentes, el artículo 64, apartado 2, del referido Reglamento prevé la posibilidad de que una autoridad de control que considere que las transferencias de datos a un país tercero deben, de manera general, prohibirse solicite el dictamen del Comité Europeo de Protección de Datos (EDPB), el cual, en aplicación del artículo 65, apartado 1, letra c), del mismo Reglamento, podrá adoptar una decisión vinculante, en particular, cuando una autoridad de control competente no siga el dictamen emitido por el Comité.

148. De lo anterior se desprende que la Decisión CPT 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.

149. Habida cuenta de todas las consideraciones anteriores, procede responder a las cuestiones prejudiciales séptima y undécima que el examen de la Decisión CPT a la luz de los artículos 7, 8 y 47 de la Carta no ha puesto de manifiesto la existencia de ningún elemento que pueda afectar a la validez de dicha Decisión.

Sobre las cuestiones prejudiciales, cuarta, quinta, novena y décima

150. Mediante la novena cuestión prejudicial, el órgano jurisdiccional remitente solicita, en esencia, que se dilucide si una autoridad de control de un Estado miembro está vinculada por las constataciones contenidas en la Decisión EP según las cuales los Estados Unidos garantizan un nivel de protección adecuado y en qué medida queda vinculada por ellas. En las cuestiones prejudiciales cuarta, quinta y décima, dicho órgano jurisdiccional pregunta, en esencia, si, habida cuenta de sus propias constataciones relativas a la normativa de los Estados Unidos, la transferencia a ese país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT vulnera los derechos garantizados en los artículos 7, 8 y 47 de la Carta y pide, en particular, al Tribunal de Justicia que determine si la creación del Defensor del Pueblo mencionado en el anexo III de la Decisión EP es compatible con el antedicho artículo 47.

151. Con carácter preliminar, debe señalarse que, si bien el recurso en el litigio principal interpuesto por el Comisario pone en entredicho únicamente la validez de la Decisión CPT, dicho recurso fue presentado ante el órgano jurisdiccional remitente con anterioridad a la adopción de la Decisión EP. En la medida en que, en sus cuestiones prejudiciales cuarta y quinta, ese órgano jurisdiccional pregunta al Tribunal de Justicia, de manera general, acerca de la protección que debe garantizarse, en virtud de los artículos 7, 8 y 47 de la Carta, en el contexto de la referida transferencia, el examen del Tribunal de Justicia debe tomar en consideración las consecuencias resultantes de la adopción de la Decisión EP, que tuvo lugar entretanto. Esto es tanto más cierto cuanto que el antedicho órgano jurisdiccional pregunta explícitamente, en su décima cuestión prejudicial, si la protección exigida por el artículo 47 de la Carta queda garantizada por medio del Defensor del Pueblo mencionado en esa última Decisión.

152. Asimismo, de las indicaciones contenidas en la petición de decisión prejudicial se desprende que, en el marco del procedimiento principal, Facebook Ireland ha alegado que la Decisión EP producía, en opinión del Comisario, efectos vinculantes por lo que atañe a la constatación de la adecuación del nivel de protección garantizado por los Estados Unidos y, por consiguiente, en lo que respecta a la legalidad de una transferencia a este país tercero de datos personales basada en las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT.

153. Pues bien, tal como se desprende del apartado 59 de la presente sentencia, en su sentencia de 3 de octubre de 2017, que se adjunta a la petición de decisión prejudicial, el órgano jurisdiccional remitente subrayó que estaba obligado a tener en cuenta las modificaciones del Derecho que tuviesen lugar entre la interposición del recurso y la vista que se organizase ante él. Por tanto, dicho órgano jurisdiccional parece estar obligado a tomar en consideración, a la hora de resolver el litigio principal, el cambio de circunstancias resultante de la adopción de la Decisión EP, así como los posibles efectos vinculantes de esta.

154. En particular, la existencia de efectos vinculantes ligados a la constatación por la Decisión EP de un nivel de protección adecuado en los Estados Unidos es pertinente a la hora de apreciar tanto las obligaciones, recordadas en los apartados 141 y 142 de la presente sentencia, que incumben al responsable del tratamiento y al destinatario de una transferencia de datos personales a un país tercero realizada sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT como las obligaciones que, en su caso, recaigan en la autoridad de control de suspender o prohibir tal transferencia.

155. Efectivamente, por lo que atañe a los efectos vinculantes de la Decisión EP, el artículo 1, apartado 1, de dicha Decisión dispone que, a los efectos del artículo 45, apartado 1, del RGPD, «los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en los Estados Unidos en el marco del Escudo de la privacidad UE-EE. UU.» Con arreglo al artículo 1, apartado 3, de la referida Decisión, se considerarán datos personales transferidos en el marco de ese Escudo aquellos que hayan sido transferidos desde la Unión a entidades establecidas en los Estados Unidos que figuren en la denominada «lista del Escudo de la privacidad», mantenida y puesta a disposición del público por el Departamento de Comercio de los Estados Unidos, de conformidad con las secciones I y III de los principios expuestos en el anexo II de la misma Decisión.

156. Tal como se desprende de la jurisprudencia recordada en los apartados 117 y 118 de la presente sentencia, la Decisión EP tiene carácter obligatorio para las autoridades de control en la medida en que constate que los Estados Unidos garantizan un nivel de protección adecuado y, por tanto, tenga el efecto de autorizar las transferencias de datos personales realizadas en el marco del Escudo de la Privacidad UE-EE. UU. Así pues, mientras la referida Decisión no haya sido declarada inválida por el Tribunal de Justicia, la autoridad de control competente no puede suspender o prohibir una transferencia de datos personales a una entidad que se haya adherido a ese Escudo basándose en que considera, contrariamente a la apreciación efectuada por la Comisión en la mencionada Decisión, que la legislación de los Estados Unidos que regula el acceso a los datos personales transferidos en el marco del antedicho Escudo y el uso de esos datos por las autoridades públicas de ese país tercero a efectos de seguridad nacional, aplicación de la ley o de interés público no garantiza un nivel de protección adecuado.

157. No es menos cierto que, con arreglo a la jurisprudencia recordada en los apartados 119 y 120 de la presente sentencia, cuando una persona le presenta una reclamación, la autoridad de control competente debe apreciar con toda independencia si la transferencia de datos personales de que se trata cumple las exigencias establecidas por el RGPD y, en caso de que considere fundadas las alegaciones formuladas por esa persona para poner en entredicho la validez de una decisión de adecuación, interponer un recurso ante los tribunales nacionales para que estos planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de esa decisión.

158. En efecto, una reclamación presentada con arreglo al artículo 77, apartado 1, del RGPD, mediante la que una persona cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país alegue que el Derecho y las prácticas de ese país no garantizan un nivel de protección adecuado, no obstante lo constatado por la Comisión en una decisión adoptada en virtud del artículo 45, apartado 3, de ese Reglamento, debe entenderse como concerniente en sustancia a la compatibilidad de esa decisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas (véase por analogía, por lo que respecta a los artículos 25, apartado 6, y 28, apartado 4, de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 59).

159. En el caso de autos, el Sr. Schrems solicitó, en esencia, al Comisario que prohibiese o suspendiese la transferencia de sus datos personales por Facebook Ireland a Facebook Inc., establecida en los Estados Unidos, aduciendo que ese país tercero no garantizaba un nivel de protección adecuado. Habida cuenta de que, a raíz de una investigación sobre las alegaciones del Sr. Schrems, el Comisario interpuso recurso ante el órgano jurisdiccional remitente, a este último, a la luz de las pruebas presentadas y del debate contradictorio desarrollado ante él, parecen haberle surgido preguntas acerca del fundamento de las dudas del Sr. Schrems por lo que respecta a la adecuación del nivel de protección garantizado por el mencionado país tercero, a pesar de las constataciones efectuadas entretanto por la Comisión en la Decisión EP, lo que ha llevado al referido órgano jurisdiccional a plantear al Tribunal de Justicia las cuestiones prejudiciales cuarta, quinta y décima.

160. Tal como ha señalado el Abogado General en el punto 175 de sus conclusiones, debe entenderse que esas cuestiones prejudiciales ponen, en esencia, en entredicho la constatación de la Comisión contenida en la Decisión EP de que los Estados Unidos garantizan un nivel de protección adecuado de los datos personales transferidos desde la Unión a ese tercer país y, por consiguiente, la validez de la antedicha Decisión.

161. Habida cuenta de las circunstancias señaladas en los apartados 121 y 157 a 160 de la presente sentencia y para dar una respuesta completa al órgano jurisdiccional remitente, es preciso apreciar si la Decisión EP se ajusta a las exigencias derivadas del RGPD entendido a la luz de la Carta (véase, por analogía, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 67).

162. La adopción por la Comisión de una decisión de adecuación en virtud del artículo 45, apartado 3, del RGPD requiere la constatación debidamente motivada por esa institución de que el tercer país considerado garantiza efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión (véase por analogía, por 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 96).

Sobre el contenido de la Decisión EP

163. La Comisión constató, en el artículo 1, apartado 1, de la Decisión EP, que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en los Estados Unidos en el marco del Escudo de la Privacidad UE-EE. UU., el cual se compone, en particular, en virtud del artículo 1, apartado 2, de dicha Decisión, de los principios establecidos por el Departamento de Comercio de los Estados Unidos el 7 de julio de 2016, tal como se exponen en el anexo II de la referida Decisión, y de los compromisos y declaraciones oficiales recogidos en los documentos enumerados en los anexos I y III a VII de la misma Decisión.

164. No obstante, la Decisión EP precisa también, en el punto I.5 de su anexo II, titulado «Principios del marco del Escudo de la privacidad UE-EE. UU.», que la adhesión a estos principios puede verse limitada, en particular, por «exigencias de seguridad nacional, interés público y cumplimiento de la Ley». Así pues, dicha Decisión reconoce, al igual que sucede con la Decisión 2000/520, la primacía de las referidas exigencias sobre los antedichos principios, primacía en virtud de la cual las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando estos entren en conflicto con esas exigencias y se manifiesten por tanto incompatibles con ellas (véase por analogía, por lo que respecta a la Decisión 2000/520, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 86).

165. Dado su carácter general, la excepción prevista en el punto I.5 del anexo II de la Decisión EP hace posibles así injerencias, fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos, en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la Unión a Estados Unidos (véase por analogía, por lo que respecta a la Decisión 2000/520, la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 87). Más concretamente, y tal como se ha constatado en la Decisión EP, las referidas injerencias pueden producirse como consecuencia del acceso a los datos personales transferidos desde la Unión a los Estados Unidos y de la utilización de esos datos por las autoridades públicas estadounidenses, en el marco de los programas de vigilancia PRISM y Upstream basados en el artículo 702 de la FISA y en la E.O. 12333.

166. En este contexto, en los considerandos 67 a 135 de la Decisión EP, la Comisión evaluó las limitaciones y las garantías previstas en la normativa de los Estados Unidos y, en particular, en el artículo 702 de la FISA, en la E.O. 12333 y en la PPD-28, por lo que atañe al acceso a los datos personales transferidos en el marco del Escudo de la Privacidad UE-EE. UU. y a la utilización de esos datos por las autoridades públicas estadounidenses a efectos de seguridad nacional, aplicación de la ley y otros fines de interés general.

167. Al término de esa evaluación, la Comisión constató, en el considerando 136 de la referida Decisión, que «los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades autocertificadas [en los Estados Unidos]» y estimó, en el considerando 140 de la antedicha Decisión, que «sobre la base de la información disponible acerca del ordenamiento jurídico de los Estados Unidos, […] las injerencias de los poderes públicos de los Estados Unidos en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a dicho país en el marco del Escudo de la privacidad a efectos de seguridad nacional, aplicación de la ley u otros fines de interés público, y las consiguientes restricciones impuestas a las entidades autocertificadas con respecto a su adhesión a los principios de privacidad, se limitarán a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que existe una tutela judicial efectiva frente a tales injerencias».

Sobre la constatación relativa al nivel de protección adecuado

168. Habida cuenta de los elementos mencionados por la Comisión en la Decisión EP y de los acreditados por el órgano jurisdiccional remitente en el marco del procedimiento principal, dicho órgano jurisdiccional alberga dudas acerca de 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. En particular, el referido órgano jurisdiccional considera que el Derecho de ese país tercero no prevé las limitaciones y las garantías necesarias con respecto a las injerencias autorizadas por su normativa nacional y tampoco garantiza una tutela judicial efectiva contra tales injerencias. En relación con este último aspecto, añade

que la creación del Defensor del Pueblo en el ámbito del Escudo de la Privacidad no puede, a su entender, subsanar esas lagunas, ya que ese Defensor del Pueblo no puede asimilarse a un tribunal, en el sentido del artículo 47 de la Carta.

169. Por lo que atañe, en primer lugar, a los artículos 7 y 8 de la Carta, que forman parte del nivel de protección exigido dentro de la Unión y cuyo respeto debe ser constatado por la Comisión antes de que esta adopte una decisión de adecuación en virtud del artículo 45, apartado 1, del RGPD, debe recordarse que el artículo 7 de la Carta garantiza a toda persona el derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones Por su parte, el artículo 8, apartado 1, de la Carta reconoce expresamente a toda persona el derecho a la protección de los datos de carácter personal que le conciernan.

170. Así pues, el acceso a los datos personales de una persona física para su conservación o su utilización afecta al derecho fundamental de dicha persona al respeto de la vida privada, garantizado en el artículo 7 de la Carta, derecho que atañe a toda información relativa a una persona física identificada o identificable. Además, los antedichos tratamientos de datos también están comprendidos dentro del ámbito del artículo 8 de la Carta porque constituyen tratamientos de datos de carácter personal en el sentido del referido artículo y, en consecuencia, deben cumplir necesariamente los requisitos de protección de los datos previstos en él [véanse, en este sentido, las sentencias de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartados 49 y 52; de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 29, y el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 122 y 123].

171. El Tribunal de Justicia ya ha declarado 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, cualquiera que sea la utilización posterior de la información comunicada. Lo mismo puede decirse de 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 [véanse, en este sentido, 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].

172. No obstante, los derechos consagrados en los artículos 7 y 8 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse según su función en la sociedad [véanse, en este sentido, las sentencias de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 48 y jurisprudencia citada; de 17 de octubre de 2013, Schwarz, C-291/12, EU:C:2013:670, apartado 33 y jurisprudencia citada, y el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 136].

173. A este respecto, debe asimismo ponerse de relieve que, a tenor del artículo 8, apartado 2, de la Carta, los datos de carácter personal deben tratarse, en particular, «para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley».

174. Asimismo, conforme al artículo 52, apartado 1, primera frase, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por esta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Según el artículo 52, apartado 1, segunda frase, de la Carta, dentro del respeto del principio de proporcionalidad, solo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

175. Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

176. Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida 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. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada).

177. A tal efecto, el artículo 45, apartado 2, letra a), del RGPD precisa que, en el marco de su evaluación de la adecuación del nivel de protección garantizado por un país tercero, la Comisión tendrá en cuenta, en particular, «el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles».

178. En el caso de autos, la constatación llevada a cabo por la Comisión en la Decisión EP según la cual los Estados Unidos garantizan un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión por el RGPD, interpretado a la luz de los artículos 7 y 8 de la Carta, ha sido puesta en entredicho fundándose, en particular, en que las injerencias resultantes de los programas de vigilancia basados en los artículos 702 de la FISA y en la E.O. 12333 no están supuestamente sujetas a exigencias que garanticen, dentro del respeto del principio de proporcionalidad, un nivel de protección sustancial equivalente al garantizado por el artículo 52, apartado 1, segunda frase, de la Carta. Por tanto, es preciso examinar si esos programas de vigilancia se aplican respetando tales exigencias, sin que sea necesario comprobar previamente el respeto por ese país tercero de requisitos sustancialmente equivalentes a los previstos en el artículo 52, apartado 1, primera frase, de la Carta.

179. A este respecto, por lo que atañe a los programas de vigilancia basados en el artículo 702 de la FISA, la Comisión constató, en el considerando 109 de la Decisión EP, que, con arreglo al antedicho artículo, «el FISC no autoriza medidas de vigilancia individuales, sino programas de vigilancia (como PRISM o Upstream) sobre la base de certificaciones anuales elaboradas por el fiscal general y el director de Inteligencia Nacional». Tal como se desprende de este considerando, el control ejercido por el FISC tiene por objeto comprobar si esos programas de vigilancia se atienen a la finalidad de obtener información en materia de inteligencia exterior, pero no tiene por objeto determinar «si [las personas objetivo seleccionadas son adecuadas] para recabar información de inteligencia exterior».

180. Por tanto, resulta evidente que del artículo 702 de la FISA en modo alguno se desprende la existencia de limitaciones a la habilitación que dicho artículo otorga para la ejecución de programas de vigilancia con fines de inteligencia exterior ni tampoco la existencia de garantías para las personas no nacionales de los Estados Unidos que sean potencialmente objeto de esos programas. En estas circunstancias, tal como el Abogado General señaló, en esencia, en los puntos 291, 292 y 297 de sus conclusiones, el referido artículo no puede garantizar un nivel de protección sustancialmente equivalente al garantizado por la Carta, tal y como esta ha sido interpretada por la jurisprudencia recordada en los apartados 175 y 176 de la presente sentencia, conforme a la cual una base legal que permita injerencias en los derechos fundamentales, para cumplir el principio de proporcionalidad, debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate y establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas.

181. Según las constataciones contenidas en la Decisión EP, es cierto que los programas de vigilancia basados en el artículo 702 de la FISA deben aplicarse respetando las exigencias resultantes de la PPD-28. Sin embargo, aunque la Comisión subrayó, en los considerandos 69 y 77 de la Decisión EP, que esas exigencias son vinculantes para los servicios de inteligencia estadounidenses, el Gobierno estadounidense ha admitido, en respuesta a una pregunta del Tribunal de Justicia, que la PPD-28 no confiere a los interesados derechos exigibles a las autoridades estadounidenses ante los tribunales. Por tanto, esta no puede garantizar un nivel de protección sustancialmente equivalente al resultante de la Carta, contrariamente a lo que exige el artículo 45, apartado 2, letra a), del RGPD, según el cual la constatación de dicho nivel de protección depende, en particular, de la existencia de

derechos efectivos y exigibles que sean reconocidos a los interesados cuyos datos personales hayan sido transferidos al país tercero de que se trate.

182. Por lo que respecta a los programas de vigilancia basados en la E.O. 12333, de los autos en poder del Tribunal de Justicia se deprende que este decreto tampoco confiere derechos exigibles a las autoridades estadounidenses ante los tribunales.

183. Es preciso añadir que la PPD-28, que debe respetarse en el marco de la aplicación de los programas a los que se hace referencia en los dos apartados anteriores, permite proceder a una «recopilación "en bloque" […] de una cantidad relativamente grande de información o datos de inteligencia de señales en circunstancias en las que los servicios de inteligencia no puedan utilizar un identificador asociado a un criterio de selección específico […] para orientar la recopilación», tal como se precisa en la carta de 21 de junio de 2016 de la Oficina del Director de Inteligencia Nacional (Office of the Director of National Intelligence) al Departamento de Comercio de los Estados Unidos y a la Administración del Comercio Internacional, recogida en el anexo VI de la Decisión EP. Pues bien, esta posibilidad, que permite, en el marco de los programas de vigilancia basados en la E.O. 12333, acceder a datos en tránsito hacia los Estados Unidos sin que dicho acceso sea objeto de ningún control judicial, no regula, en cualquier caso, de manera suficientemente clara y precisa el alcance de la antedicha recopilación en bloque de datos personales.

184. Por tanto, resulta evidente que ni el artículo 702 de la FISA ni la E.O. 12333, interpretados en relación con la PPD-28, satisfacen las exigencias mínimas establecidas por el Derecho de la Unión con respecto al principio de proporcionalidad, de modo que no puede considerarse que los programas de vigilancia basados en esas disposiciones se limiten a lo estrictamente necesario.

185. En estas circunstancias, las limitaciones de la protección de datos personales que se derivan de la normativa interna de los Estados Unidos relativa al acceso y la utilización, por las autoridades estadounidenses, de los datos transferidos desde la Unión a los Estados Unidos, que la Comisión evaluó en la Decisión EP, no están reguladas conforme a exigencias sustancialmente equivalentes a las requeridas, en el Derecho de la Unión, en el artículo 52, apartado 1, segunda frase, de la Carta.

186. Por lo que atañe, en segundo lugar, al artículo 47 de la Carta, que forma parte también del nivel de protección exigido dentro de la Unión cuyo respeto debe ser constatado por la Comisión antes de adoptar una decisión de adecuación en virtud del artículo 45, apartado 1, del RGPD, debe recordarse que el primer párrafo del referido artículo 47 requiere que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión 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.

187. Según reiterada jurisprudencia, la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho. Así, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta (sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 95 y jurisprudencia citada).

188. A tal efecto, el artículo 45, apartado 2, letra a), del RGPD exige que, en el marco de su evaluación de la adecuación del nivel de protección garantizado por un país tercero, la Comisión tenga en cuenta, en particular, «el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de […] recursos administrativos y acciones judiciales que sean efectivos». El considerando 104 del RGPD subraya, a este respecto, que el tercer país «debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros» y precisa que se debe «reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas».

189. La existencia de posibilidades efectivas de acciones administrativas y judiciales en el país tercero de que se trate tiene una especial importancia en el contexto de una transferencia de datos personales a ese país tercero, en la medida en que, tal como se desprende del considerando 116 del RGPD, los interesados pueden verse confrontados a la insuficiencia de las facultades y medios de las autoridades administrativas y judiciales de los Estados miembros a la hora de dar curso eficazmente a sus reclamaciones basadas en un tratamiento supuestamente ilegal, en ese país tercero, de los datos de ese modo transferidos, lo que puede obligarles a dirigirse a las autoridades y órganos jurisdiccionales de ese mismo país tercero.

190. En el caso de autos, la constatación realizada por la Comisión en la Decisión EP, según la cual los Estados Unidos garantizan un nivel de protección sustancialmente equivalente al garantizado 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 la Privacidad no puede subsanar las lagunas constatadas por la propia Comisión por lo que respecta a la tutela judicial de las personas cuyos datos personales son transferidos a ese país tercero.

191. A este respecto, la Comisión ha señalado, en el considerando 115 de la Decisión EP, que, si bien «las personas, incluidos los interesados de la [Unión], disponen […] de una serie de vías de recurso cuando han sido objeto de vigilancia (electrónica) no autorizada a efectos de seguridad nacional, también es evidente que no están cubiertas todas las bases jurídicas que pueden invocar los servicios de inteligencia estadounidenses (por ejemplo, [la] EO 12333)». Por tanto, por lo que atañe a la E.O. 12333, la Comisión hizo hincapié, en el referido considerando 115, en la inexistencia de vías de recurso. Pues bien, según la jurisprudencia recordada en el apartado 187 de la presente sentencia, una laguna de ese tipo en la tutela judicial con respecto a las injerencias ligadas a los programas de inteligencia basados en el mencionado decreto presidencial impide que pueda concluirse, como hizo la Comisión en la Decisión EP, que el Derecho de los Estados Unidos garantiza un nivel de protección sustancialmente equivalente al garantizado en el artículo 47 de la Carta.

192. Asimismo, en lo que respecta tanto a los programas de vigilancia basados en el artículo 702 de la FISA como a los basados en la E.O. 12333, se ha señalado en los apartados 181 y 182 de la presente sentencia que ni la PPD-28 ni la E.O. 12333 confieren a los interesados derechos exigibles a las autoridades estadounidenses ante los tribunales, de modo que esas personas no disponen de tutela judicial efectiva.

193. Sin embargo, la Comisión observó, en los considerandos 115 y 116 de la Decisión EP, que, debido a la existencia del mecanismo del Defensor del Pueblo establecido por las autoridades estadounidenses, tal como se describe en la carta del secretario de Estado estadounidense a la comisaria europea de Justicia, Consumidores e Igualdad de Género, de 7 de julio de 2016, contenida en el anexo III de la antedicha Decisión, y a la naturaleza de la misión encomendada al Defensor del Pueblo, en este caso, como «coordinador superior de la diplomacia internacional en materia de tecnología de la información», podía considerarse que los Estados Unidos garantizan un nivel de protección sustancialmente equivalente al garantizado en el artículo 47 de la Carta.

194. El examen de la cuestión de si el mecanismo del Defensor del Pueblo contemplado en la Decisión EP puede efectivamente subsanar las limitaciones del derecho a la tutela judicial constatadas por la Comisión debe, con arreglo a las exigencias que se derivan del artículo 47 de la Carta y de la jurisprudencia recordada en el apartado 187 de la presente sentencia, partir del principio de que los justiciables han de tener la posibilidad de ejercer acciones en Derecho ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión.

195. Pues bien, en la carta mencionada en el apartado 193 de la presente sentencia, aunque se describe al defensor del pueblo en el ámbito del Escudo de la Privacidad como «independiente de los servicios de inteligencia», se dice que «informará directamente al secretario de Estado, que garantizará que aquel desempeñe sus funciones de manera objetiva y sin ninguna influencia indebida que pueda afectar a la respuesta que debe proporcionarse». Asimismo, aparte del hecho de que, como ha observado la Comisión en el considerando 116 de la Decisión EP, el defensor del pueblo es nombrado por el secretario de Estado y forma parte integrante del Departamento de Estado, no existe, en la referida Decisión, como ha señalado el Abogado General en el punto 337 de sus conclusiones, ninguna indicación de que la destitución del defensor del pueblo o la anulación de su nombramiento vengan acompañadas de garantías específicas, lo que pone en entredicho la independencia del Defensor del Pueblo con

respecto al poder ejecutivo (véase, en este sentido, la sentencia de 21 de enero de 2020, Banco de Santander, C-274/14, EU:C:2020:17, apartados 60 y 63 y jurisprudencia citada).

196. Asimismo, tal como ha subrayado el Abogado General en el punto 338 de sus conclusiones, si bien el considerando 120 de la Decisión EP pone de manifiesto un compromiso del Gobierno estadounidense a que el servicio de inteligencia en cuestión esté obligado a corregir cualquier infracción de las normas aplicables detectada por el defensor del pueblo en el ámbito del Escudo de la Privacidad, dicha Decisión no contiene ninguna indicación de que dicho defensor del pueblo esté facultado para adoptar decisiones vinculantes con respecto a esos servicios ni tampoco menciona ninguna garantía legal que acompañe a ese compromiso y pueda ser invocada por los interesados.

197. Por tanto, el mecanismo del Defensor del Pueblo contemplado en la Decisión EP no proporciona ninguna vía de recurso ante un órgano que ofrezca a las personas cuyos datos se transfieren a los Estados Unidos garantías sustancialmente equivalentes a las exigidas en el artículo 47 de la Carta.

198. Por consiguiente, al declarar, en el artículo 1, apartado 1, de la Decisión EP, que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en ese país tercero en el marco del Escudo de la Privacidad UE-EE. UU., la Comisión 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.

199. De lo anterior se desprende que el artículo 1 de la Decisión EP es incompatible con el artículo 45, apartado 1, del RGPD, interpretado a la luz de los artículos 7, 8 y 47 de la Carta, y que es, por ello, inválido.

200. Toda vez que el artículo 1 de la Decisión EP es indisociable de los artículos 2 a 6 y de los anexos de esta, su invalidez tiene el efecto de afectar a la validez de esa Decisión en su conjunto.

201. Habida cuenta de todas las consideraciones anteriores, debe concluirse que la Decisión EP es inválida.

202. Por lo que respecta a si es preciso mantener los efectos de la antedicha Decisión para evitar la creación de un vacío legal (véase, en este sentido, la sentencia de 28 de abril de 2016, Borealis Polyolefine y otros, C-191/14, C-192/14, C-295/14, C-389/14 y C-391/14 a C-393/14, EU:C:2016:311, apartado 106), debe señalarse que, en cualquier caso, habida cuenta del artículo 49 del RGPD, la anulación de una decisión de adecuación como la Decisión EP no crea tal vacío legal. En efecto, el antedicho artículo 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.

Costas

203. Dado que el procedimiento tiene, para las partes del litigio principal, el carácter de un incidente promovido ante el órgano jurisdiccional nacional, corresponde a este resolver sobre las costas. Los gastos efectuados por quienes, no siendo partes del litigio principal, han presentado observaciones ante el Tribunal de Justicia no pueden ser objeto de reembolso.

En virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) declara:

1) El artículo 2, apartados 1 y 2, del 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), debe interpretarse en el sentido de que está comprendida dentro del ámbito de aplicación de ese Reglamento una transferencia de datos personales realizada con fines comerciales por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, a pesar de que, en el transcurso de esa transferencia o tras ella,

esos datos puedan ser tratados por las autoridades del país tercero en cuestión con fines de seguridad nacional, defensa y seguridad del Estado.

2) El artículo 46, apartados 1 y apartado 2, letra c), del Reglamento 2016/679 debe interpretarse 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 de los Derechos Fundamentales de la Unión Europea. 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, apartado 2, del referido Reglamento.

3) El artículo 58, apartado 2, letras f) y j), del Reglamento 2016/679 debe interpretarse en el sentido de que, a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión Europea, 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, 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, en particular, por los artículos 45 y 46 del mencionado Reglamento y por la Carta de los Derechos Fundamentales, no puede garantizarse mediante otros medios, si el responsable o el encargado del tratamiento establecidos en la Unión no han suspendido la transferencia o puesto fin a esta por sí mismos.

4) El examen de la Decisión 2010/87/UE 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, en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016, a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales no ha puesto de manifiesto la existencia de ningún elemento que pueda afectar a la validez de dicha Decisión.

5) La Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU., es inválida.

Firmas

* Lengua de procedimiento: inglés.

Fuente: sitio internet del Tribunal de Justicia.