Recopilación de la Jurisprudencia

EDICIÓN PROVISIONAL 26/11/2019

CONCLUSIONES DEL ABOGADO GENERAL
SR. HENRIK SAUGMANDSGAARD ØE
presentadas el 19 de diciembre de 2019[1]

Asunto C-311/18

Data Protection Commissioner
contra
Facebook Ireland Limited,
Maximillian Schrems,
con intervención de
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

[Petición de decisión prejudicial presentada por la High Court (Tribunal Superior, Irlanda)]

«Procedimiento prejudicial — Protección de las personas físicas en lo que respecta al tratamiento de datos personales — Reglamento (UE) 2016/679 — Artículo 2, apartado 2 — Ámbito de aplicación — Transferencia de datos personales con fines comerciales a los Estados Unidos de América — Tratamiento de los datos transferidos con fines de seguridad nacional por parte de las autoridades públicas de los Estados Unidos de América — Artículo 45 — Apreciación de la adecuación del nivel de protección garantizado en un tercer país — Artículo 46 — Garantías adecuadas ofrecidas por el responsable del tratamiento — Cláusulas tipo de protección — Artículo 58, apartado 2 — Facultades de las autoridades de control — Decisión 2010/87/UE — Validez — Decisión de Ejecución (UE) 2016/1250 — "Escudo de la privacidad UE-EE. UU." — Validez — Artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea»

Índice

1 Lengua original: francés.

I. Introducción

1. Al no existir garantías comunes en materia de protección de datos personales a nivel mundial, los flujos transfronterizos de dichos datos presentan un riesgo de ruptura en la continuidad del nivel de protección garantizado dentro de la Unión Europea. Con el fin de facilitar dichos flujos, a la vez que se limita el mencionado riesgo, el legislador de la Unión ha establecido tres mecanismos en virtud de los cuales pueden transferirse datos personales desde la Unión a un tercer Estado.

2. En primer lugar, tal transferencia puede efectuarse sobre la base de una decisión mediante la cual la Comisión Europea declare que el tercer Estado en cuestión garantiza un «nivel de protección adecuado» de los datos que se transfieren a este.[2] En segundo lugar, en defecto de tal decisión, se puede autorizar la transferencia si se acompaña de «garantías adecuadas».[3] Dichas garantías pueden presentar la forma de un contrato entre el exportador y el importador de los datos que incluya cláusulas tipo de protección adoptadas por la Comisión. En tercer lugar, el RGPD prevé determinadas excepciones, basadas en particular en el consentimiento del interesado, que permiten la transferencia a un tercer país incluso en ausencia de una decisión de adecuación o de garantías adecuadas.[4]

2 Véase el artículo 45 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) (DO 2016, L 119, p. 1; en lo sucesivo, «RGPD»).

3 Véase el artículo 46 del RGPD.

4 Véase el artículo 49 del RGPD.

3. La petición de decisión prejudicial presentada por la High Court (Tribunal Superior, Irlanda) se refiere al segundo de estos mecanismos. Más concretamente, versa sobre la validez de la Decisión 2010/87/UE,[5] mediante la cual la Comisión ha establecido cláusulas contractuales tipo para determinadas categorías de transferencias, con arreglo a los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»).

4. 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, «DPC») y, por otra parte, Facebook Ireland Ltd y el Sr. Maximillian Schrems. Este presentó ante el DPC una reclamación interpuesta en relación con la transferencia de datos personales que le conciernen por parte de Facebook Ireland a Facebook Inc., su sociedad matriz establecida en los Estados Unidos de América (en lo sucesivo, «Estados Unidos»). El DPC considera que la tramitación de esta reclamación depende de que la Decisión 2010/87 sea válida. En este contexto, ha recurrido ante el órgano jurisdiccional remitente pidiéndole que pregunte al respecto al Tribunal de Justicia.

5. De entrada, debo señalar que, en mi opinión, el examen de las cuestiones prejudiciales no ha revelado ningún elemento que pueda afectar a la validez de la Decisión 2010/87.

6. Asimismo, el órgano jurisdiccional remitente ha expresado algunas dudas referidas, en esencia, a la adecuación del nivel de protección garantizado por los Estados Unidos en relación con las injerencias que generan las actividades de los servicios de inteligencia estadounidenses en el ejercicio de los derechos fundamentales de las personas cuyos datos se transfieren a este tercer país. Estas dudas ponen indirectamente en entredicho las apreciaciones efectuadas por la Comisión a este respecto en la Decisión de Ejecución (UE) 2016/1250.[6] A pesar de que la resolución del litigio principal no exige que el Tribunal de Justicia dirima esta cuestión y de que, por tanto, le sugiero que se abstenga de ello, expondré con carácter subsidiario las razones que me llevan a cuestionar la validez de esta Decisión.

7. Todo mi análisis estará dirigido a la búsqueda de un equilibrio entre, por una parte, la necesidad de demostrar un «grado de pragmatismo razonable con el fin de permitir la interacción con el resto del mundo»,[7] y, por otra parte, la de afirmar los valores fundamentales reconocidos en los ordenamientos jurídicos de la Unión y de sus Estados miembros, en particular mediante la Carta.

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

6 Decisión de la Comisión, de 12 de julio de 2016, con arreglo a la [Directiva 95/46/CE], 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 sobre el "Escudo de la privacidad"»).

7 Véase el discurso del antiguo Supervisor Europeo de Protección de Datos (SEPD) P. Hustinx, «Le droit de l'Union européenne sur la protection des données: la révision de la Directive 95/46/CE et la proposition de règlement général sur la protection des données», p. 49, disponible en la dirección de Internet https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_fr.pdf.

II. Marco jurídico

A. Directiva 95/46/CE

8. El artículo 3, apartado 2, de la Directiva 95/46/CE 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 [8] establecía lo siguiente:

«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,

[…]».

9. El artículo 13, apartado 1, de esta Directiva rezaba de la siguiente manera:

«Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión […], incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque solo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.»

8 Directiva del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (DO 1995, L 281, p. 31), en su versión modificada por el Reglamento (CE) n.º 1882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003 (DO 2003, L 284, p. 1) (en lo sucesivo, «Directiva 95/46»).

10. El artículo 25 de dicha Directiva enunciaba:

«1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

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; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

[…]

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.»

11. El artículo 26, apartados 2 y 4, de la misma 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 […] 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.»

12. El artículo 28, apartado 3, de la Directiva 95/46 estaba formulado de la siguiente manera:

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

[…]

– 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.

[…]»

B. RGPD

13. El RGPD derogó la Directiva 95/46 en virtud de su artículo 94, apartado 1, con efecto a partir del 25 de mayo de 2018, fecha en la que comenzó a aplicarse este Reglamento con arreglo a su artículo 99, apartado 2.

14. El artículo 2, apartado 2, de dicho Reglamento dispone:

«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;

[…]

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.»

15. El artículo 4, punto 2, del mismo Reglamento define el «tratamiento» como «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».

16. El artículo 23 del RGPD 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;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro […];

[…]

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.»

17. El artículo 44 de este Reglamento, titulado «Principio general de las transferencias», enuncia:

«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.»

18. Según el artículo 45 de dicho Reglamento, que lleva por título «Transferencias basadas en una decisión de adecuación»:

«1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. […]

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la [Directiva 95/46].

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. […]

6. La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

[…]

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la [Directiva 95/46] permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.»

19. El artículo 46 del mismo Reglamento, titulado «Transferencias mediante garantías adecuadas», tiene el siguiente tenor literal:

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

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

[…]

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

[…]

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la [Directiva 95/46] seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la [Directiva 95/46] permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.»

20. A tenor del artículo 58, apartados 2, 4 y 5, del RGPD:

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

a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

[…]

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

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.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.»

C. Decisión 2010/87

21. El artículo 26, apartado 4, de la Directiva 95/46 condujo a la adopción por parte de la Comisión de tres Decisiones mediante las cuales constató que las cláusulas contractuales tipo enunciadas en estas ofrecen garantías suficientes 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 respectivos derechos (en lo sucesivo, «Decisiones sobre las CCT»).[9]

22. Entre ellas figura la Decisión 2010/87, cuyo artículo 1 dispone que «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]».

23. En virtud del artículo 3 de esta Decisión:

«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 aplicable": 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;

[…]».

9 Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva [95/46] (DO 2001, L 181, p. 19); Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497 en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países (DO 2004, L 385, p. 74), así como la Decisión 2010/87.

24. En su versión inicial, el artículo 4 de dicha Decisión establecía, en su apartado 1:

«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.»

25. En su versión actual, según resulta de la modificación de la Decisión 2010/87 mediante la Decisión de Ejecución (UE) 2016/2297,[10] el artículo 4 de la Decisión 2010/87 dispone que «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».

26. El anexo de la Decisión 2010/87 contiene un conjunto de cláusulas contractuales tipo. En particular, la cláusula 3 que figura en dicho anexo, titulada «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.

[…]»

10 Decisión de la Comisión, de 16 de diciembre de 2016, por la que se modifican las Decisiones 2001/497 y 2010/87 relativas a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46 (DO 2016, L 344, p. 100).

27. La cláusula 4 enunciada en dicho anexo, que lleva por título «Obligaciones del exportador de datos», dispone:

«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;

c) el importador de datos ofrecerá garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas especificadas en el apéndice 2 del presente contrato;

d) ha verificado que, de conformidad con la legislación de protección de datos aplicable, dichas medidas resultan apropiadas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o contra cualquier otra forma ilícita de tratamiento y que dichas medidas garantizan un nivel de seguridad apropiado a los riegos que entraña el tratamiento y la naturaleza de los datos que han de protegerse, habida cuenta del estado de la técnica y del coste de su aplicación;

e) asegurará que dichas medidas se lleven a la práctica;

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;

h) pondrá a disposición de los interesados, previa petición de estos, una copia de las cláusulas, a excepción del apéndice 2, y una descripción sumaria de las medidas de seguridad, así como una copia de cualquier contrato para los servicios de subtratamiento de los datos que debe efectuarse de conformidad con las cláusulas, a menos que las cláusulas o el contrato contengan información comercial, en cuyo caso podrá eliminar dicha información comercial;

i) que, en caso de subtratamiento, la actividad de tratamiento se llevará a cabo de conformidad con la cláusula 11 por un subencargado del tratamiento que proporcionará por lo menos el mismo nivel de protección de los datos personales y los derechos de los interesados que el importador de datos en virtud de las presentes cláusulas; y

j) que asegurará que las letras a) a i) de la cláusula 4 se lleven a la práctica.»

28. La cláusula 5 prevista en el mismo anexo, titulada «Obligaciones del importador de datos», establece:

«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;

c) ha puesto en práctica las medidas de seguridad técnicas y organizativas que se indican en el apéndice 2 antes de efectuar el tratamiento de los datos personales transferidos;

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;

e) tratará adecuadamente en los períodos de tiempo prescritos todas las consultas del exportador de datos relacionadas con el tratamiento que este realice de los datos personales sujetos a transferencia y se atendrá a la opinión de la autoridad de control en lo que respecta al tratamiento de los datos transferidos;

f) ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control;

[…]».

29. Con arreglo a la nota a pie de página 1 a la que se refiere el título de la cláusula 5 que figura en el anexo de la Decisión 2010/87:

«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. Algunos ejemplos de obligaciones que no van más allá de las restricciones necesarias en una sociedad democrática son, entre otras, las sanciones reconocidas en el ámbito internacional, las obligaciones de notificación en materia fiscal o las impuestas por la lucha contra el blanqueo de dinero.»

30. La cláusula 6 contenida en este anexo, titulada «Responsabilidad», dice lo siguiente:

«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, 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, en cuyo caso los interesados podrán exigir sus derechos a dicha entidad.

[…]»

31. La cláusula 7 enunciada en dicho anexo, que lleva por título «Mediación y jurisdicción», dispone:

«1. El importador de datos acuerda que, si el interesado invoca en su contra derechos de tercero beneficiario o reclama una indemnización por daños y perjuicios con arreglo a las cláusulas, aceptará la decisión del interesado de:

a) someter el conflicto a mediación por parte de una persona independiente o, si procede, por parte de la autoridad de control;

b) someter el conflicto a los tribunales del Estado miembro de establecimiento del exportador de datos.

2. Las partes acuerdan que las opciones del interesado no obstaculizarán sus derechos sustantivos o procedimentales a obtener reparación de conformidad con otras disposiciones de Derecho nacional o internacional.»

32. La cláusula 9 recogida en el mismo anexo, titulada «Legislación aplicable», establece que las cláusulas contractuales tipo se regirán por la legislación del Estado miembro de establecimiento del exportador de datos.

D. Decisión sobre el «Escudo de la privacidad»

33. El artículo 25, apartado 6, de la Directiva 95/46 sirvió de base para la adopción por parte de la Comisión de dos Decisiones sucesivas mediante las cuales constató que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos a empresas establecidas en los Estados Unidos que, mediante un procedimiento de autocertificación, han declarado que cumplirán los principios enunciados en dichas Decisiones.

34. En primer término, la Comisión adoptó la Decisión 2000/520/CE sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de [los Estados Unidos].[11] En la sentencia de 6 de octubre de 2015, Schrems,[12] el Tribunal de Justicia declaró la invalidez de esta Decisión.

35. En segundo término, a raíz de dicha sentencia, la Comisión adoptó la Decisión sobre el «Escudo de la privacidad».

36. El artículo 1 de esta Decisión dispone:

«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.»

37. El anexo III A de esta Decisión, 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», junto a una carta del Sr. John Kerry, en ese momento Secretary of State (Secretario de Estado, Estados Unidos), de 7 de julio de 2016, contiene un memorando que describe un nuevo procedimiento de mediación ante un «Coordinador superior de la diplomacia internacional en materia de tecnología de la información» (en lo sucesivo, «Defensor del Pueblo») nombrado por el Secretario de Estado.

38. Según este memorando, dicho procedimiento se estableció «para facilitar el tratamiento de las peticiones relacionadas con el acceso a efectos de la seguridad nacional a los datos transmitidos desde la [Unión] a los Estados Unidos en virtud del Escudo de la privacidad, las cláusulas contractuales estándar, las normas vinculantes para las empresas, las "excepciones" o "posibles futuras excepciones", a través de las vías establecidas en virtud de la legislación y la política estadounidense aplicable, y la respuesta a estas peticiones».

III. Litigio principal, cuestiones prejudiciales y procedimiento ante el Tribunal de Justicia

39. El Sr. Schrems, nacional austriaco residente en Austria, es usuario de la red social Facebook. Todos los usuarios de esta red social residentes en el territorio de la Unión deben 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 estos usuarios se transfieren total o parcialmente a servidores pertenecientes a Facebook Inc., situados en el territorio de los Estados Unidos, donde son objeto de tratamiento.

11 Decisión de 26 de julio de 2000, con arreglo a la Directiva 95/46 (DO 2000, L 215, p. 7; en lo sucesivo, «Decisión de puerto seguro»).

12 C-362/14, en lo sucesivo, «sentencia Schrems», EU:C:2015:650.

40. El 25 de junio de 2013, el Sr. Schrems presentó ante el DPC una reclamación en la que le solicitaba, en esencia, que prohibiera a Facebook Ireland transferir sus datos personales a los Estados Unidos. En dicha reclamación alegaba que el Derecho y las prácticas en vigor en ese país tercero no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las injerencias derivadas de las actividades de vigilancia llevadas a cabo por las autoridades públicas. El Sr. Schrems hacía referencia en ese sentido a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de inteligencia de Estados Unidos, en particular las de la National Security Agency (Agencia de Seguridad Nacional, Estados Unidos; en lo sucesivo, «NSA»).

41. Esta reclamación fue desestimada basándose en que, en particular, toda cuestión relativa a la adecuación de la protección garantizada en los Estados Unidos debía resolverse con arreglo a la Decisión de puerto seguro. En la citada Decisión, la Comisión había declarado que este país tercero ofrecía un nivel adecuado de protección de los datos personales transferidos a empresas situadas en su territorio adheridas a los principios enunciados en dicha Decisión.

42. El Sr. Schrems interpuso un recurso contra la decisión de desestimación de su reclamación ante la High Court (Tribunal Superior). Dicho órgano jurisdiccional consideró que, si bien el Sr. Schrems no había cuestionado formalmente la validez de la Decisión de puerto seguro, en realidad su reclamación impugnaba la licitud del régimen establecido por tal Decisión. En estas circunstancias, el citado órgano jurisdiccional planteó al Tribunal de Justicia una serie de cuestiones prejudiciales que tenían por objeto, en esencia, dilucidar si las autoridades de los Estados miembros responsables de la protección de los datos (en lo sucesivo, «autoridades de control»), cuando se les formula una reclamación relativa a la protección de los derechos y libertades de una persona en relación con el tratamiento de sus datos personales que se hayan transferido a un tercer Estado, están vinculadas por las apreciaciones relativas a la adecuación del nivel de protección que ofrece dicho tercer Estado realizadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, aun cuando el reclamante impugne tales apreciaciones.

43. Tras haber declarado, en los apartados 51 y 52 de la sentencia Schrems, que una decisión de adecuación vincula a las autoridades de control mientras no haya sido declarada inválida, el Tribunal de Justicia enunció lo siguiente en los apartados 63 y 65 de la referida sentencia:

«63. […] Cuando una persona, cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país que haya sido objeto de una decisión de la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, presenta a la autoridad nacional de control una solicitud para la protección de sus derechos y libertades frente al tratamiento de esos datos, e impugna con ocasión de esa solicitud […] la compatibilidad de dicha decisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas, incumbe a esa autoridad examinar la referida solicitud con toda la diligencia exigible.

[…]

65. En el supuesto [de que] esa autoridad considere fundadas las alegaciones expuestas por [esta persona], la referida autoridad debe tener capacidad para comparecer en juicio, conforme al artículo 28, apartado 3, párrafo primero, tercer guion, de la Directiva 95/46, entendido a la luz del artículo 8, apartado 3, de la Carta. A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de esta.»

44. En dicha sentencia, el Tribunal de Justicia también examinó la validez de la Decisión de puerto seguro en relación con los requisitos derivados de la Directiva 95/46, interpretada a la luz de la Carta. Al término de dicho examen, declaró la invalidez de esa Decisión. [13]

45. A raíz de la sentencia Schrems, el órgano jurisdiccional remitente anuló la decisión mediante la cual el DPC había desestimado la reclamación del Sr. Schrems y la devolvió al DPC para que la examinase. Este último abrió una investigación e instó al Sr. Schrems a volver a presentar su reclamación habida cuenta de la declaración de invalidez de la Decisión de puerto seguro.

46. A tal fin, el Sr. Schrems solicitó a Facebook Ireland que identificara los fundamentos jurídicos en los que se basaban las transferencias de datos personales de los usuarios de la red social Facebook desde la Unión a los Estados Unidos. Facebook Ireland, sin identificar todas las bases jurídicas en las que se basaba, hizo referencia a un contrato de transferencia y tratamiento de datos (*data transfer processing agreement*) concluido entre ella misma y Facebook Inc., aplicable desde el 20 de noviembre de 2015, e invocó la Decisión 2010/87.

47. En su reclamación modificada, el Sr. Schrems alega, por una parte, que las cláusulas contenidas en dicho contrato no se ajustan a las cláusulas contractuales tipo recogidas en el anexo de la Decisión 2010/87. Por otra parte, el Sr. Schrems argumenta que, en todo caso, esas cláusulas contractuales tipo no pueden servir de base para la transferencia de datos personales relativos a su persona hacia los Estados Unidos. Afirma que esto se debe a que el Derecho estadounidense obliga a Facebook Inc. a poner los datos personales de los usuarios a disposición de las autoridades estadounidenses, como la NSA y el Federal Bureau of Investigation (Oficina Federal de Investigación, Estados Unidos; en lo sucesivo «FBI»), en el marco de programas de vigilancia que, a su entender, limitan el ejercicio de los derechos garantizados en los artículos 7, 8 y 47 de la Carta. El Sr. Schrems alega que no existe ninguna vía de recurso que permita a los interesados invocar sus derechos al respeto de la vida privada y a la protección de los datos personales. En estas condiciones, el Sr. Schrems solicita al DPC que suspenda esta transferencia en virtud del artículo 4 de la Decisión 2010/87.

48. Facebook Ireland ha reconocido, en el marco de la investigación del DPC, que continúa transfiriendo los datos personales de los usuarios de la red social Facebook residentes en la Unión a los Estados Unidos y que, a tal efecto, se basa en gran medida en las cláusulas contractuales tipo recogidas en el anexo de la Decisión 2010/87.

49. La investigación del DPC tenía por objeto determinar, por un lado, si los Estados Unidos garantizan una protección adecuada de los datos personales de los ciudadanos de la Unión y, por otro, en caso de respuesta negativa, si las Decisiones sobre las CCT ofrecen garantías suficientes en lo referente a la protección de los derechos y libertades fundamentales de estos últimos.

50. A este respecto, en un proyecto de decisión (*draft decision*), el DPC consideró con carácter provisional que el Derecho estadounidense no ofrece vías de recurso efectivas en el sentido del artículo 47 de la Carta a los ciudadanos de la Unión cuyos datos se transfieren a los Estados Unidos, donde pueden ser tratados por las agencias estadounidenses con fines de seguridad nacional de una manera incompatible con los artículos 7 y 8 de la Carta. Según el DPC, las garantías previstas en las cláusulas recogidas en los anexos de las Decisiones sobre las CCT no subsanan esta deficiencia, puesto que no vinculan a las autoridades o agencias de los Estados Unidos y solo confieren a los interesados derechos contractuales contra el exportador o el importador de los datos.

13 Véase la sentencia Schrems, apartado 106.

51. En estas circunstancias, el DPC consideró que no podía resolver la reclamación del Sr. Schrems hasta que el Tribunal de Justicia hubiera examinado la validez de las Decisiones sobre las CCT. Por lo tanto, con arreglo a lo establecido en el apartado 65 de la sentencia Schrems, el DPC inició un procedimiento ante el órgano jurisdiccional remitente al objeto de que este último, si compartía las dudas del DPC, planteara una petición de decisión prejudicial al Tribunal de Justicia sobre la validez de dichas Decisiones.

52. Se autorizó la intervención del Gobierno estadounidense, del Electronic Privacy Information Centre (EPIC), de la Business Software Alliance (BSA) y de Digitaleurope ante el órgano jurisdiccional remitente.

53. Con el fin de determinar si compartía las dudas expresadas por el DPC sobre la validez de las Decisiones sobre las CCT, la High Court (Tribunal Superior) recibió las pruebas aportadas por las partes en el litigio y oyó las alegaciones presentadas por estas, así como por los intervinientes. En particular, se presentaron pruebas periciales sobre las disposiciones del Derecho estadounidense. En Derecho irlandés, el Derecho extranjero se considera una cuestión de hecho que debe acreditarse mediante pruebas, de la misma forma que cualquier otro hecho. Sobre la base de estas pruebas, el órgano jurisdiccional remitente valoró las disposiciones del Derecho estadounidense que autorizan la vigilancia por parte de las autoridades y agencias gubernamentales, el funcionamiento de dos programas de vigilancia públicamente reconocidos («PRISM» y «Upstream»), los diferentes recursos de que disponen los particulares cuyos derechos se hayan visto vulnerados por medidas de vigilancia, así como las garantías sistémicas y los mecanismos de control. Dicho órgano jurisdiccional reseñó los resultados de esta valoración en una sentencia de primera instancia de 3 de octubre de 2017, adjunta a su resolución de remisión [en lo sucesivo, «sentencia de primera instancia de la High Court (Tribunal Superior) de 3 de octubre de 2017»].

54. En esta sentencia de primera instancia, el órgano jurisdiccional remitente hizo referencia, entre los fundamentos jurídicos que autorizan la interceptación de comunicaciones extranjeras por parte de los servicios de inteligencia estadounidenses, al artículo 702 de la Foreign Intelligence Surveillance Act (Ley de Vigilancia de la Inteligencia Exterior; en lo sucesivo, «FISA») y a la Executive Order 12333 (Decreto presidencial n.º 12333; en lo sucesivo, «EO 12333»).

55. Según las apreciaciones efectuadas en dicha sentencia de primera instancia, el artículo 702 de la FISA permite al Attorney General (Fiscal General, Estados Unidos) y al Director of National Intelligence (DNI) (Director de los Servicios de Inteligencia Nacionales, Estados Unidos; en lo sucesivo, «DNI») autorizar conjuntamente, por un plazo de un año y con el fin de obtener información en materia de inteligencia exterior, la vigilancia de personas que no sean ciudadanas estadounidenses y que no residan de forma permanente en los Estados Unidos (denominadas «personas no estadounidenses») cuando sea razonable suponer que se encuentran fuera del territorio de los Estados Unidos.[14] A tenor de la FISA, el concepto de «inteligencia exterior» significa la información relativa a la capacidad del Gobierno para prevenir los ataques extranjeros, al terrorismo, a la proliferación de las armas de destrucción masiva, así como a la administración de los asuntos exteriores de los Estados Unidos.[15]

14 50 U.S.C. 1881 (a).

15 50 U.S.C. 1881 (e).

56. Estas autorizaciones anuales, al igual que los procedimientos que regulan la selección de las personas que deben ser vigiladas y el tratamiento («minimización») de la información recopilada,[16] deben ser aprobados por el Foreign Intelligence Surveillance Court (Tribunal de Vigilancia de la Inteligencia Exterior, Estados Unidos; en lo sucesivo «FISC»). Mientras que la vigilancia «tradicional» efectuada sobre la base de otras disposiciones de la FISA exige que se establezca una «causa probable» que permita sospechar que las personas vigiladas pertenecen a una potencia extranjera o que son sus agentes, las actividades de vigilancia llevadas a cabo en virtud del artículo 702 de la FISA no están supeditadas al establecimiento de tal «causa probable» ni a la aprobación por parte del FISC de la selección de personas determinadas. Asimismo, siempre de conformidad con las apreciaciones del órgano jurisdiccional remitente, los procedimientos de minimización no se aplican a las personas no estadounidenses situadas fuera de los Estados Unidos.

57. En la práctica, una vez que el FISC ha concedido su autorización, la NSA envía a los proveedores de servicios de comunicaciones electrónicas establecidos en los Estados Unidos órdenes que contienen criterios de búsqueda, denominados «selectores», asociados a personas seleccionadas como objetivos (como números de teléfono o direcciones de correo electrónico). A continuación, estos proveedores deben transmitir a la NSA los datos correspondientes a los selectores y deben mantener en secreto las órdenes que han recibido. Pueden presentar una solicitud ante el FISC dirigida a que se modifique o descarte una orden de la NSA. La decisión del FISC puede ser objeto de recurso ante la Foreign Intelligence Surveillance Court of Review (Tribunal de Revisión de la Vigilancia de la Inteligencia Exterior, Estados Unidos; en lo sucesivo «FISCR»).

58. La High Court (Tribunal Superior) señaló que el artículo 702 de la FISA constituye la base jurídica de los programas PRISM y Upstream.

59. En el marco del programa PRISM, los proveedores de servicios de comunicaciones electrónicas deben entregar a la NSA todas las comunicaciones «procedentes» del selector comunicado por esta última o «destinadas» a este. A su juicio, una parte de estas comunicaciones se transmite al FBI y a la Central Intelligence Agency (Agencia Central de Inteligencia, Estados Unidos; en lo sucesivo, «CIA»). Según el órgano jurisdiccional remitente, en 2015, 94 386 personas fueron sometidas a vigilancia y, en 2011, el Gobierno estadounidense se hizo con más de 250 millones de comunicaciones en el marco de este programa.

60. El programa Upstream se basa en la asistencia obligatoria de las empresas que explotan la «red troncal» —a saber, la red de cables, conmutadores y enrutadores— por la que circulan las comunicaciones telefónicas y las comunicaciones por Internet. Estas empresas están obligadas a permitir a la NSA copiar y filtrar los flujos de tráfico de Internet con el fin de obtener comunicaciones «procedentes» de un selector mencionado en una orden de dicha agencia o «destinadas» o «relativas» a este. Las comunicaciones «relativas» a un selector designan a aquellas que hacen referencia a dicho selector, sin que la persona no estadounidense asociada a dicho selector participe necesariamente en ellas. Aunque de un dictamen del FISC de 26 de abril de 2017 se desprende que, desde esa fecha, el Gobierno estadounidense ya no recoge ni obtiene comunicaciones «relativas» a un selector, este dictamen no indica que la NSA haya dejado de copiar y filtrar los flujos de comunicaciones que circulan a través de su dispositivo de vigilancia. De este modo, en su opinión, el programa Upstream implica el acceso de la NSA tanto a los metadatos como al contenido de las comunicaciones. Considera que, desde 2011, la NSA ha recopilado alrededor de 26,5 millones de comunicaciones cada año en el marco del programa Upstream, lo que, no obstante, únicamente representa una pequeña parte de las comunicaciones sujetas al proceso de filtrado llevado a cabo en virtud de este programa.

16 El órgano jurisdiccional remitente ha señalado que los procedimientos de fijación de objetivos se refieren a la forma en que el Poder Ejecutivo determina que es razonable suponer que un individuo particular es una persona no estadounidense situada fuera de los Estados Unidos y que la selección de este individuo puede conducir a la adquisición de información en materia de inteligencia exterior. Los procedimientos de minimización comprenden la adquisición, la conservación, la utilización y la divulgación de toda información no pública relativa a una persona estadounidense adquirida con arreglo al artículo 702 de la FISA.

61. Asimismo, según las apreciaciones realizadas por la High Court (Tribunal Superior), el EO 12333 autoriza la vigilancia de las comunicaciones electrónicas fuera del territorio de los Estados Unidos al permitir el acceso, con fines de inteligencia exterior, a datos que bien están «en tránsito» hacia dicho territorio, o bien «circulan» por dicho territorio sin estar destinados a ser objeto de tratamiento en este, así como la recogida y conservación de tales datos. El EO 12333 define el concepto de «inteligencia exterior» en el sentido de que incluye la información relativa a las capacidades, intenciones o actividades de gobiernos extranjeros, organizaciones extranjeras o personas extranjeras. [17]

62. Según la High Court (Tribunal Superior), el EO 12333 habilita a la NSA para acceder a los cables submarinos situados sobre el lecho del océano Atlántico mediante los cuales se transfieren datos desde la Unión hacia los Estados Unidos, antes de que dichos datos lleguen a los Estados Unidos y estén sujetos, por este motivo, a las disposiciones de la FISA. Sin embargo, no existe ninguna prueba de la existencia de un programa semejante que se aplique en virtud de este decreto presidencial.

63. Aunque el EO 12333 establece límites relativos a la recogida, la conservación y la divulgación de información, estos límites no se aplican a las personas no estadounidenses. Estas últimas disfrutan únicamente de las garantías establecidas en la Presidential Policy Directive 28 (Orden Estratégica Presidencial n.º 28; en lo sucesivo, «PPD 28»), que se aplica a todas las actividades de recogida y utilización de información en materia de inteligencia exterior de señales. La PPD 28 dispone que el respeto a la vida privada forma parte integrante de las consideraciones que deben tenerse en cuenta en la planificación de estas actividades, que la recogida debe tener como único objetivo la adquisición de información en materia de inteligencia exterior, así como de contraespionaje, y que dichas actividades deben ser «lo más adaptadas posible».

64. Según el órgano jurisdiccional remitente, las actividades de la NSA basadas en el EO 12333, que el Presidente de los Estados Unidos puede modificar o revocar en cualquier momento, no se rigen por la ley, no son objeto de control jurisdiccional y no pueden ser objeto de recursos judiciales.

65. Sobre la base de estas apreciaciones, el citado órgano jurisdiccional considera que los Estados Unidos realizan un tratamiento masivo e indiscriminado de datos personales que podría exponer a los interesados al riesgo de que se violasen los derechos que les otorgan los artículos 7 y 8 de la Carta.

66. Más aún, dicho órgano jurisdiccional indica que los ciudadanos de la Unión no tienen acceso a los mismos recursos judiciales contra el tratamiento ilegal de sus datos personales por parte de las autoridades estadounidenses que los nacionales estadounidenses. La cuarta enmienda de la Constitución de los Estados Unidos, que a su entender constituye la protección más importante contra la vigilancia ilegal, no es aplicable a los ciudadanos de la Unión que carezcan de una conexión voluntaria significativa con los Estados Unidos. Si bien estos últimos, a pesar de todo, disponen de algunos otros recursos, se enfrentan a obstáculos importantes.

67. En particular, el artículo III de la Constitución de los Estados Unidos supedita todo recurso ante los tribunales federales a que el interesado acredite su legitimación activa (*standing*). La legitimación activa supone, en particular, que esa persona demuestre que ha sufrido un perjuicio real que sea, por una parte, concreto y particularizado, y, por otra, actual o inminente. Haciendo referencia, entre otras, a la sentencia de la Supreme Court of the United States (Tribunal Supremo de los Estados Unidos, Estados Unidos), Clapper v. Amnesty International US, [18] el órgano jurisdiccional remitente considera que, en la práctica, este requisito es excesivamente difícil de cumplir, habida cuenta, en particular, de que no existe obligación alguna de informar a los interesados sobre las medidas de vigilancia

17 EO 12333, apartado 3.5, letra e).

18 133 S.Ct. 1138 (2013).

adoptadas en su contra.[19] Asimismo, entiende que una parte de los recursos a disposición de los ciudadanos de la Unión está sujeta al cumplimiento de otros requisitos restrictivos, como la necesidad de demostrar la existencia de un perjuicio económico. La inmunidad soberana reconocida a las agencias de inteligencia y la clasificación de la información de que se trata también obstaculizan el ejercicio de determinadas vías de recurso.[20]

68. Asimismo, la High Court (Tribunal Superior) menciona diversos mecanismos de control y de supervisión de las actividades de las agencias de inteligencia.

69. Entre ellos figuran, por un lado, el mecanismo de certificación anual por parte del FISC de los programas basados en el artículo 702 de la FISA, en cuyo marco, no obstante, el FISC no aprueba los selectores individuales. Además, ningún control judicial previo regula la recogida de información en materia de inteligencia exterior con arreglo al EO 12333.

70. Por otro lado, el órgano jurisdiccional remitente hace referencia a diversos mecanismos de supervisión extrajudicial de las actividades de inteligencia. Menciona, en particular, el papel que desempeñan los Inspectors General (Inspectores Generales, Estados Unidos) quienes, dentro de cada agencia de inteligencia, son responsables de la supervisión de las actividades de vigilancia. Además, el Privacy and Civil Liberties Oversight Board (Consejo de Vigilancia de la Vida Privada y de las Libertades Civiles, Estados Unidos; en lo sucesivo, «PCLOB»), una agencia independiente dentro del Poder Ejecutivo, recibe los informes de personas nombradas dentro de cada agencia como agentes de las libertades civiles o de la vida privada (*civil liberties or privacy officers*). El PCLOB elabora regularmente informes para las comisiones parlamentarias y el Presidente. Las agencias de que se trata deben comunicar entre otros al DNI los incidentes relativos al incumplimiento de las normas y procedimientos que regulan la recogida de inteligencia exterior. Estos incidentes también se notifican al FISC. El Congreso de los Estados Unidos, a través de las comisiones de inteligencia de la Cámara de Representantes y del Senado, por su parte, es asimismo responsable de controlar las actividades de inteligencia exterior.

71. Sin embargo, la High Court (Tribunal Superior) destaca la diferencia fundamental entre, por una parte, las normas que tienen por objeto garantizar que los datos se obtengan de forma legal y que, una vez obtenidos, no se haga un uso abusivo de ellos, y, por otra parte, los recursos disponibles cuando se infringen dichas normas. La protección de los derechos fundamentales de los interesados solo se garantiza, a su entender, si existen vías de recurso efectivas que les permitan invocar sus derechos en caso de incumplimiento de dichas normas.

72. En estas circunstancias, el órgano jurisdiccional remitente considera fundadas las alegaciones, invocadas por el DPC, según las cuales las limitaciones que impone el Derecho estadounidense al derecho de recurso de las personas cuyos datos se transfieren desde la Unión no respetan el contenido esencial del derecho garantizado en el artículo 47 de la Carta y, en todo caso, constituyen injerencias desproporcionadas en el ejercicio de dicho derecho.

73. Según la High Court (Tribunal Superior), la introducción por parte del Gobierno estadounidense del mecanismo de mediación descrito en la Decisión sobre el «Escudo de la privacidad» no desvirtúa esta apreciación. Tras haber señalado que pueden acceder a este mecanismo los ciudadanos de la Unión que consideren de forma razonable que sus datos se han transferido con arreglo a las

19 Sin embargo, el órgano jurisdiccional remitente ha señalado que el principio según el cual no se exige la notificación a la persona a la que se refiere una medida de vigilancia tiene una excepción, cuando el Gobierno estadounidense pretenda utilizar datos recogidos con arreglo al artículo 702 de la FISA contra dicha persona en el marco de un procedimiento penal o administrativo.

20 En particular, el órgano jurisdiccional remitente ha señalado que, si bien la Judicial Redress Act (Ley sobre la Tutela judicial; en lo sucesivo, «JRA») ha ampliado a los ciudadanos de la Unión las disposiciones de la Privacy Act (Ley sobre la Protección de la Vida Privada), que permite el acceso de las personas físicas a la información referida a estas en posesión de determinadas agencias en relación con determinados terceros países, la NSA no figura en el listado de agencias enumeradas en virtud de la JRA.

Decisiones sobre las CCT,[21] este órgano jurisdiccional observó que el Defensor del Pueblo no constituye un tribunal que responda a los requisitos establecidos en el artículo 47 de la Carta y, en particular, no es independiente del Poder Ejecutivo.[22] Dicho órgano jurisdiccional duda también de que la intervención del Defensor del Pueblo, cuyas decisiones no pueden ser objeto de un recurso judicial, represente una vía de recurso efectiva. En efecto, esta intervención no permite a las personas cuyos datos personales hayan sido recogidos, tratados o compartidos ilegalmente obtener una indemnización o una orden conminatoria para el cese de los actos ilegales, dado que el Defensor del Pueblo no confirma ni niega que un solicitante haya sido objeto de una medida de vigilancia electrónica.

74. Tras haber expuesto de esta manera sus inquietudes acerca de la equivalencia sustancial entre las garantías establecidas en el Derecho estadounidense y los requisitos derivados de los artículos 7, 8 y 47 de la Carta, el órgano jurisdiccional remitente expresó sus dudas acerca de si las cláusulas contractuales tipo previstas en las Decisiones sobre las CCT —que, por su propia naturaleza, no vinculan a las autoridades estadounidenses— pueden, con todo, garantizar la protección de los derechos fundamentales de los interesados. Este órgano jurisdiccional concluyó de lo anterior que comparte las dudas del DPC relativas a la validez de estas Decisiones.

75. A este respecto, el órgano jurisdiccional remitente considera, en particular, que el artículo 28, apartado 3, de la Directiva 95/46, al que hace referencia el artículo 4 de la Decisión 2010/87, en la medida en que reconoce a las autoridades de control la facultad de suspender o prohibir las transferencias basadas en las cláusulas contractuales tipo previstas en esta Decisión, no basta para disipar estas dudas. Además de que esta facultad únicamente tiene, a su entender, un carácter discrecional, el órgano jurisdiccional remitente se pregunta, a la vista del considerando 11 de la Decisión 2010/87, sobre la posibilidad de ejercitarla cuando las deficiencias constatadas no se refieran a un caso particular y excepcional, sino que tengan un carácter general y sistémico.[23] Considera igualmente que el riesgo de que se pronuncien decisiones contradictorias en diferentes Estados miembros podría oponerse a que se confíe la apreciación de tales deficiencias a las autoridades de control.

76. En estas circunstancias, la High Court (Tribunal Superior) decidió, mediante resolución de 4 de mayo de 2018,[24] presentada ante el Tribunal de Justicia el 9 de mayo de 2018, 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 2010/87], 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?

21 El órgano jurisdiccional remitente hace referencia, a este respecto, al anexo III A de la Decisión sobre el «Escudo de la privacidad» (véanse los puntos 37 y 38 de las presentes conclusiones).

22 El órgano jurisdiccional remitente invoca la sentencia de 27 de enero de 2005, Denuit y Cordenier (C-125/04, EU:C:2005:69), apartado 12.

23 El considerando 11 de la Decisión 2010/87 dispone: «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.»

24 Facebook Ireland interpuso un recurso contra la resolución de remisión ante la Supreme Court (Tribunal Supremo, Irlanda). Este recurso fue desestimado mediante la sentencia de 31 de mayo de 2019, The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Appeal n.º 2018/68 [en lo sucesivo, «sentencia de la Supreme Court (Tribunal Supremo) de 31 de mayo de 2019»].

2) a) A efectos de la Directiva [95/46], al determinar si el hecho de transferir con arreglo a la Decisión [2010/87] 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 TUE, el TFUE, 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 (en lo sucesivo, "CEDH")] (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 2010/87], 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 [2010/87]:

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 [2010/87] 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 [2010/87], ¿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 control], entran en conflicto con las [cláusulas contractuales tipo], los artículos 25 y 26 de la Directiva [95/46] o la Carta, ¿está obligada una [autoridad de control] 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 2010/87], o acaso puede la [autoridad de control] 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 [sobre el "Escudo de la privacidad"] una constatación de alcance general vinculante para las [autoridades de control] 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 sobre el ["Escudo de la privacidad"] en la valoración efectuada en cuanto a la adecuación de la protección ofrecida a los datos transferidos a EE. UU. conforme a la Decisión [2010/87]?

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 [III A] de la Decisión sobre el ["Escudo de la privacidad"], 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 [2010/87]?

11) ¿Viola la Decisión [2010/87] los artículos 7, 8 y/o 47 de la Carta?»

77. El DPC, Facebook Ireland, el Sr. Schrems, el Gobierno estadounidense, el EPIC, la BSA, Digitaleurope, Irlanda, los Gobiernos alemán, neerlandés, austriaco, polaco, portugués y del Reino Unido, el Parlamento Europeo y la Comisión presentaron observaciones escritas ante el Tribunal de Justicia. El DPC, Facebook Ireland, el Sr. Schrems, el Gobierno estadounidense, el EPIC, la BSA, Digitaleurope, Irlanda, los Gobiernos belga, checo, alemán, francés, neerlandés, austriaco y del Reino Unido, el Parlamento, la Comisión y el Comité Europeo de Protección de Datos (CEPD) estuvieron representados en la vista celebrada el 9 de julio de 2019.

IV. Apreciación

A. Observaciones preliminares

78. Tras la invalidación de la Decisión de puerto seguro por parte del Tribunal de Justicia en la sentencia Schrems, las transferencias de datos personales hacia los Estados Unidos continuaron sobre la base de otros fundamentos jurídicos. En particular, las sociedades exportadoras de datos pudieron recurrir a contratos con los importadores de datos que incluían cláusulas tipo elaboradas por la Comisión. Estas cláusulas sirven también de base jurídica para las transferencias hacia una multitud de otros países terceros respecto de los cuales la Comisión no ha adoptado una decisión de adecuación.[25] Actualmente, la Decisión sobre el «Escudo de la privacidad» permite a las empresas que hayan autocertificado su adhesión a los principios enunciados en esta transferir datos personales a los Estados Unidos sin otras formalidades.

79. Tal como indica expresamente la resolución de remisión y como destacaron la BSA, Digitaleurope, Irlanda, los Gobiernos austriaco y francés, el Parlamento y la Comisión, el litigio principal, que está pendiente ante la High Court (Tribunal Superior), tiene por único objeto determinar si la Decisión mediante la cual la Comisión estableció las cláusulas contractuales tipo invocadas en apoyo de las transferencias contempladas en la reclamación del Sr. Schrems, a saber la Decisión 2010/87,[26] es válida.

80. Este litigio tiene su origen en una demanda mediante la cual el DPC solicitó al órgano jurisdiccional remitente que planteara al Tribunal de Justicia una cuestión prejudicial relativa a la validez de la Decisión 2010/87. Según este órgano jurisdiccional, el litigio principal se refiere, por tanto, al ejercicio de la vía de recurso que el Tribunal de Justicia exigió a los Estados miembros que establecieran en el apartado 65 de la sentencia Schrems.

81. Cabe recordar que, en el apartado 63 de esa sentencia, el Tribunal de Justicia declaró que las autoridades de control deben tramitar con toda la diligencia exigible las reclamaciones en cuyo marco una persona cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país que haya sido objeto de una decisión de adecuación impugne la compatibilidad de dicha decisión con la protección de los derechos fundamentales consagrados en la Carta. Con arreglo al apartado 65 de dicha sentencia, cuando esa autoridad considere fundadas las alegaciones expuestas en la mencionada reclamación, la referida autoridad debe tener capacidad para comparecer en juicio, con arreglo al artículo 28, apartado 3, párrafo primero, tercer guion, de la Directiva 95/46 (que concuerda con el artículo 58, apartado 5, del RGPD), interpretado a la luz del artículo 8, apartado 3, de la Carta. A este efecto, el legislador nacional debe establecer vías de acción que permitan a dicha autoridad de control exponer estas alegaciones ante los órganos jurisdiccionales nacionales para que estos últimos, si concuerdan con las dudas de dicha autoridad, planteen una petición de decisión prejudicial sobre la validez de la decisión en cuestión.

82. Al igual que el órgano jurisdiccional remitente, considero que estas conclusiones son aplicables por analogía cuando, con ocasión de la tramitación de una reclamación presentada ante ella, una autoridad de control alberga dudas sobre la validez no de una decisión de adecuación, sino de una decisión, como la Decisión 2010/87, que establezca cláusulas contractuales tipo para la transferencia de datos

25 La BSA afirma que el 70 % de las empresas que son miembros de esta alianza y que respondieron a una encuesta al respecto declararon haber recurrido a cláusulas contractuales tipo como fundamento principal de las transferencias de datos personales a terceros países. Digitaleurope considera también que las cláusulas contractuales tipo representan el instrumento jurídico principal invocado en apoyo de dichas transferencias.

26 Aunque el órgano jurisdiccional remitente indica que su petición de decisión prejudicial tiene por objeto la validez de las tres Decisiones sobre las CCT, que se examinan en el proyecto de decisión del DPC y en la sentencia de primera instancia de la High Court (Tribunal Superior) de 3 de octubre de 2017, las cuestiones prejudiciales se refieren exclusivamente a la Decisión 2010/87. Esto es así debido a que Facebook Ireland identificó dicha Decisión ante este órgano jurisdiccional como la base jurídica de las transferencias de los datos de los usuarios europeos de la red social Facebook a los Estados Unidos. Por lo tanto, mi análisis se referirá únicamente a esa Decisión.

personales a terceros países. En contra de lo alegado por el Gobierno alemán, carece de relevancia el hecho de que tales dudas se correspondan con imputaciones invocadas por quien interpuso la reclamación o de que tal autoridad cuestione por propia iniciativa la validez de la decisión de que se trate. En efecto, los requisitos que establecen el artículo 58, apartado 5, del RGPD y el artículo 8, apartado 3, de la Carta, en los que se fundamentó la motivación del Tribunal de Justicia, se aplican con independencia de cuáles sean el fundamento jurídico de la transferencia a la que se refiere la reclamación presentada ante la autoridad de control y los motivos que han llevado a esta autoridad a poner en duda la validez de la decisión de que se trate en el contexto de la tramitación de dicha reclamación.

83. Una vez hechas estas puntualizaciones, si el DPC solicitó al órgano jurisdiccional remitente que consultara al Tribunal de Justicia sobre la validez de la Decisión 2010/87 fue porque le pareció necesario obtener una aclaración del Tribunal de Justicia a este respecto para tramitar la reclamación mediante la cual el Sr. Schrems le solicita que ejerza la facultad, de la que disponía en virtud del artículo 28, apartado 3, segundo guion, de la Directiva 95/46 —y que actualmente le confiere el artículo 58, apartado 2, letra f), del RGPD—, de suspender la transferencia de sus datos personales por parte de Facebook Ireland a Facebook Inc.

84. Así pues, aunque el litigio principal tiene únicamente por objeto la validez *in abstracto* de la Decisión 2010/87, el procedimiento subyacente en curso ante el DPC versa sobre el ejercicio por parte de este de su facultad de adoptar medidas correctoras *en un caso concreto*. Quisiera proponer al Tribunal de Justicia que se limite a examinar las cuestiones prejudiciales planteadas en la medida necesaria para pronunciarse sobre la validez de la Decisión 2010/87, dado que tal examen es suficiente para que el órgano jurisdiccional remitente resuelva el litigio del que conoce. [27]

85. Antes de analizar la validez de esta Decisión, es preciso descartar algunas objeciones planteadas contra la admisibilidad de la petición de decisión prejudicial.

B. Sobre la admisibilidad de la petición de decisión prejudicial

86. La admisibilidad de la petición de decisión prejudicial se ha impugnado por diversos motivos, referidos, esencialmente, a la inaplicabilidad *ratione temporis* de la Directiva 95/46 contemplada en las cuestiones prejudiciales (sección 1), al hecho de que se afirma que el procedimiento incoado ante el DPC no ha alcanzado una fase suficientemente avanzada para justificar su utilidad (sección 2) y a la persistencia de dudas relativas al marco fáctico descrito por el órgano jurisdiccional remitente (sección 3).

87. Responderé a estas causas de inadmisión de la demanda teniendo presente la presunción de pertinencia de que gozan las cuestiones prejudiciales planteadas al Tribunal de Justicia con arreglo al artículo 267 TFUE. Según reiterada jurisprudencia, el Tribunal de Justicia solo puede abstenerse de pronunciarse sobre una petición de decisión prejudicial cuando resulte evidente que la interpretación solicitada del Derecho de la Unión carece de 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 o de Derecho necesarios para responder de manera útil a las cuestiones planteadas. [28]

27 Véanse los puntos 167 a 186 de las presentes conclusiones.

28 Véanse, en particular, las sentencias de 10 de diciembre de 2018, Wightman y otros (C-621/18, EU:C:2018:999), apartado 27, y de 19 de noviembre de 2019, A. K. y otros (Independencia de la Sala Disciplinaria del Tribunal Supremo) (C-585/18, C-624/18 y C-625/18, EU:C:2019:982), apartado 98.

1. Sobre la aplicabilidad ratione temporis de la Directiva 95/46

88. Facebook Ireland alega la inadmisibilidad de las cuestiones prejudiciales basándose en que hacen referencia a la Directiva 95/46, cuando esta Directiva fue derogada y sustituida por el RGPD con efecto a partir del 25 de mayo de 2018. [29]

89. Comparto el punto de vista según el cual la validez de la Decisión 2010/87 debe examinarse a la luz de las disposiciones del RGPD.

90. A tenor del artículo 94, apartado 2, de este Reglamento, «toda referencia a la Directiva derogada se entenderá hecha [a dicho Reglamento]». A mi juicio, de ello se desprende que la Decisión 2010/87, en la medida en que menciona como fundamento jurídico el artículo 26, apartado 4, de la Directiva 95/46, debe entenderse en el sentido de que hace referencia al artículo 46, apartado 2, letra c), del RGPD, que reproduce en esencia su contenido. [30] Por consiguiente, las decisiones de ejecución adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46, antes de la entrada en vigor del RGPD, deben interpretarse a la luz de dicho Reglamento. Su validez también debe evaluarse, en su caso, en función del referido Reglamento.

91. Esta conclusión no se ve desvirtuada por la jurisprudencia según la cual la legalidad de un acto de la Unión debe apreciarse en función de los elementos de hecho y de Derecho existentes en la fecha en que se adoptó dicho acto. Esta jurisprudencia se refiere, en efecto, al examen de la validez de un acto de la Unión en relación con las circunstancias de hecho pertinentes en el momento de su adopción [31] o de las normas procesales que regulan su adopción. [32] En cambio, el Tribunal de Justicia ha examinado de forma reiterada la validez de actos de Derecho derivado en función de normas sustantivas de rango superior que entraron en vigor después de la adopción de dichos actos. [33]

92. Sin embargo, la mención, en el enunciado de las cuestiones prejudiciales, de un acto que ya no resulta aplicable *ratione temporis*, si bien justifica la reformulación de esas cuestiones, no puede suponer su inadmisión. [34] Como han alegado el DPC y el Sr. Schrems, las referencias a la Directiva 95/46 en el enunciado de las cuestiones prejudiciales, por lo demás, pueden explicarse a la luz del calendario procesal del presente asunto, dado que dichas cuestiones fueron planteadas al Tribunal de Justicia antes de la entrada en vigor del RGPD.

93. En cualquier caso, las disposiciones del RGPD que se abordarán a los efectos del análisis de las cuestiones prejudiciales —a saber, en particular, sus artículos 45, 46 y 58— reproducen en esencia, aunque desarrollándolo y con ciertas matizaciones, el contenido de los artículos 25, 26 y 28 de la Directiva 95/46. En lo tocante a sus aspectos pertinentes para resolver sobre la validez de la Decisión 2010/87, no veo ninguna razón para atribuir a estas disposiciones del RGPD un alcance distinto al de las disposiciones concordantes de la Directiva 95/46. [35]

29 Véanse los artículos 94, apartado 1, y 99, apartado 1, del RGPD.

30 Debo destacar que, con arreglo al artículo 46, apartado 5, del RGPD, las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46 permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.

31 Véanse, en particular, las sentencias de 7 de febrero de 1979, Francia/Comisión (15/76 y 16/76, EU:C:1979:29), apartado 7; de 17 de mayo de 2001, IECC/Comisión (C-449/98 P, EU:C:2001:275), apartado 87, y de 17 de octubre de 2013, Schaible (C-101/12, EU:C:2013:661), apartado 50.

32 Véanse, en particular, las sentencias de 16 de abril de 2015, Parlamento/Consejo (C-540/13, EU:C:2015:224), apartado 35; de 16 de abril de 2015, Parlamento/Consejo (C-317/13 y C-679/13, EU:C:2015:223), apartado 45, y de 22 de septiembre de 2016, Parlamento/Consejo (C-14/15 y C-116/15, EU:C:2016:715), apartado 48.

33 En particular, en la sentencia Schrems, el Tribunal de Justicia examinó la validez de la Decisión de puerto seguro a la luz de las disposiciones de la Carta, cuya adopción es posterior a la de esta Decisión. Véanse también las sentencias de 17 de marzo de 2011, AJD Tuna (C-221/09, EU:C:2011:153), apartado 48, y de 11 de junio de 2015, Pfeifer & Langen (C-51/14, EU:C:2015:380), apartado 42.

34 Véanse, en particular, las sentencias de 15 de julio de 2010, Pannon Gép Centrum (C-368/09, EU:C:2010:441), apartados 30 a 35; de 10 de febrero de 2011, Andersson (C-30/10, EU:C:2011:66), apartados 20 y 21, y de 25 de octubre de 2018, Roche Lietuva (C-413/17, EU:C:2018:865), apartados 17 a 20.

35 Véanse, a este respecto, las conclusiones del Abogado General Bobek presentadas en el asunto Fashion ID (C-40/17, EU:C:2018:1039), punto 87.

2. Sobre el carácter provisional de las dudas expresadas por el DPC

94. Según el Gobierno alemán, la petición de decisión prejudicial es inadmisible debido a que el procedimiento de recurso al que se alude en el apartado 65 de la sentencia Schrems supone que la autoridad de control se haya formado una opinión definitiva en cuanto a la procedencia de las alegaciones invocadas por el recurrente contra la validez de la Decisión en cuestión. A su entender, esto no sucede en el presente asunto, en la medida en que el DPC ha expresado sus dudas sobre la validez de la Decisión 2010/87 —que el Sr. Schrems, por lo demás, no rebate— en un proyecto de decisión presentado con carácter provisional, sin perjuicio de la posible presentación de observaciones complementarias por parte de Facebook Ireland y del Sr. Schrems.

95. En mi opinión, el carácter provisional de las dudas expresadas por el DPC no afecta a la admisibilidad de la petición de decisión prejudicial. En efecto, los criterios de admisibilidad de una cuestión prejudicial deben apreciarse en relación con el objeto del litigio tal como lo haya definido el órgano jurisdiccional remitente.[36] Pues bien, consta que este se refiere a la validez de la Decisión 2010/87. Según la resolución de remisión y la sentencia de primera instancia adjunta a esta, dicho órgano jurisdiccional estimó que las dudas expresadas por el DPC —con independencia de si estas se expresaron con carácter provisional o definitivo— estaban fundadas y, en consecuencia, preguntó al Tribunal de Justicia sobre la validez de dicha Decisión. En estas condiciones, las aclaraciones que pueda aportar el Tribunal de Justicia a este respecto son sin duda pertinentes para permitirle pronunciarse sobre el litigio del que conoce.

3. Sobre las dudas que rodean a la definición del marco fáctico

96. El Gobierno del Reino Unido alega que el marco fáctico descrito por el órgano jurisdiccional remitente presenta diversas lagunas que comprometen la admisibilidad de las cuestiones prejudiciales. Considera que el referido órgano jurisdiccional no ha aclarado si los datos personales relativos al Sr. Schrems fueron efectivamente transferidos a los Estados Unidos ni, en caso de respuesta afirmativa, si fueron recogidos por las autoridades estadounidenses. A su entender, tampoco se ha identificado con certeza la base jurídica de estas posibles transferencias, ya que la resolución de remisión se ha limitado a mencionar que los datos de los usuarios europeos de la red social Facebook se transfieren «en gran medida» basándose en las cláusulas contractuales tipo previstas en la Decisión 2010/87. En cualquier caso, entiende que no se ha acreditado que el contrato entre Facebook Ireland y Facebook Inc., invocado en apoyo de la transferencia controvertida, incorpore de forma fiel tales cláusulas. El Gobierno alemán también impugna la admisibilidad de la petición de decisión prejudicial alegando que el órgano jurisdiccional remitente no ha examinado si el Sr. Schrems dio su consentimiento de forma indubitada a las transferencias en cuestión, en cuyo caso estas se habrían basado de forma válida en el artículo 26, apartado 1, de la Directiva 95/46 [cuyo contenido reproduce esencialmente el artículo 49, apartado 1, letra a), del RGPD].

97. Estos argumentos no cuestionan en absoluto la pertinencia de la petición de decisión prejudicial en relación con el objeto del litigio principal. Dado que este litigio tiene su origen en el ejercicio por parte del DPC de la vía de recurso prevista en el apartado 65 de la sentencia Schrems, su propio objeto consiste en conseguir que el órgano jurisdiccional nacional plantee una petición de decisión prejudicial sobre la validez de la Decisión 2010/87. Los Gobiernos alemán y del Reino Unido niegan, en realidad, la necesidad de las cuestiones prejudiciales, no para determinar si dicha Decisión es válida, sino más bien para permitir al DPC pronunciarse *in concreto* sobre la reclamación del Sr. Schrems.

36 Véase el punto 87 de las presentes conclusiones.

98. En todo caso, incluso desde el punto de vista de este procedimiento subyacente al litigio principal, no me parece que las cuestiones prejudiciales relativas a la validez de la Decisión 2010/87 carezcan de pertinencia. En efecto, el órgano jurisdiccional remitente ha acreditado que Facebook Ireland continuó transfiriendo los datos de sus usuarios hacia los Estados Unidos tras la invalidación de la Decisión de puerto seguro y que estas transferencias se basaron, al menos en parte, en la Decisión 2010/87. Además, aunque puede tener sus ventajas que el conjunto de los hechos pertinentes se establezca antes de que ejerza su competencia con arreglo al artículo 267 TFUE, corresponde únicamente al órgano jurisdiccional remitente apreciar en qué fase del procedimiento necesita una decisión prejudicial del Tribunal de Justicia. [37]

99. Habida cuenta de las consideraciones precedentes, considero que la petición de decisión prejudicial es admisible.

C. Sobre la aplicabilidad del Derecho de la Unión a las transferencias con fines comerciales de datos personales a un tercer Estado que puede tratarlos por razones de seguridad nacional (primera cuestión prejudicial)

100. Mediante su primera cuestión prejudicial, el órgano jurisdiccional remitente pretende averiguar si el Derecho de la Unión es aplicable a una transferencia de datos personales por parte de una sociedad situada en un Estado miembro a una sociedad establecida en un tercer país realizada por razones comerciales cuando, tras haber iniciado la transferencia, los datos pueden ser tratados por las autoridades públicas de ese tercer país con fines que incluyen la protección de la seguridad nacional.

101. La trascendencia de esta cuestión para la resolución del litigio principal reside en el hecho de que, si tal transferencia quedara fuera del ámbito de aplicación del Derecho de la Unión, el conjunto de las objeciones formuladas contra la validez de la Decisión 2010/87 en el presente asunto se vería privado de fundamento.

102. Tal como ha observado el órgano jurisdiccional remitente, los tratamientos de datos personales que tienen por objeto la seguridad nacional estaban excluidos del ámbito de aplicación de la Directiva 95/46 en virtud del artículo 3, apartado 2, de esta Directiva. Actualmente, el artículo 2, apartado 2, del RGPD precisa que este Reglamento no se aplica, en particular, a los tratamientos de datos en el marco de una actividad que no se encuentre comprendida en el ámbito de aplicación del Derecho de la Unión o efectuados por las autoridades competentes con fines de protección de la seguridad pública. Estas disposiciones reflejan la reserva de competencia que el artículo 4 TUE, apartado 2, reconoce a los Estados miembros en materia de protección de la seguridad nacional.

103. El DPC, el Sr. Schrems, Irlanda, los Gobiernos alemán, austriaco, belga, checo, neerlandés, polaco y portugués, así como el Parlamento y la Comisión alegan que transferencias como las contempladas en la reclamación del Sr. Schrems no están cubiertas por estas disposiciones y, por tanto, están comprendidas en el ámbito de aplicación del Derecho de la Unión. Facebook Ireland defiende la tesis contraria. Suscribo el punto de vista de los primeros.

104. A este respecto, es importante señalar que la transferencia de datos personales a partir de un Estado miembro hacia un tercer país constituye, en sí misma, un «tratamiento», en el sentido del artículo 4, apartado 2, del RGPD, efectuado en el territorio de un Estado miembro. [38] La primera cuestión prejudicial tiene precisamente por objeto determinar si el Derecho de la Unión se aplica *al*

37 Véanse, en este sentido, las sentencias de 1 de abril de 1982, Holdijk y otros (141/81 a 143/81, EU:C:1982:122), apartado 5, y de 9 de diciembre de 2003, Gasser (C-116/02, EU:C:2003:657), apartado 27.

38 Véanse, en este sentido, la sentencia de 30 de mayo de 2006, Parlamento/Consejo y Comisión (C-317/04 y C-318/04, en lo sucesivo, «sentencia PNR», EU:C:2006:346), apartado 56, y la sentencia Schrems (apartado 45). El artículo 4, apartado 2, del RGPD reproduce esencialmente la definición del concepto de «tratamiento» que figuraba en el artículo 2, letra b), de la Directiva 95/46.

tratamiento constituido por la propia transferencia. Esta cuestión no se refiere a la aplicabilidad del Derecho de la Unión a los posibles tratamientos posteriores, por las autoridades estadounidenses por razones de seguridad nacional, de los datos transferidos a los Estados Unidos, que no están comprendidos en el ámbito de aplicación territorial del RGPD. [39]

105. Desde esta perspectiva, a los efectos de determinar si el Derecho de la Unión se aplica a la transferencia de datos de que se trata, solo debe tomarse en consideración la actividad en el marco de la cual se inscribe esta transferencia, sin importar el objeto de los posibles tratamientos posteriores que sufrirán los datos transferidos por las autoridades públicas del tercer país de destino. [40]

106. Pues bien, de la resolución de remisión se desprende que la transferencia a la que se refiere la reclamación del Sr. Schrems forma parte de una actividad comercial. Además, esta transferencia no se produce con el objetivo de permitir el tratamiento posterior de los datos de que se trata por las autoridades estadounidenses por razones de seguridad nacional.

107. A mayor abundamiento, el enfoque propuesto por Facebook Ireland privaría de efecto útil a las disposiciones del RGPD relativas a las transferencias hacia terceros países, ya que nunca se puede excluir que los datos transferidos en el marco de una actividad comercial sean tratados por razones de seguridad nacional después de la transferencia.

108. La interpretación que propongo se ve confirmada por el tenor literal del artículo 45, apartado 2, letra a), del RGPD. Esta disposición indica que, cuando adopte una decisión de adecuación, la Comisión tendrá en cuenta, en particular, la legislación del tercer país al que se refiere *en materia de seguridad nacional*. De ello puede deducirse que la posibilidad de que los datos sufran, por parte de las autoridades del país tercero de destino, un tratamiento que tenga por objeto la protección de la seguridad nacional no hace que el Derecho de la Unión resulte inaplicable al tratamiento que constituye la transferencia de datos a ese país tercero.

109. El razonamiento y las conclusiones adoptados por el Tribunal de Justicia en la sentencia Schrems se basan igualmente en esta premisa. En particular, en dicha sentencia el Tribunal de Justicia examinó la validez de la Decisión de puerto seguro, en la medida en que esta tenía por objeto las transferencias de datos personales hacia los Estados Unidos, donde podían ser recogidas y tratadas por razones de protección de la seguridad nacional, teniendo en cuenta el artículo 25, apartado 6, de la Directiva 95/46, interpretada a la luz de la Carta. [41]

110. Habida cuenta de estas consideraciones, estimo que el Derecho de la Unión se aplica a una transferencia de datos personales desde un Estado miembro a un tercer país cuando dicha transferencia se enmarque en una actividad comercial, con independencia de que los datos transferidos puedan ser sometidos por las autoridades públicas de dicho tercer país a tratamientos dirigidos a proteger su seguridad nacional.

39 Con arreglo al artículo 3, apartado 1, del RGPD, este Reglamento se aplica a todo tratamiento efectuado en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. La cuestión de la aplicabilidad del Derecho de la Unión a los tratamientos por parte de los servicios de inteligencia de un tercer país fuera de la Unión debe distinguirse de la de la pertinencia de las normas y prácticas que rodean a estos tratamientos en el tercer país en cuestión con el fin de determinar si en este se garantiza un nivel adecuado de protección. Esta última temática constituye el objeto de la segunda cuestión prejudicial y se abordará en los puntos 201 a 229 de las presentes conclusiones.

40 En mis conclusiones presentadas en el asunto Ministerio Fiscal (C-207/16, EU:C:2018:300), punto 47, destaqué la distinción entre, por una parte, el tratamiento directo de datos personales en el marco de actividades regalianas del Estado, y, por otra parte, el tratamiento comercial seguido de una utilización por parte de las autoridades públicas.

41 De la misma manera, en el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017 (en lo sucesivo, «dictamen 1/15», EU:C:2017:592), el Tribunal de Justicia examinó la conformidad con los artículos 7, 8 y 47 de la Carta de un proyecto de acuerdo internacional entre Canadá y la Unión relativo a datos que, una vez transferidos a Canadá, estaban destinados a ser tratados por las autoridades públicas con fines de protección de la seguridad nacional.

D. Sobre el nivel de protección exigido en el marco de una transferencia basada en cláusulas contractuales tipo (primera parte de la sexta cuestión prejudicial)

111. A tenor de la primera parte de su sexta cuestión prejudicial, el órgano jurisdiccional remitente pretende averiguar cuál es el nivel de protección de los derechos fundamentales de los interesados que debe garantizarse para que se puedan transferir datos personales a un tercer país en virtud de las cláusulas contractuales tipo establecidas en la Decisión 2010/87.

112. El referido órgano jurisdiccional destaca que, en la sentencia Schrems, el Tribunal de Justicia interpretó el artículo 25, apartado 6, de la Directiva 95/46 (cuyo contenido reproduce esencialmente el artículo 45, apartado 3, del RGPD), en la medida en que establecía que la Comisión solo puede adoptar una decisión de adecuación tras haberse asegurado de que el tercer país en cuestión garantiza un nivel de protección adecuado, en el sentido de que supone que esta acredite que dicho país garantiza un nivel de protección de las libertades y los derechos fundamentales *sustancialmente equivalente* al garantizado en la Unión por esta Directiva, interpretada a la luz de la Carta.[42]

113. En este contexto, la primera parte de la sexta cuestión prejudicial solicita al Tribunal de Justicia que determine si la aplicación de «cláusulas contractuales tipo» adoptadas por la Comisión con arreglo al artículo 26, apartado 4, de la Directiva 95/46 —que se corresponden con las «cláusulas tipo de protección» actualmente mencionadas en el artículo 46, apartado 2, letra c), del RGPD— debe permitir alcanzar un nivel de protección correspondiente al mismo estándar de «equivalencia sustancial».

114. A este respecto, el artículo 46, apartado 1, del RGPD dispone que, a falta de una decisión de adecuación, el responsable 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» (el subrayado es mío).[43] A tenor del artículo 46, apartado 2, letra c), del RGPD, estas garantías pueden resultar, en particular, de cláusulas tipo de protección elaboradas por la Comisión.

115. Al igual que el DPC, el Sr. Schrems e Irlanda, considero que las «garantías adecuadas» proporcionadas por el responsable del tratamiento a las que hace referencia el artículo 46, apartado 1, del RGPD deben garantizar que los derechos de las personas cuyos datos se transfieren gocen, como en el marco de una transferencia basada en una decisión de adecuación, de un nivel de protección sustancialmente equivalente al resultante del RGPD, interpretado a la luz de la Carta.

116. Esta conclusión se deduce del objetivo de esta disposición y del instrumento del que forma parte.

117. Los artículos 45 y 46 del RGPD tienen como finalidad garantizar la continuidad del elevado nivel de protección de los datos personales ofrecido por este Reglamento cuando se transfieran fuera de la Unión. En efecto, el artículo 44 del RGPD, titulado «Principio general de las transferencias», abre el capítulo V relativo a las transferencias a terceros países estableciendo que todas las disposiciones de este capítulo se aplicarán a fin de asegurar que el nivel de protección garantizado por el RGPD no se vea menoscabado en caso de transferencia a un tercer Estado.[44] Esta norma pretende evitar que los estándares de protección derivados del Derecho de la Unión sean eludidos mediante la transferencia

42 Sentencia Schrems, apartado 73. El Tribunal de Justicia confirmó esta conclusión en el dictamen 1/15, apartado 134.

43 El artículo 26, apartado 2, de la Directiva 95/46 establecía que un Estado miembro puede autorizar tal transferencia «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» (el subrayado es mío). En mi opinión, los conceptos de «garantías suficientes» y de «garantías adecuadas», mencionados en esta disposición y en el artículo 46, apartado 1, del RGPD, respectivamente, tienen el mismo contenido.

44 A este respecto, el considerando 6 del RGPD indica que se debe garantizar un «elevado nivel» de protección de los datos tanto dentro de la Unión como en caso de transferencia fuera de esta. Véase también el considerando 101 del RGPD.

de los datos personales a un tercer país con el fin de tratarlos en este.[45] A la vista de este objetivo, es irrelevante que la transferencia se base en una decisión de adecuación o en garantías ofrecidas por el responsable del tratamiento, en particular mediante cláusulas contractuales. Los requisitos de protección de los derechos fundamentales garantizados por la Carta no establecen una distinción en función del fundamento jurídico en el que se base una transferencia determinada.[46]

118. En cambio, la manera en que se protege la continuidad del elevado nivel de protección difiere en función de la base jurídica de la transferencia.

119. Por un lado, una decisión de adecuación tiene por objeto constatar que el propio tercer país en cuestión garantiza un nivel de protección sustancialmente equivalente al que debe alcanzarse en Derecho de la Unión. La adopción de una decisión de adecuación supone que la Comisión evalúe previamente, para un tercer país determinado, el nivel de protección garantizado por el Derecho y las prácticas de dicho tercer país habida cuenta de los factores enunciados en el artículo 45, apartado 3, del RGPD. A partir de entonces se pueden transferir datos personales a dicho tercer país sin que el responsable del tratamiento deba obtener una autorización específica.

120. Por otro lado, como se expondrá con más detalle en la siguiente sección, las garantías adecuadas ofrecidas por el responsable del tratamiento pretenden garantizar un elevado nivel de protección en el supuesto de que las garantías disponibles en el tercer país de destino sean insuficientes. Así pues, si bien el artículo 46, apartado 1, del RGPD permite que se transfieran datos personales a terceros Estados que no garantizan un nivel adecuado de protección, esta disposición solo autoriza dichas transferencias cuando se ofrecen garantías adecuadas por otros medios. A este respecto, las cláusulas contractuales tipo adoptadas por la Comisión constituyen un mecanismo general aplicable a las transferencias con independencia de cuáles sean el tercer país de destino y el nivel de protección que este ofrece.

E. Sobre la validez de la Decisión 2010/87 en relación con los artículos 7, 8 y 47 de la Carta (cuestiones prejudiciales séptima, octava y undécima)

121. Mediante su séptima cuestión prejudicial, el órgano jurisdiccional remitente pregunta, en esencia, si la Decisión 2010/87 es inválida debido al hecho de que no vincula a las autoridades de los terceros Estados hacia los que se transfieren los datos en virtud de las cláusulas contractuales tipo previstas en el anexo de dicha Decisión y, en particular, de que no les impide exigir al importador que ponga a su disposición tales datos. Por lo tanto, esta cuestión prejudicial pone en entredicho la posibilidad misma de garantizar un nivel adecuado de protección de tales datos mediante mecanismos de naturaleza exclusivamente contractual. La undécima cuestión prejudicial se refiere de forma más global a la validez de la Decisión 2010/87 en relación con los artículos 7, 8 y 47 de la Carta.

122. La octava cuestión prejudicial solicita al Tribunal de Justicia que determine si una autoridad de control debe utilizar las facultades que le confiere el artículo 58, apartado 2, letras f) y j), del RGPD para suspender una transferencia a un tercer país basada en las cláusulas contractuales tipo previstas en la Decisión 2010/87 cuando considere que el importador de los datos está sujeto en dicho país a obligaciones que le impiden cumplir dichas cláusulas y que tienen por efecto que no se garantice una protección adecuada de los datos transferidos. En la medida en que, en mi opinión, la respuesta a esta cuestión afecta a la validez de la Decisión 2010/87,[47] la examinaré de forma conjunta con las cuestiones prejudiciales séptima y undécima.

45 Véanse la sentencia Schrems, apartado 73, y el dictamen 1/15, apartado 214.

46 Esto es cierto sin perjuicio de la posibilidad de transferir datos personales, aun a falta de garantías adecuadas, sobre la base de los motivos de excepción previstos en el artículo 49, apartado 1, del RGPD.

47 Véase el punto 128 de las presentes conclusiones.

123. El tenor literal del artículo 46, apartado 1, del RGPD, en la medida en que establece que, «*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 […] *si hubiera ofrecido* garantías adecuadas […]» (el subrayado es mío), pone de manifiesto la lógica en la que se basan los mecanismos contractuales como el previsto en la Decisión 2010/87. Como señalan los considerandos 108 y 114 del RGPD, estos mecanismos tienen por objeto permitir las transferencias a terceros países respecto de los cuales la Comisión no haya adoptado una decisión de adecuación, debiendo *compensarse* entonces las posibles insuficiencias de la protección garantizada en el ordenamiento jurídico de dicho tercer país mediante las garantías que el exportador y el importador de los datos se comprometen contractualmente a respetar.

124. Dado que la razón de ser de las garantías contractuales consiste precisamente en subsanar las posibles deficiencias de la protección ofrecida por los terceros países de destino, con independencia de cuáles sean, la validez de una decisión mediante la cual la Comisión declara que determinadas cláusulas tipo solucionan adecuadamente dichas carencias no puede depender del nivel de protección garantizado en cada uno de los terceros países concretos a los que se puedan transferir los datos. La validez de dicha decisión depende únicamente de la solidez de las garantías que establecen estas cláusulas para compensar la posible insuficiencia de la protección en el tercer país de destino. La efectividad de estas garantías debe valorarse teniendo también en cuenta las salvaguardias que constituyen las facultades de las autoridades de control en virtud del artículo 58, apartado 2, del RGPD.

125. A este respecto, tal como han señalado, en esencia, el DPC, el Sr. Schrems, la BSA, Irlanda, los Gobiernos austriaco, francés, polaco y portugués, así como la Comisión, las garantías que contienen las cláusulas contractuales tipo pueden verse reducidas, o incluso anuladas, cuando el Derecho del tercer país de destino imponga al importador obligaciones contrarias a lo que exigen dichas cláusulas. Así pues, en función de las circunstancias concretas de la transferencia,[48] el contexto jurídico que rige en el tercer país de destino puede imposibilitar el cumplimiento de las obligaciones previstas en dichas cláusulas.

126. En estas circunstancias, tal como han señalado el Sr. Schrems y la Comisión, el mecanismo contractual previsto en el artículo 46, apartado 2, letra c), del RGPD se basa en la responsabilización del exportador, así como, con carácter subsidiario, de las autoridades de control. El responsable del tratamiento o, en su defecto, la autoridad de control debe examinar *caso por caso*, para cada transferencia específica, si el Derecho del tercer país de destino impide la ejecución de las cláusulas tipo y, por consiguiente, una protección adecuada de los datos transferidos, de modo que se deban prohibir o suspender las transferencias.

127. Teniendo en cuenta estas observaciones, considero que el hecho de que la Decisión 2010/87 y las cláusulas contractuales tipo que establece no vinculen a las autoridades del tercer país de destino no invalida, por sí solo, dicha Decisión. La conformidad de la Decisión 2010/87 con los artículos 7, 8 y 47 de la Carta depende, en mi opinión, de si existen mecanismos suficientemente sólidos que permitan garantizar que se suspendan o prohíban las transferencias basadas en las cláusulas contractuales tipo en caso de violación de dichas cláusulas o de imposibilidad de cumplirlas.

128. A estos efectos, el artículo 46, apartado 1, del RGPD establece que solo podrán tener lugar las transferencias basadas en garantías adecuadas «a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas». Se deberá comprobar si las garantías previstas en las cláusulas que figuran en el anexo de la Decisión 2010/87, complementadas por las facultades de las

48 Imaginemos, por ejemplo, que un tercer país imponga a los proveedores de servicios de telecomunicaciones la obligación de conceder a las autoridades públicas un acceso a los datos transferidos sin ninguna limitación ni garantía. Si bien tales proveedores serían incapaces de respetar las cláusulas contractuales tipo, no por ello se verían imposibilitadas para cumplirlas las empresas que no estuvieran sujetas a dicha obligación.

autoridades de control, permiten garantizar el cumplimiento de este requisito. A mi entender, no será así a menos que exista una *obligación* —impuesta a los responsables del tratamiento (sección 1) y, en caso de inacción de estos últimos, a las autoridades de control (sección 2)— de suspender o prohibir las transferencias cuando, debido a un conflicto entre las obligaciones resultantes de las cláusulas tipo y las impuestas por el Derecho del tercer país de destino, no se puedan cumplir dichas cláusulas.

1. Sobre las obligaciones de los responsables del tratamiento

129. En primer lugar, las cláusulas contractuales tipo incluidas en el anexo de la Decisión 2010/87 exigen que en caso de conflicto entre las obligaciones que establecen y las disposiciones resultantes del Derecho del tercer país de destino, no se invoquen estas cláusulas en apoyo de una transferencia a dicho tercer país o que, si ya se ha iniciado la transferencia sobre la base de las referidas cláusulas, se informe al exportador de este conflicto y pueda suspender esa transferencia.

130. Así pues, con arreglo a la cláusula 5, letra a), el importador se compromete a tratar los datos personales transferidos solo en nombre del exportador, de conformidad con sus instrucciones y las cláusulas contractuales tipo. En caso de que el importador no pueda cumplir estas cláusulas, informará de ello sin demora al exportador, en cuyo caso este estará facultado para suspender la transferencia o resolver el contrato. [49]

131. La nota a pie de página 5 correspondiente a la cláusula 5 precisa que no se produce una violación de las cláusulas tipo cuando el importador cumpla las obligaciones impuestas por la legislación nacional que le es aplicable en el tercer país, a condición de que estas obligaciones no vayan más allá de las restricciones necesarias en una sociedad democrática para proteger uno de los intereses recogidos en el artículo 13, apartado 1, de la Directiva 95/46 (cuyo contenido se reproduce en lo fundamental en el artículo 23, apartado 1, del RGPD), entre los que figuran la seguridad pública y la seguridad del Estado. Por el contrario, el incumplimiento de estas cláusulas con el fin de acatar una obligación contradictoria basada en el Derecho del tercer país de destino que exceda de lo que sea proporcionado para la salvaguarda de un interés legítimo reconocido por la Unión se considera una violación de dichas cláusulas.

132. En mi opinión, tal como han alegado el Sr. Schrems y la Comisión, la cláusula 5, letra a), no puede interpretarse en el sentido de que implica que la suspensión de la transferencia o la resolución del contrato es únicamente opcional cuando el importador no está en condiciones de respetar las cláusulas tipo. Si bien esta cláusula solo alude a un derecho en este sentido en beneficio del exportador, este tenor literal debe entenderse por referencia al marco contractual en el que se inscribe. El hecho de que el exportador tenga el derecho, *en sus relaciones bilaterales con el importador*, de suspender la transferencia o de resolver el contrato cuando este último se encuentre incapacitado para cumplir las cláusulas tipo no afecta a la obligación que recae sobre el exportador de actuar de este modo *en relación con los requisitos de protección de los derechos de los interesados*

49 Debo señalar, asimismo, que la cláusula 5, letra d), inciso i), exime al importador de su obligación de informar al exportador de una solicitud jurídicamente vinculante de divulgación presentada por una autoridad encargada de la aplicación de la ley del tercer país cuando el Derecho de dicho tercer país se oponga a tal información. En tal supuesto, el exportador no tendrá la posibilidad de suspender la transferencia si dicha divulgación, de la que no tendrá conocimiento, viola las cláusulas tipo. Sin embargo, el importador sigue estando obligado, con arreglo a la cláusula 5, letra a), a informar, en su caso, al exportador del hecho de que considera que la legislación de ese tercer país le impide cumplir sus obligaciones en virtud de las cláusulas contractuales acordadas.

derivados del RGPD. Cualquier otra interpretación implicaría la invalidez de la Decisión 2010/87 en la medida en que las cláusulas contractuales tipo que establece no permitirían dar unas «garantías adecuadas» a la transferencia, como exige el artículo 46, apartado 1, del RGPD, en relación con las disposiciones de la Carta. [50]

133. Por añadidura, con arreglo a la cláusula 5, letra b), el importador certificará que no tiene motivos para creer que la legislación que le es de aplicación le impide cumplir las instrucciones del exportador y sus obligaciones a tenor del contrato. En caso de modificación de esta legislación que pueda tener un importante efecto negativo sobre las garantías y obligaciones estipuladas en las cláusulas tipo, notificará dicha modificación al exportador en cuanto tenga conocimiento de esta, en cuyo caso este último estará facultado para suspender la transferencia de datos o resolver el contrato. De conformidad con la cláusula 4, letra g), el exportador deberá enviar la notificación recibida del importador a la autoridad de control competente en caso de que decida proseguir la transferencia.

134. Llegados a este punto, creo necesario realizar algunas aclaraciones relativas al contenido del examen que deben efectuar las partes del contrato con el fin de determinar, a la vista de la nota a pie de página correspondiente a la cláusula 5, si las obligaciones que impone el Derecho del tercer Estado al importador suponen una violación de las cláusulas tipo y, por tanto, impiden que la transferencia goce de unas garantías adecuadas. Esta problemática se ha planteado, en esencia, en el marco de la segunda parte de la sexta cuestión prejudicial.

135. A mi entender, dicho examen implica tomar en consideración el conjunto de las circunstancias que caracterizan cada transferencia, entre las cuales pueden encontrarse la naturaleza de los datos y su posible carácter sensible, los mecanismos aplicados por el exportador o el importador para garantizar su seguridad, [51] la naturaleza y la finalidad de los tratamientos por parte de las autoridades públicas del tercer país a los que estarán expuestos los datos, las condiciones de dichos tratamientos, así como las limitaciones y garantías ofrecidas por ese tercer país. Considero que los elementos que caracterizan las actividades de tratamiento por parte de las autoridades públicas y las garantías aplicables en el ordenamiento jurídico de dicho tercer país pueden coincidir con los recogidos en el artículo 45, apartado 2, del RGPD.

136. En segundo lugar, las cláusulas contractuales tipo recogidas en el anexo de la Decisión 2010/87 establecen, en beneficio de los interesados, derechos exigibles, así como vías de recurso contra el exportador y, subsidiariamente, contra el importador.

137. Así pues, la cláusula 3, titulada «Cláusula de tercero beneficiario», establece, en su apartado 1, un derecho de recurso del interesado contra el exportador en caso de violación, entre otras, de las letras a) o b) de la cláusula 5. Con arreglo a la cláusula 3, apartado 2, cuando el exportador haya desaparecido *de facto* o haya cesado de existir jurídicamente, el interesado podrá exigir al importador el cumplimiento de esta cláusula.

138. La cláusula 6, apartado 1, concede a los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones mencionadas en la cláusula 3 el derecho a percibir una indemnización del exportador por el daño sufrido. En virtud de la cláusula 7, apartado 1, el importador acuerda que si el interesado invoca respecto de sí mismo derechos de tercero beneficiario

50 De la jurisprudencia se desprende que las disposiciones de un acto de ejecución deben interpretarse de conformidad con lo dispuesto en el acto de base mediante el cual el legislador autorizó su adopción [véanse, en este sentido, en particular, las sentencias de 26 de julio de 2017, República Checa/Comisión (C-696/15 P, EU:C:2017:595), apartado 51; de 17 de mayo de 2018, Evonik Degussa (C-229/17, EU:C:2018:323), apartado 29, y de 20 de junio de 2019, ExxonMobil Production Deutschland (C-682/17, EU:C:2019:518), apartado 112]. Asimismo, todo acto de la Unión debe interpretarse, en la medida de lo posible, de un modo que no cuestione su validez y de conformidad con el conjunto del Derecho primario y, en particular, con las disposiciones de la Carta [véase, entre otras, la sentencia de 14 de mayo de 2019, M y otros (Revocación del estatuto de refugiado) (C-391/16, C-77/17 y C-78/17, EU:C:2019:403), apartado 77 y jurisprudencia citada].

51 A este respecto, el considerando 109 del RGPD invita al exportador y al importador a añadir garantías adicionales a las cláusulas tipo de protección, en particular por vía contractual.

o reclama una indemnización por daños y perjuicios, aceptará la decisión de dicho interesado de someter el conflicto a mediación por parte de una persona independiente o, si procede, por parte de la autoridad de control, o de someter el conflicto a los tribunales del Estado miembro de establecimiento del exportador.

139. Además de las vías de recurso de que disponen en virtud de las cláusulas contractuales tipo recogidas en el anexo de la Decisión 2010/87, cuando consideren que se han violado estas cláusulas, los interesados podrán solicitar a las autoridades de control que adopten medidas correctoras con arreglo al artículo 58, apartado 2, del RGPD, al que remite el artículo 4 de la Decisión 2010/87. [52]

2. Sobre las obligaciones de las autoridades de control

140. Las siguientes razones me llevan a pensar, al igual que el Sr. Schrems, Irlanda, los Gobiernos alemán, austriaco, belga, neerlandés y portugués, así como el CEPD, que el artículo 58, apartado 2, del RGPD obliga a las autoridades de control a adoptar las medidas adecuadas para subsanar esta ilegalidad, si fuera necesario ordenando la suspensión de la transferencia, cuando consideren, tras un examen diligente, que los datos transferidos a un tercer país no disfrutan de una protección apropiada debido al incumplimiento de las cláusulas contractuales acordadas.

141. En primer lugar, debo señalar que, contrariamente a lo que afirma el DPC, ninguna disposición de la Decisión 2010/87 limita a los casos excepcionales el ejercicio de las facultades para «imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición», y para «ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país» de las que disponen las autoridades de control en virtud del artículo 58, apartado 2, letras f) y j), del RGPD.

142. Es cierto que la versión inicial del artículo 4 de la Decisión 2010/87, en su apartado 1, restringía el ejercicio por parte de las autoridades de control de sus facultades para suspender o prohibir los flujos transfronterizos de datos a ciertos supuestos en los que se hubiese demostrado que una transferencia basada en cláusulas contractuales tipo podía tener efectos negativos considerables en las garantías dirigidas a proteger al interesado. Sin embargo, el artículo 4 de esta Decisión, en su versión modificada por la Comisión en 2016 con el fin de ajustarse a la sentencia Schrems, [53] actualmente se limita a hacer referencia a estas facultades, sin limitarlas en modo alguno. En todo caso, una decisión de ejecución de la Comisión, como la Decisión 2010/87, no puede restringir válidamente las facultades conferidas a las autoridades de control en virtud del propio RGPD. [54]

143. Esta conclusión no se ve desvirtuada por el considerando 11 de la Decisión 2010/87, que señala que las autoridades de control solo pueden ejercer las facultades de suspensión y de prohibición de las transferencias en «casos excepcionales». Este considerando, que ya estaba presente en la versión inicial de esta Decisión, se refería al antiguo artículo 4, apartado 1, de dicha Decisión, que limitaba las facultades de las autoridades de control. Tras la revisión de la Decisión 2010/87 mediante la Decisión 2016/2297, la Comisión no retiró o modificó el mencionado considerando para adaptar su contenido a lo establecido en el nuevo artículo 4. No obstante, el considerando 5 de la Decisión 2016/2297 reafirmó la facultad de las autoridades de control para suspender o prohibir toda transferencia que

52 Si bien el artículo 4, apartado 1, de la Decisión 2010/87 hace referencia al artículo 28, apartado 3, de la Directiva 95/46, debo recordar que, en virtud del artículo 94, apartado 2, del RGPD, las referencias a esta Directiva deberán entenderse hechas a las disposiciones correspondientes del RGPD.

53 Véanse los considerandos 6 y 7 de la Decisión 2016/2297. En los apartados 101 a 104 de la sentencia Schrems, el Tribunal de Justicia había declarado la invalidez de una disposición de la Decisión de puerto seguro que limitaba a los «casos excepcionales» las facultades conferidas a las autoridades de control en el artículo 28 de la Directiva 95/46, debido a que la Comisión no era competente para restringir estas facultades.

54 Véase la sentencia Schrems, apartado 103.

consideren contraria al Derecho de la Unión, en particular debido al incumplimiento por parte del importador de las cláusulas contractuales tipo. El considerando 11 de la Decisión 2010/87, en la medida en que actualmente contradice tanto el tenor como el objetivo de una disposición jurídicamente vinculante, debe considerarse obsoleto. [55]

144. En segundo lugar, contrariamente a lo que también afirma el DPC, el ejercicio de las facultades de suspensión y de prohibición previstas en el artículo 58, apartado 2, letras f) y j), del RGPD tampoco constituye una mera potestad que se deje a la discreción de las autoridades de control. A mi entender, esta conclusión se desprende de una interpretación del artículo 58, apartado 2, del RGPD realizada a la luz de otras disposiciones de este Reglamento y de la Carta, así como de la lógica y los objetivos de la Decisión 2010/87.

145. En particular, el artículo 58, apartado 2, del RGPD debe interpretarse en relación con el artículo 8, apartado 3, de la Carta y del artículo 16 TFUE, apartado 2. Con arreglo a estas disposiciones, el cumplimiento de los requisitos que implica el derecho fundamental a la protección de los datos personales está sujeto al control de autoridades independientes. Esta misión de vigilancia del cumplimiento de los requisitos relativos a la protección de los datos personales, que también se menciona en el artículo 57, apartado 1, letra a), del RGPD, supone que las autoridades de control están obligadas a actuar de manera que se garantice la correcta aplicación de este Reglamento.

146. Así pues, una autoridad de control debe examinar con toda la diligencia exigida la reclamación presentada por una persona cuyos datos hayan sido presuntamente transferidos a un tercer Estado incumpliendo las cláusulas contractuales tipo aplicables a la transferencia. [56] A tal efecto, el artículo 58, apartado 1, del RGPD otorga a las autoridades de control importantes facultades de investigación. [57]

147. La autoridad de control competente también está obligada a actuar de manera adecuada ante las posibles violaciones de los derechos del interesado que haya constatado a raíz de su investigación. A este respecto, cada autoridad de control dispone, en virtud del artículo 58, apartado 2, del RGPD, de una amplia gama de medios —las distintas facultades para adoptar medidas correctoras enumeradas en cada disposición— para llevar a cabo la función que se le ha encomendado. [58]

148. A pesar de que la elección del medio más eficaz queda a la discreción de la autoridad de control competente, teniendo en cuenta todas las circunstancias de la transferencia en cuestión, esta debe cumplir la misión de vigilancia que se le ha encomendado de forma plena. En su caso, esta autoridad debe suspender la transferencia si concluye que no se respetan las cláusulas contractuales tipo y que no se puede garantizar la adecuada protección de los datos transferidos por otros medios, si el propio exportador no ha puesto fin a la transferencia por sí mismo.

55 En todo caso, la exposición de motivos de un acto de la Unión no tiene valor jurídico vinculante y no puede ser invocada para establecer excepciones a las propias disposiciones de ese acto. Véanse las sentencias de 19 de noviembre de 1998, Nilsson y otros (C-162/97, EU:C:1998:554), apartado 54; de 12 de mayo de 2005, Meta Fackler (C-444/03, EU:C:2005:288), apartado 25, y de 10 de enero de 2006, IATA y ELFAA (C-344/04, EU:C:2006:10), apartado 76.

56 Véase, por analogía, la sentencia Schrems, apartado 63.

57 Debo añadir que, en virtud de la cláusula 8, apartado 2, que figura en el anexo de la Decisión 2010/87, las partes contratantes acuerdan conceder a la autoridad de control la facultad de auditar al importador en las mismas condiciones en que lo haría respecto del exportador conforme a la legislación aplicable.

58 Véase, en este sentido, la sentencia Schrems, apartado 43.

149. Esta interpretación se ve corroborada por el artículo 58, apartado 4, del RGPD, que dispone que el ejercicio de las facultades conferidas a las autoridades de control con arreglo a este artículo está sujeto a las garantías adecuadas, que incluyen el derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta. Asimismo, el artículo 78, apartados 1 y 2, del RGPD reconoce el derecho de toda persona a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna o cuando dicha autoridad no dé curso a su reclamación. [59]

150. Estas disposiciones implican, como alegan, en esencia, el Sr. Schrems, la BSA, Irlanda, los Gobiernos polaco y del Reino Unido, así como la Comisión, que una decisión mediante la cual una autoridad de control se abstenga de prohibir o de suspender una transferencia a un tercer país, a petición de una persona que invoque el riesgo de que los datos que le conciernan sean tratados en dicho país tercero de forma que vulnere sus derechos fundamentales, puede ser objeto de un recurso judicial. Pues bien, el reconocimiento de un derecho a interponer un recurso jurisdiccional supone la existencia de una competencia reglada, y no puramente discrecional, de las autoridades de control. Además, el Sr. Schrems y la Comisión destacaron acertadamente que el ejercicio de un control jurisdiccional efectivo implica que la autoridad autora del acto impugnado motive este de forma adecuada. [60] En mi opinión, esta obligación de motivación se extiende a la decisión por parte de las autoridades de control de ejercer una u otra de las facultades que les confiere el artículo 58, apartado 2, del RGPD.

151. Sin embargo, también procede responder a los argumentos mediante los cuales el DPC alega que, si bien es cierto que las autoridades de control están obligadas a suspender o a prohibir una transferencia cuando la protección de los derechos del interesado lo exija, esto no garantiza la validez de la Decisión 2010/87.

152. En primer término, el DPC considera que la existencia de tal obligación no corrige los problemas sistémicos relativos a la falta de garantías adecuadas en un tercer país como los Estados Unidos. En efecto, las facultades de las autoridades de control solo pueden ejercerse caso por caso, aun cuando, a su juicio, las lagunas que caracterizan el Derecho estadounidense tienen una naturaleza general y estructural. Entiende que de ello se deriva un riesgo de que se adopten decisiones contradictorias relativas a transferencias comparables por parte de diferentes autoridades de control.

153. A este respecto, no puedo ignorar las dificultades prácticas relacionadas con la decisión legislativa de imponer a las autoridades de control la responsabilidad de velar por el respeto de los derechos fundamentales de los interesados en el marco de transferencias específicas o de flujos hacia un destinatario determinado. No obstante, no me parece que estas dificultades supongan la invalidez de la Decisión 2010/87.

154. En efecto, creo que el Derecho de la Unión no exige que se aporte una solución global y preventiva para el conjunto de las transferencias hacia un tercer país determinado que puedan implicar los mismos riesgos de vulneración de los derechos fundamentales.

155. Asimismo, el riesgo de fragmentación de los enfoques seguidos por las diferentes autoridades de control es inherente a la arquitectura de vigilancia descentralizada elegida por el legislador. [61] A mayor abundamiento, tal como ha señalado el Gobierno alemán, el capítulo VII del RGPD, que lleva por título «Cooperación y coherencia», establece mecanismos destinados a evitar este riesgo. El artículo 60 de este Reglamento prevé, en caso de tratamiento transfronterizo de datos, un procedimiento de

59 A tenor del considerando 141 del RGPD, toda persona debe tener derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si la autoridad de control «no [actúa] cuando sea necesario para proteger los derechos de [esta persona]». Véanse también los considerandos 129 y 143 del RGPD.

60 Véanse, en particular, las sentencias de 28 de julio de 2011, Samba Diouf (C-69/10, EU:C:2011:524), apartado 57, y de 17 de noviembre de 2011, Gaydarov (C-430/10, EU:C:2011:749), apartado 41.

61 Véase, a este respecto, la sentencia de 5 de junio de 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388), apartados 69 a 73.

cooperación entre las autoridades de control interesadas y la autoridad de control del establecimiento del responsable del tratamiento, denominada «autoridad de control principal». [62] En caso de opiniones discrepantes, el CEPD debe resolver el conflicto. [63] Este último también es competente para emitir dictámenes, a petición de una autoridad de control, sobre cualquier cuestión cuyo interés se extienda a varios Estados miembros. [64]

156. En segundo término, el DPC alega la invalidez de la Decisión 2010/87 en virtud del artículo 47 de la Carta basándose en que las autoridades de control solo pueden proteger los derechos de los interesados de cara al futuro, sin ofrecer una solución a aquellos cuyos datos ya se han transferido. En particular, el DPC señala que el artículo 58, apartado 2, del RGPD no prevé un derecho de acceso, de rectificación y de supresión de los datos recogidos por las autoridades públicas del tercer país ni la posibilidad de una indemnización por los daños sufridos por los interesados.

157. En cuanto a la supuesta falta de un derecho de acceso, de rectificación y de supresión de los datos recogidos, resulta obligado reconocer que, cuando no existe ningún recurso efectivo en el tercer país de destino, las vías de recurso previstas dentro de la Unión contra el responsable del tratamiento no permiten obtener de las autoridades públicas de ese tercer país el acceso a dichos datos ni tampoco su rectificación o su supresión.

158. En mi opinión, no obstante, esta objeción no justifica la incompatibilidad de la Decisión 2010/87 con el artículo 47 de la Carta. En efecto, la validez de esta Decisión no depende del nivel de protección existente en cada tercer país al que se podrían transferir datos sobre la base de las cláusulas contractuales tipo que recoge. Si el Derecho del tercer Estado de destino impide al importador cumplir estas cláusulas al exigir que conceda a las autoridades públicas un acceso a los datos que no venga acompañado de posibilidades de recurso adecuadas, en caso de que el exportador no haya suspendido la transferencia en virtud de la cláusula 5, letras a) o b), que figura en el anexo de la Decisión 2010/87, corresponde a las autoridades de control adoptar medidas correctoras.

159. Además, tal como ha señalado el Sr. Schrems, las personas cuyos derechos han sido violados disfrutan actualmente, con arreglo al artículo 82 del RGPD, de un derecho a una indemnización por el perjuicio material o moral ocasionado por la infracción de dicho Reglamento por parte del responsable del tratamiento o del encargado del tratamiento. [65]

160. Según se desprende del conjunto de estas consideraciones, mi análisis no ha revelado ningún elemento que pueda afectar a la validez de la Decisión 2010/87 en relación con los artículos 7, 8 y 47 de la Carta.

F. Sobre la falta de necesidad de responder a las demás cuestiones prejudiciales y de examinar la validez de la Decisión sobre el «Escudo de la privacidad»

161. En la presente sección, expondré las razones, principalmente relacionadas con la limitación del objeto del litigio principal a la validez de la Decisión 2010/87, por las que considero que no procede responder a las cuestiones prejudiciales segunda a quinta, así como a las cuestiones prejudiciales novena y décima, ni pronunciarse sobre la validez de la Decisión sobre el «Escudo de la privacidad».

62 Véase el artículo 56, apartado 1, del RGPD. Con arreglo al artículo 61 de este Reglamento, las autoridades de control deben prestarse asistencia mutua. El artículo 62 de dicho Reglamento las autoriza a realizar operaciones conjuntas.

63 Véase el artículo 65 del RGPD.

64 Véase el artículo 64, apartado 2, del RGPD.

65 El artículo 83, apartado 5, letra c), del RGPD también prevé multas para el responsable del tratamiento en caso de infracción de los artículos 44 a 49 de este Reglamento.

162. La segunda cuestión prejudicial tiene por objeto la identificación de los estándares de protección que debe respetar un tercer país para que se puedan transferir datos de forma lícita a dicho país sobre la base de cláusulas contractuales tipo cuando tales datos, tras su transferencia, puedan ser tratados con fines de seguridad nacional por las autoridades de ese tercer país. La tercera cuestión prejudicial planteada al Tribunal de Justicia se refiere a la determinación de los elementos que caracterizan el régimen de protección aplicable en el tercer Estado de destino que deben tenerse en cuenta para comprobar si cumple dichos estándares.

163. Mediante sus cuestiones prejudiciales cuarta, quinta y décima, el órgano jurisdiccional remitente trata esencialmente de dilucidar si, habida cuenta de los hechos que ha comprobado en relación con el Derecho estadounidense, dicho Derecho establece garantías adecuadas contra las injerencias por parte de las autoridades de inteligencia estadounidenses en el ejercicio de los derechos fundamentales al respeto a la vida privada, a la protección de los datos personales y a la tutela judicial efectiva.

164. La novena cuestión prejudicial versa sobre la importancia que tiene, en el marco del examen mediante el cual una autoridad de control verifica si una transferencia hacia los Estados Unidos basada en las cláusulas contractuales tipo recogidas en la Decisión 2010/87 presenta las garantías adecuadas, el hecho de que la Comisión, en la Decisión sobre el «Escudo de la privacidad», haya declarado que los Estados Unidos ofrecen un nivel de protección adecuado de los derechos fundamentales de los interesados contra tales injerencias.

165. El órgano jurisdiccional remitente no ha planteado de forma explícita la cuestión de la validez de la Decisión sobre el «Escudo de la privacidad» —aunque, como se explica más adelante,[66] las cuestiones prejudiciales cuarta, quinta y décima cuestionan indirectamente la procedencia de la declaración de adecuación que realizó la Comisión en dicha Decisión—.

166. A mi juicio, a la vista de los elementos que se desprenden del análisis precedente, las aclaraciones que aporte el Tribunal de Justicia sobre estas cuestiones prejudiciales no pueden afectar a su conclusión relativa a la validez *in abstracto* de la Decisión 2010/87 ni, por tanto, influir en la resolución del litigio principal (sección 1). Asimismo, aunque en una fase posterior las respuestas del Tribunal de Justicia a dichas cuestiones podrían resultar útiles al DPC para determinar, en el marco del procedimiento subyacente a este litigio, si las transferencias en cuestión deben suspenderse, *in concreto*, debido a la supuesta falta de garantías adecuadas, en mi opinión sería prematuro resolverlas en el marco del presente asunto (sección 2).

1. Sobre la falta de necesidad de las respuestas del Tribunal de Justicia en relación con el objeto del litigio principal

167. Debo recordar que el litigio principal resulta del ejercicio por parte del DPC de la vía de acción descrita en el apartado 65 de la sentencia Schrems, según el cual cada Estado miembro debe permitir a una autoridad de control, cuando lo estime necesario para tramitar una reclamación de la que conoce, solicitar a un órgano jurisdiccional nacional que remita al Tribunal de Justicia una cuestión prejudicial relativa a la validez de una decisión de adecuación —o, por analogía, de una decisión que establezca cláusulas contractuales tipo—.

66 Véase el punto 175 de las presentes conclusiones.

168. A este respecto, la High Court (Tribunal Superior) señaló que las únicas opciones de que disponía, tras haberle sometido el asunto el DPC, eran plantear la petición de decisión prejudicial sobre la validez de la Decisión 2010/87 solicitada por el DPC en caso de que compartiera sus dudas acerca de la validez de esta Decisión, o bien negarse a acceder a esta solicitud en el caso contrario. El referido órgano jurisdiccional considera que, si hubiera optado por esta segunda vía, debería haber desestimado el recurso dado que la demanda del DPC no tenía ningún otro objeto. [67]

169. En este mismo sentido, la Supreme Court (Tribunal Supremo), ante la que Facebook Ireland interpuso un recurso contra la resolución de remisión, describió el litigio principal como un proceso declarativo mediante el cual el DPC solicitaba al órgano jurisdiccional remitente que planteara al Tribunal de Justicia una cuestión prejudicial sobre la validez de la Decisión 2010/87. Según el órgano jurisdiccional supremo irlandés, la única cuestión sustancial planteada ante el órgano jurisdiccional remitente y ante el Tribunal de Justicia se refiere, por tanto, a la validez de esta Decisión. [68]

170. Habida cuenta del objeto del litigio principal, delimitado de este modo, el órgano jurisdiccional remitente planteó al Tribunal de Justicia sus diez primeras cuestiones prejudiciales en la medida en que consideraba que su examen forma parte en la valoración de conjunto que debe realizar el Tribunal de Justicia para pronunciarse, en respuesta a la undécima cuestión prejudicial, sobre la validez de la Decisión 2010/87 en relación con los artículos 7, 8 y 47 de la Carta. Esta cuestión representa, a tenor de la resolución de remisión, la culminación lógica de las cuestiones prejudiciales que la preceden.

171. Desde esta perspectiva, me parece que la premisa según la cual la validez de la Decisión 2010/87 depende del nivel de protección de los derechos fundamentales establecido en cada uno de los terceros Estados a los que se pueden transferir datos sobre la base de las cláusulas contractuales tipo que prevé dicha Decisión subyace a las cuestiones prejudiciales segunda a quinta, así como a las cuestiones novena y décima. Pues bien, tal como se desprende de mi análisis de la séptima cuestión prejudicial, [69] en mi opinión esta premisa es errónea. El examen del Derecho del tercer país de destino solo entra en juego cuando la Comisión adopta una decisión de adecuación o cuando el responsable del tratamiento —o, en su defecto, la autoridad de control competente— verifica si, en el marco de una transferencia basada en una serie de garantías adecuadas en el sentido del artículo 46, apartado 1, del RGPD, las obligaciones que impone el Derecho de este tercer país al importador no comprometen la efectividad de la protección que ofrecen dichas garantías.

172. Por consiguiente, las respuestas del Tribunal de Justicia a las cuestiones antes mencionadas no pueden influir en su conclusión sobre la undécima cuestión prejudicial. [70] Asimismo, tampoco procede darles respuesta desde el punto de vista del objeto del litigio principal.

173. Propongo al Tribunal de Justicia que se limite a tratar el presente asunto desde el punto de vista del objeto de este litigio. En mi opinión, el Tribunal de Justicia no debería ir más allá de lo que exige la resolución de dicho litigio al abordar las cuestiones prejudiciales desde el punto de vista del procedimiento subyacente en curso ante el DPC. Como se expondrá a continuación, esta invitación a

67 Sentencia de primera instancia de la High Court (Tribunal Superior) de 3 de octubre de 2017, apartado 337.

68 A tenor de la sentencia de la Supreme Court (Tribunal Supremo) de 31 de mayo de 2019, apartado 2.7, «the sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]». El apartado 2.9 de dicha sentencia sigue diciendo: «Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*» (el subrayado es mío).

69 Véase el punto 124 de las presentes conclusiones.

70 Por esta misma razón, la Supreme Court (Tribunal Supremo), en su sentencia de 31 de mayo de 2019, apartados 8.1 a 8.5, a la vez que se reconocía incompetente para impugnar la decisión del órgano jurisdiccional remitente de plantear al Tribunal de Justicia las cuestiones prejudiciales y para modificar su contenido, expresó dudas sobre la necesidad de algunas de estas cuestiones. En particular, el apartado 8.5 de esta sentencia establece: «The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures […]»

la contención procede, por una parte, del deseo de no cortocircuitar el normal desarrollo del procedimiento que deberá continuar ante el DPC después de que el Tribunal de Justicia se haya pronunciado sobre la validez de la Decisión 2010/87. Por otra parte, en vista de los hechos del presente caso, me parece algo precipitado, incluso desde el punto de vista de la cuestión en juego en este procedimiento, que el Tribunal de Justicia examine las problemáticas planteadas por las cuestiones prejudiciales segunda a quinta, así como por las cuestiones novena y décima.

2. Sobre las razones que militan en contra de un examen por parte del Tribunal de Justicia en relación con el objeto del procedimiento pendiente ante el DPC

174. En su reclamación ante el DPC, el Sr. Schrems solicita a esta autoridad de control que ejerza las facultades de que dispone en virtud del artículo 58, apartado 2, letra f), del RGPD ordenando a Facebook Ireland que suspenda la transferencia a los Estados Unidos, efectuada sobre la base de cláusulas contractuales, de los datos personales que le conciernen. En apoyo de esta solicitud, el Sr. Schrems invoca esencialmente el carácter inadecuado de estas garantías contractuales en relación con las injerencias en el ejercicio de sus derechos fundamentales derivadas de las actividades de los servicios de inteligencia estadounidenses.

175. La argumentación del Sr. Schrems cuestiona la constatación, efectuada por la Comisión en la Decisión sobre el «Escudo de la privacidad», según la cual los Estados Unidos garantizan un nivel de protección adecuado de los datos transferidos en virtud de tal Decisión, habida cuenta de las restricciones impuestas al acceso a estos datos y a su utilización por parte de las autoridades de inteligencia estadounidenses, así como a la protección jurídica ofrecida a los interesados.[71] Las preocupaciones expresadas por el DPC con carácter provisional,[72] al igual que por el órgano jurisdiccional remitente en el marco de sus cuestiones prejudiciales cuarta, quinta y décima, también arrojan dudas sobre la procedencia de esta constatación.

176. Ciertamente, la Decisión sobre el «Escudo de la privacidad» se limita a declarar la adecuación del nivel de protección de los datos personales transferidos, con arreglo a los principios que enuncia, a empresas establecidas en los Estados Unidos que hayan autocertificado su adhesión a dichos principios.[73] Sin embargo, las consideraciones que figuran en esta exceden del contexto de las transferencias cubiertas por dicha Decisión en la medida en que se refieren al Derecho y a las prácticas en vigor en este tercer país en relación con el tratamiento, con fines de protección de la seguridad nacional, de los datos transferidos. Como han observado en esencia Facebook Ireland, el Sr. Schrems, el Gobierno estadounidense y la Comisión, la vigilancia ejercida por las autoridades de inteligencia estadounidenses, del mismo modo que las garantías contra el riesgo de abuso que implica y los mecanismos dirigidos a controlar su cumplimiento, se aplican con independencia de cuál sea, desde el punto de vista del Derecho de la Unión, la base jurídica invocada para fundamentar la transferencia.

71 Véanse los considerandos 64 a 141 de la Decisión sobre el «Escudo de la privacidad». Debo recordar que, tal como se desprende del artículo 1, apartado 2, de esta Decisión, el Escudo de la privacidad de los datos se compone no solo de principios que deben cumplir las empresas que desean transferir datos con arreglo a dicha Decisión, sino también de los compromisos y declaraciones oficiales obtenidos del Gobierno estadounidense y que están recogidos en los documentos adjuntos a esta.

72 El proyecto de decisión del DPC es anterior a la adopción de la Decisión sobre el «Escudo de la privacidad». Tal como precisó el DPC en dicho proyecto, si bien concluyó provisionalmente que las garantías previstas en el Derecho estadounidense no permitían, como mínimo, garantizar la conformidad de las transferencias a este tercer país con el artículo 47 de la Carta, *no examinó ni tuvo en cuenta, en esta fase, los nuevos acuerdos contemplados en el proyecto de acuerdo relativo al «Escudo de la privacidad» dado que este no se había adoptado todavía*. Dicho esto, en el apartado 307 de su sentencia de primera instancia de 3 de octubre de 2017, la High Court (Tribunal Superior) declara: «It is fair to conclude […] that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U.S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U.S.], conflicts with the case made by the DPC to this court».

73 Véase el artículo 1, apartados 1 y 3, así como los considerandos 14 a 16 de la Decisión sobre el «Escudo de la privacidad».

177. Desde esta perspectiva, la cuestión de si las conclusiones alcanzadas a este respecto en la Decisión sobre el «Escudo de la privacidad» vinculan a las autoridades de control cuando estas examinan la legalidad de una transferencia realizada sobre la base de cláusulas contractuales tipo podría resultar pertinente a los efectos de la tramitación de la reclamación del Sr. Schrems por parte del DPC. En caso de respuesta afirmativa a esta cuestión, se plantea la de si esta Decisión es efectivamente válida.

178. Sin embargo, desaconsejo al Tribunal de Justicia que se pronuncie sobre estas cuestiones prejudiciales con el único objetivo de ayudar al DPC a tramitar esta reclamación aunque no proceda responder a estas para permitir al órgano jurisdiccional remitente resolver el litigio principal. Dado que el procedimiento previsto en el artículo 267 TFUE establece un diálogo entre jueces, el Tribunal de Justicia no debe aportar una aclaración con la única finalidad de asistir a una autoridad administrativa en el marco de un procedimiento subyacente a ese litigio.

179. En mi opinión, se impone la reserva, tanto más cuanto no se le ha planteado expresamente la cuestión de la validez de la Decisión sobre el «Escudo de la privacidad» —en vista de que esta Decisión, además, ya constituye el objeto de un recurso de anulación pendiente ante el Tribunal General de la Unión Europea—.[74]

180. Por añadidura, al pronunciarse sobre las problemáticas antes descritas, considero que el Tribunal de Justicia alteraría el curso normal del procedimiento que debe desarrollarse después de que haya dictado su sentencia en el presente asunto. En el marco de este procedimiento, corresponderá al DPC tramitar la reclamación del Sr. Schrems teniendo en cuenta la respuesta que dé el Tribunal de Justicia a la undécima cuestión prejudicial. Si el Tribunal de Justicia declara, como propongo y contrariamente a lo que ha sostenido el DPC ante este, que la Decisión 2010/87 no es inválida en virtud de los artículos 7, 8 y 47 de la Carta, a mi juicio el DPC debería tener la posibilidad de volver a examinar el expediente del procedimiento en curso del que conoce. En el supuesto de que el DPC considere que no está en disposición de resolver la reclamación del Sr. Schrems sin que el Tribunal de Justicia determine previamente si la Decisión sobre el «Escudo de la privacidad» impide el ejercicio de sus facultades para suspender la transferencia en cuestión y confirme que alberga dudas sobre la validez de esta Decisión, podría acudir de nuevo a los tribunales nacionales para que estos consulten al Tribunal de Justicia a este respecto.[75]

181. Entonces se pondría en marcha un procedimiento que permitiría a todas las partes y a todos los interesados a los que se refiere el artículo 23, párrafo segundo, del Estatuto del Tribunal de Justicia presentar al Tribunal de Justicia observaciones específicamente referidas a la validez de la Decisión sobre el «Escudo de la privacidad», indicando, en su caso, las apreciaciones particulares que impugnan, así como las razones por las cuales consideran que la Comisión ha rebasado en dicha Decisión el margen de apreciación reducido de que disponía.[76] En el marco de tal procedimiento, la Comisión tendría la oportunidad de responder de forma precisa y detallada a cada una de las posibles críticas dirigidas contra dicha Decisión. Aunque el presente asunto haya ofrecido la oportunidad a las partes y los interesados que han presentado observaciones al Tribunal de Justicia de debatir sobre determinados aspectos pertinentes para evaluar la conformidad de la Decisión sobre el «Escudo de la privacidad» con los artículos 7, 8 y 47 de la Carta, esta cuestión merece, habida cuenta de su transcendencia, que se le consagre un diálogo exhaustivo y detallado.

74 Asunto pendiente T-738/16, La Quadrature du Net y otros/Comisión (DO 2017, C 6, p. 39).

75 Debo señalar, por lo demás, que, en sus observaciones escritas, el DPC no adoptó una postura sobre la influencia de la Decisión sobre el «Escudo de la privacidad» en la tramitación de la reclamación de la que conoce.

76 Véase, a este respecto, la sentencia Schrems, apartado 78.

182. En mi opinión, la prudencia exige esperar a que se llegue a estas etapas procesales antes de que el Tribunal de Justicia examine la influencia que ejerce la Decisión sobre el «Escudo de la privacidad» sobre la tramitación por parte de una autoridad de control de una petición de suspensión de una transferencia efectuada hacia los Estados Unidos con arreglo al artículo 46, apartado 1, del RGPD y se pronuncie sobre la validez de esta Decisión.

183. Esto es cierto, con mayor motivo, en la medida en que el sumario presentado al Tribunal de Justicia no permite concluir que la tramitación por parte del DPC de la reclamación del Sr. Schrems dependerá necesariamente de si la Decisión sobre el «Escudo de la privacidad» impide el ejercicio por parte de las autoridades de control de su facultad de suspender una transferencia basada en cláusulas contractuales tipo.

184. A este respecto, en primer lugar, no puede excluirse que el DPC tenga que suspender la transferencia en cuestión por otros motivos distintos de los relativos a la presunta inadecuación del nivel de protección que se ofrece en los Estados Unidos frente a las violaciones de los derechos fundamentales de los interesados derivados de las actividades de los servicios de inteligencia estadounidenses. En particular, el órgano jurisdiccional remitente precisó que el Sr. Schrems sostiene, en su reclamación ante el DPC, que las cláusulas contractuales invocadas por Facebook Ireland en apoyo de esta transferencia no reflejan fielmente las enunciadas en el anexo de la Decisión 2010/87. El Sr. Schrems alega, asimismo, que dicha transferencia no está comprendida en el ámbito de aplicación de esta Decisión, sino más bien en el de otras Decisiones sobre las CCT. [77]

185. En segundo lugar, el DPC y el órgano jurisdiccional remitente han señalado que Facebook Ireland no ha invocado la Decisión sobre el «Escudo de la privacidad» en apoyo de la transferencia contemplada en la reclamación del Sr. Schrems, [78] extremo que esta sociedad confirmó en la vista. A pesar de que Facebook Inc. ha autocertificado su adhesión a los principios del Escudo de la privacidad desde el 30 de septiembre de 2016, [79] Facebook Ireland afirma que esta adhesión solo se refiere a la transferencia de determinadas categorías de datos, a saber, las relativas a los socios comerciales de Facebook Inc. Me parece inoportuno que el Tribunal de Justicia anticipe las preguntas que podrían suscitarse al respecto al examinar si, suponiendo que Facebook Ireland no pueda invocar la Decisión 2010/87 en apoyo de la transferencia en cuestión, a pesar de todo, dicha transferencia estaría amparada por la Decisión sobre el «Escudo de la privacidad», aun cuando este último no ha planteado esta alegación ante el órgano jurisdiccional remitente ni ante el DPC.

186. Concluyo de ello que no procede responder a las cuestiones prejudiciales segunda a quinta, ni a las cuestiones novena y décima, ni examinar la validez de la Decisión sobre el «Escudo de la privacidad».

G. Observaciones con carácter subsidiario relativas a los efectos y a la validez de la Decisión sobre el «Escudo de la privacidad»

187. Aunque el análisis anterior me lleva a proponer al Tribunal de Justicia, con carácter principal, que se abstenga de pronunciarse sobre la influencia de la Decisión sobre el «Escudo de la privacidad» en la tramitación de una reclamación como la planteada por el Sr. Schrems ante el DPC y sobre la validez de dicha Decisión, me parece útil desarrollar, con carácter subsidiario y con reservas, algunas observaciones no exhaustivas al respecto.

77 El Sr. Schrems alega, en apoyo de esta tesis, que no debe considerarse a Facebook Inc. únicamente como un encargado del tratamiento, sino también como un «responsable del tratamiento», en el sentido del artículo 4, apartado 7, del RGPD, en lo tocante al tratamiento de los datos personales de los usuarios de la red social Facebook. Véase, a este respecto, la sentencia de 5 de junio de 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388), apartado 30.

78 Véase la sentencia de primera instancia de la High Court (Tribunal Superior) del 3 de octubre de 2017, apartado 66.

79 Véase la página web del «Escudo de la privacidad» (https://www.privacyshield.gov/participant_search).

1. Sobre la influencia de la Decisión sobre el «Escudo de la privacidad» en el marco de la tramitación por parte de una autoridad de control de una reclamación relativa a la licitud de una transferencia basada en garantías contractuales

188. La novena cuestión prejudicial plantea la cuestión de si la conclusión alcanzada en la Decisión sobre el «Escudo de la privacidad» relativa al carácter adecuado del nivel de protección garantizado en los Estados Unidos, habida cuenta de las limitaciones establecidas al acceso a los datos transferidos y a su utilización por parte de las autoridades estadounidenses con fines de seguridad nacional, así como de la protección jurídica de los interesados, impide que una autoridad de control suspenda una transferencia hacia este tercer país realizada en virtud de cláusulas contractuales tipo.

189. Me parece que esta problemática debe analizarse teniendo en cuenta los apartados 51 y 52 de la sentencia Schrems, de los que se desprende que las decisiones de adecuación vinculan a las autoridades de control en tanto en cuanto no hayan sido declaradas inválidas. Por lo tanto, la autoridad de control ante la que se haya planteado la reclamación de una persona cuyos datos se transfieran al tercer país al que se refiere una decisión de adecuación no puede suspender la transferencia alegando que el nivel de protección en dicho país es inadecuado, sin que el Tribunal de Justicia haya declarado previamente la invalidez de dicha decisión. [80]

190. En esencia, el órgano jurisdiccional remitente pretende averiguar si, en lo referente a una decisión de adecuación —como la Decisión sobre el «Escudo de la privacidad» o, antes de esta, la Decisión de puerto seguro— que se basa en la adhesión voluntaria de las empresas a los principios que establece, esta conclusión únicamente es válida en la medida en que la transferencia al tercer país de que se trate esté amparada por dicha Decisión o también cuando se fundamente en una base jurídica distinta.

191. Según el Sr. Schrems, los Gobiernos alemán, neerlandés, polaco y portugués, así como la Comisión, la constatación de adecuación efectuada en la Decisión sobre el «Escudo de la privacidad» no priva a las autoridades de control de su facultad para suspender o prohibir una transferencia hacia los Estados Unidos efectuada en virtud de cláusulas contractuales tipo. En su opinión, cuando la transferencia a los Estados Unidos no se base en la Decisión sobre el «Escudo de la privacidad», las autoridades de control no estarán formalmente vinculadas por esta Decisión en el marco del ejercicio de las facultades que les confiere el artículo 58, apartado 2, del RGPD. En otras palabras, estas autoridades pueden apartarse de las conclusiones alcanzadas por la Comisión en cuanto a la adecuación del nivel de protección contra las injerencias de las autoridades públicas estadounidenses en el ejercicio de los derechos fundamentales de los interesados. El Gobierno neerlandés y la Comisión precisan, no obstante, que las autoridades de control deben tenerlas en cuenta cuando hagan uso de estas facultades. A juicio del Gobierno alemán, estas autoridades únicamente pueden realizar apreciaciones contrarias tras un examen sobre el fondo, que incluya las investigaciones pertinentes, de las conclusiones alcanzadas por la Comisión.

192. En cambio, Facebook Ireland y el Gobierno estadounidense alegan, en esencia, que el efecto vinculante de una decisión de adecuación implica, a la luz de los requisitos de seguridad jurídica y de aplicación uniforme del Derecho de la Unión, que las autoridades de control no están facultadas para cuestionar las conclusiones recogidas en esa decisión, incluso en el marco de la tramitación de una reclamación que tenga por objeto lograr la suspensión de transferencias efectuadas hacia el tercer país en cuestión sobre la base de un fundamento distinto de dicha decisión.

80 Véase, en este sentido, la sentencia Schrems, apartado 59.

193. Suscribo el primero de estos enfoques. Dado que el ámbito de aplicación de la Decisión sobre el «Escudo de la privacidad» está limitado a las transferencias realizadas hacia una empresa autocertificada con arreglo a esta Decisión, la referida Decisión no puede obligar formalmente a las autoridades de control en lo tocante a las transferencias que no estén comprendidas en dicho ámbito de aplicación. Por consiguiente, la Decisión sobre el «Escudo de la privacidad» no tiene como objetivo garantizar la seguridad jurídica salvo en beneficio de los exportadores que transfieran datos dentro del marco que esta establece. A mi juicio, la independencia que reconoce el artículo 52 del RGPD a las autoridades de control parece oponerse también a que estén vinculadas por las conclusiones de la Comisión en una decisión de adecuación aun fuera de su ámbito de aplicación.

194. Obviamente, las constataciones que aparecen en la Decisión sobre el «Escudo de la privacidad» en relación con la adecuación del nivel de protección garantizado en los Estados Unidos contra las injerencias relativas a las actividades de sus servicios de inteligencia constituyen el punto de partida del análisis mediante el cual una autoridad de control evalúa, caso por caso, si una transferencia basada en las cláusulas contractuales tipo debe suspenderse debido a tales injerencias. Sin embargo, si tras una investigación detallada considera que no puede estar de acuerdo con estas conclusiones en lo referente a la transferencia sobre la que se le ha consultado, en mi opinión la autoridad de control competente conserva la facultad de ejercer las facultades que le confiere el artículo 58, apartado 2, letras f) y j), del RGPD.

195. Dicho esto, en el supuesto de que el Tribunal de Justicia diera a la cuestión actualmente examinada una respuesta contraria a la que defiendo, procedería examinar si, a pesar de todo, esas facultades deben restaurarse debido a la invalidez de la Decisión sobre el «Escudo de la privacidad».

2. Sobre la validez de la Decisión sobre el «Escudo de la privacidad»

196. Las siguientes observaciones plantearán determinadas preguntas en cuanto a la procedencia de las apreciaciones que figuran en la Decisión sobre el «Escudo de la privacidad» por lo que respecta al carácter adecuado, en el sentido del artículo 45, apartado 1, del RGPD, del nivel de protección garantizado por los Estados Unidos respecto de las actividades de vigilancia de las comunicaciones electrónicas llevadas a cabo por las autoridades de inteligencia estadounidenses. Estas observaciones no pretenden exponer una postura definitiva o exhaustiva sobre la validez de esta Decisión. Se limitarán a aportar algunas reflexiones que podrían resultar útiles al Tribunal de Justicia en caso de que desee pronunciarse sobre este punto, contrariamente a lo que recomiendo.

197. A este respecto, del considerando 64 y del apartado I.5 del anexo II de la Decisión sobre el «Escudo de la privacidad» se desprende que la adhesión de las empresas a los principios establecidos en esta Decisión puede verse limitada, en particular, por las exigencias de la seguridad nacional, el interés público y el cumplimiento de la ley o por conflictos de obligaciones derivados del Derecho estadounidense.

198. En consecuencia, la Comisión evaluó las salvaguardias existentes en el Derecho de los Estados Unidos con respecto al acceso a los datos transferidos y su utilización por los poderes públicos estadounidenses, en particular, a efectos de seguridad nacional. [81] Obtuvo del Gobierno estadounidense determinados compromisos relativos, por una parte, a las limitaciones al acceso y a la utilización por parte de las autoridades estadounidenses de los datos transferidos, así como, por otra parte, a la protección jurídica ofrecida a los interesados. [82]

81 Véase el considerando 65 de la Decisión sobre el «Escudo de la privacidad».

82 Véanse los anexos III a VII de la Decisión sobre el «Escudo de la privacidad».

199. Ante el Tribunal de Justicia, el Sr. Schrems alega la invalidez de la Decisión sobre el «Escudo de la privacidad» basándose en que las garantías así descritas no bastan para proporcionar un nivel adecuado de protección de los derechos fundamentales de las personas cuyos datos se transfieren a los Estados Unidos. El DPC, el EPIC, así como los Gobiernos austriaco, polaco y portugués, sin cuestionar directamente la validez de esta Decisión, impugnan las apreciaciones efectuadas en dicho acto por la Comisión relativas a la adecuación del nivel de protección contra las injerencias derivadas de las actividades de los servicios de inteligencia estadounidenses. Estas dudas reflejan las inquietudes expresadas por el Parlamento,[83] el CEPD[84] y el SEPD.[85]

200. Antes de examinar la procedencia de la declaración de adecuación efectuada en la Decisión sobre el «Escudo de la privacidad», es necesario precisar la metodología que debe guiar dicho examen.

a) Precisiones relativas al contenido del examen de validez de una decisión de adecuación

1) Sobre los términos de la comparación que permiten evaluar la «equivalencia sustancial» del nivel de protección

201. De conformidad con el artículo 45, apartado 3, del RGPD y la jurisprudencia del Tribunal de Justicia,[86] la Comisión solo puede declarar que un tercer país garantiza un nivel de protección adecuado a condición de que haya concluido, de forma debidamente motivada, que el nivel de protección de los derechos fundamentales de los interesados en dicho país es «sustancialmente equivalente» al exigido en la Unión con arreglo a este Reglamento interpretado a la luz de la Carta.

202. Así pues, la verificación del carácter adecuado del nivel de protección garantizado en un tercer país implica necesariamente una comparación entre las normas y las prácticas aplicables en dicho tercer país, por un lado, y los estándares de protección en vigor en la Unión, por otro. Mediante su segunda cuestión prejudicial, el órgano jurisdiccional remitente solicita al Tribunal de Justicia que precise los términos de esta comparación.[87]

203. Más concretamente, este órgano jurisdiccional pretende averiguar si la reserva de competencia que reconocen el artículo 4 TUE, apartado 2, y el artículo 2, apartado 2, del RGPD a los Estados miembros en materia de protección de la seguridad nacional supone que el ordenamiento jurídico de la Unión no incorpora estándares de protección con los que se deban comparar, con el fin de evaluar

83 Resoluciones del Parlamento de 6 de abril de 2017, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., P8_TA(2017)0131, y de 5 de julio de 2018, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., P8 _TA(2018)0315.

84 Véanse Grupo de Trabajo del Artículo 29 sobre la protección de datos (en lo sucesivo, «Grupo 29»), Opinion 1/2016 on the EU-US. Privacy Shield draft adequacy decision, 13 de abril de 2016, WP. 238; Grupo 29, EU-US Privacy Shield — First Annual Joint Review, 28 de noviembre de 2017, WP. 255, y CEPD, EU-US Privacy Shield — Second Annual Joint Review, 22 de enero de 2019. El Grupo 29 se había creado en virtud del artículo 29, apartado 1, de la Directiva 95/46 que establecía su carácter consultivo e independiente. Con arreglo al apartado 2 de dicho artículo, este Grupo se componía de un representante de cada una de las autoridades de control nacionales, un representante de cada autoridad creada por las instituciones y organismos comunitarios y un representante de la Comisión. Desde la entrada en vigor del RGPD, el Grupo 29 fue sustituido por el CEPD (véase el artículo 94, apartado 2, de este Reglamento).

85 Véase SEPD, dictamen 4/2016 relativo al «Escudo de la privacidad UE-EE. UU.» (Privacy Shield) — Proyecto de decisión de adecuación, de 30 de mayo de 2016. El SEPD fue creado mediante el artículo 1, apartado 2, del Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO 2001, L 8, p. 1). Supervisa la aplicación de las disposiciones de ese Reglamento.

86 Véase el punto 112 de las presentes conclusiones.

87 Recuerdo que la equivalencia sustancial del nivel de protección garantizado por un tercer Estado en relación con el que se exige en la Unión también debe evaluarse cuando, en el marco de una transferencia específica basada en cláusulas contractuales tipo previstas en la Decisión 2010/87, el responsable del tratamiento o, en su defecto, la autoridad de control competente verifiquen si las autoridades públicas del tercer país de destino someten al exportador a exigencias que exceden los límites de lo que es necesario en una sociedad democrática (véase la cláusula 5 que figura en el anexo de la Decisión 2010/87, así como la nota a pie de página correspondiente). Véanse los puntos 115, 134 y 135 de las presentes conclusiones.

su adecuación, las garantías en las que se enmarca en un tercer país el tratamiento por parte de las autoridades públicas, con fines de protección de la seguridad nacional, de los datos que se transfieren hacia dicho país. En caso de respuesta afirmativa, dicho órgano jurisdiccional desea saber cómo debe determinarse el marco de referencia pertinente.

204. A este respecto, se debe recordar que la razón de ser de las restricciones que establece el Derecho de la Unión a las transferencias internacionales de datos personales, al exigir que se garantice la continuidad del nivel de protección de los derechos de los interesados, tiene por objeto evitar el riesgo de elusión de los estándares aplicables dentro de la Unión. [88] Según alegó, en esencia, Facebook Ireland, no existe justificación alguna, en relación con ese objetivo, para esperar que un tercer país cumpla requisitos que no se correspondan con obligaciones que incumban a los Estados miembros.

205. Pues bien, según su artículo 51, apartado 1, la Carta se aplica a los Estados miembros únicamente cuando estos apliquen el Derecho de la Unión. Por consiguiente, la validez de una decisión de adecuación respecto de las restricciones al ejercicio de los derechos fundamentales de los interesados derivadas de la normativa del tercer país de destino depende de una comparación entre dichas restricciones y las que permitirían a los Estados miembros las disposiciones de la Carta *únicamente en la medida en que una normativa similar de un Estado miembro estuviese comprendida en el ámbito de aplicación del Derecho de la Unión*.

206. Sin embargo, la adecuación del nivel de protección ofrecido en el tercer Estado de destino no puede apreciarse ignorando las posibles injerencias en el ejercicio de los derechos fundamentales de los interesados que resultarían de medidas estatales, en particular en el ámbito de la seguridad nacional, que, si fueran adoptadas por un Estado miembro, quedarían excluidas del ámbito de aplicación del Derecho de la Unión. A los efectos de esta apreciación, el artículo 45, apartado 2, letra a), del RGPD exige que se tenga en cuenta, sin limitación alguna, la normativa en materia de seguridad nacional en vigor en dicho tercer Estado.

207. La evaluación del carácter adecuado del nivel de protección respecto de tales medidas estatales implica, en mi opinión, comparar las garantías de las que vienen acompañadas con el nivel de protección exigido dentro de la Unión con arreglo al Derecho de los Estados miembros, incluyendo sus compromisos en virtud del CEDH. Dado que la adhesión de los Estados miembros al CEDH obliga a estos a ajustar sus Derechos internos a las disposiciones de dicho Convenio y constituye de este modo, como han señalado en esencia Facebook Ireland, los Gobiernos alemán y checo y la Comisión, un denominador común de los Estados miembros, consideraré estas disposiciones como el elemento de comparación pertinente a los efectos de dicha evaluación.

208. En el presente asunto, como se ha indicado anteriormente, [89] las exigencias de la seguridad nacional de los Estados Unidos prevalecen sobre las obligaciones de las empresas autocertificadas con arreglo a la Decisión sobre el «Escudo de la privacidad». Asimismo, la validez de esta Decisión depende de si tales exigencias vienen acompañadas de garantías que ofrezcan un nivel de protección sustancialmente equivalente al que se debe garantizar en la Unión.

209. La respuesta a esta cuestión exige, antes que nada, que se identifiquen los estándares —a saber, los basados en la Carta o bien en el CEDH— que debería cumplir, en la Unión, una normativa en materia de vigilancia de las comunicaciones electrónicas similar a la que examinó la Comisión en la Decisión sobre el «Escudo de la privacidad». La determinación de los estándares aplicables depende

88 Véase el punto 117 de las presentes conclusiones.

89 Véase el punto 197 de las presentes conclusiones.

de si unas normas como el artículo 702 de la FISA y el EO 12333 entrarían o no, en caso de que procedieran de un Estado miembro, dentro del alcance de la limitación efectuada al ámbito de aplicación del RGPD en virtud del artículo 2, apartado 2, de este Reglamento, interpretado a la luz del artículo 4 TUE, apartado 2.

210. A este respecto, del tenor del artículo 4 TUE, apartado 2, y de reiterada jurisprudencia se desprende que el Derecho de la Unión y, en particular, los instrumentos de Derecho derivado relativos a la protección de los datos personales no se aplican a las actividades de protección de la seguridad nacional en la medida en que estas constituyen actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares. [90]

211. Este principio implica, *por una parte*, que una normativa en el ámbito de la protección de la seguridad nacional no entra dentro del ámbito de aplicación del Derecho de la Unión cuando regula únicamente actividades estatales, sin incluir ninguna actividad ejercida por particulares. En consecuencia, a mi juicio, este Derecho no se aplica a las medidas nacionales relativas a la recogida y a la utilización de datos personales llevadas a cabo directamente por el Estado con fines de protección de la seguridad nacional, sin imponer obligaciones específicas a operadores privados. En particular, como alegó la Comisión en la vista, una medida adoptada por un Estado miembro que, a semejanza del EO 12333, autorice el acceso directo por sus servicios de seguridad a los datos en tránsito, estaría excluida del ámbito de aplicación del Derecho de la Unión. [91]

212. Mucho más compleja es la cuestión de si, *por otra parte*, de las disposiciones nacionales que, de la misma manera que el artículo 702 de la FISA, obligan a los proveedores de servicios de comunicaciones electrónicas a ofrecer su asistencia a las autoridades competentes en materia de seguridad nacional con el fin de permitirles acceder a determinados datos personales queda también fuera del ámbito de aplicación del Derecho de la Unión.

213. Aunque la sentencia PNR aboga por una respuesta afirmativa a esta cuestión, el razonamiento adoptado en las sentencias Tele2 Sverige y Ministerio Fiscal podría justificar que se le diera una respuesta negativa.

214. En la sentencia PNR, el Tribunal de Justicia anuló la Decisión mediante la cual la Comisión había declarado la adecuación del nivel de protección de los datos personales incluidos en los registros de nombres de los pasajeros aéreos (Passenger Name Records, PNR) que se transferían a la autoridad estadounidense competente en materia de aduanas y de protección de fronteras. [92] El Tribunal de Justicia declaró que el tratamiento al que se refería esta Decisión —a saber, la transferencia de los datos PNR por las compañías aéreas a la autoridad en cuestión— entraba, *habida cuenta de su objeto*, dentro del alcance de la exclusión del ámbito de aplicación de la Directiva 95/46 prevista en su artículo 3, apartado 2. Según el Tribunal de Justicia, este tratamiento no era necesario para la realización de una prestación de servicios, sino para la salvaguarda de la seguridad pública y para fines represivos. Dado que la transferencia en cuestión se inscribía en un marco establecido por los poderes

90 Véanse, en particular, las sentencias de 6 de noviembre de 2003, Lindqvist (C-101/01, EU:C:2003:596), apartados 43 y 44; PNR, apartado 58; de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia (C-73/07, EU:C:2008:727), apartado 41; de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C-203/15 y C-698/15, en lo sucesivo, «sentencia Tele2 Sverige», EU:C:2016:970), apartado 69, y de 2 de octubre de 2018, Ministerio Fiscal (C-207/16, en lo sucesivo, «sentencia Ministerio Fiscal», EU:C:2018:788), apartado 32.

91 Con el fin de evitar toda confusión sobre este punto debo señalar que, en la Decisión sobre el «Escudo de la privacidad», la Comisión no pudo determinar si los Estados Unidos interceptan efectivamente las comunicaciones que circulan por los cables transatlánticos, dado que las autoridades estadounidenses no confirmaron ni desmintieron esta afirmación [véase el considerando 75 de esta Decisión, así como la carta del Sr. Robert Litt, de 22 de febrero de 2016, que figura en su anexo VI, apartado I, letra a)]. No obstante, comoquiera que el Gobierno estadounidense no ha negado recoger datos en tránsito sobre la base del EO 12333, me parece que, antes de proceder a la declaración de la adecuación, la Comisión debería haber obtenido de parte de este último garantías de que tal recogida, en el caso de que se produjera, se vería rodeada de salvaguardias suficientes contra los riesgos de abuso. En los considerandos 68 a 77 de dicha Decisión, la Comisión examinó desde esta perspectiva las limitaciones y garantías que deberían aplicarse en tal supuesto en virtud de la PPD 28.

92 Se trataba de la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (DO 2004, L 235, p. 11).

públicos y referido a la seguridad pública, estaba excluida del ámbito de aplicación de esta Directiva a pesar del hecho de que los datos PNR inicialmente eran recogidos por operadores privados en el marco de una actividad comercial comprendida en dicho ámbito de aplicación y de que estos últimos organizaban dicha transferencia. [93]

215. En la sentencia posterior Tele2 Sverige, [94] el Tribunal de Justicia declaró que unas disposiciones nacionales, basadas en el artículo 15, apartado 1, de la Directiva 2002/58/CE, [95] que regulan tanto la conservación de datos de tráfico y de localización por los proveedores de servicios de telecomunicaciones, como el acceso de las autoridades públicas a los datos conservados para los fines mencionados en esa disposición —que incluyen la represión penal y la protección de la seguridad nacional— están comprendidas en el ámbito de aplicación de esta Directiva y, por tanto, de la Carta. Según el Tribunal de Justicia, ni las disposiciones relativas a la conservación de los datos, ni las relativas al acceso a los datos conservados entran dentro del alcance de la exclusión del ámbito de aplicación de esta Directiva prevista en su artículo 1, apartado 3, que hace referencia, en particular, a las actividades del Estado en materia de lucha contra la delincuencia y de protección de la seguridad nacional. [96] El Tribunal de Justicia confirmó esta jurisprudencia en la sentencia Ministerio Fiscal. [97]

216. Sin embargo, el artículo 702 de la FISA difiere de tal normativa en el sentido de que esta disposición no impone a los proveedores de servicios de comunicaciones electrónicas ninguna obligación de conservar los datos ni de realizar ningún tratamiento adicional en ausencia de una petición de acceso a los datos procedente de las autoridades de inteligencia.

217. Por lo tanto, se plantea la cuestión de si están comprendidas en el ámbito de aplicación del RGPD y, en consecuencia, de la Carta, unas medidas nacionales que impongan a estos proveedores la obligación de poner datos a disposición de las autoridades públicas, con fines de seguridad nacional, *con independencia de cualquier obligación de conservación*. [98]

218. Un *primer enfoque* podría consistir en conciliar, en la medida de lo posible, las dos líneas jurisprudenciales mencionadas anteriormente interpretando la conclusión extraída por el Tribunal de Justicia en las sentencias Tele2 Sverige y Ministerio Fiscal, relativa a la aplicabilidad del Derecho de la Unión a las medidas que regulan el acceso a los datos por las autoridades nacionales, en particular, con

93 Sentencia PNR (apartados 56 a 58). Por lo demás, en la sentencia de 10 de febrero de 2009, Irlanda/Parlamento y Consejo (C-301/06, EU:C:2009:68), apartados 90 y 91, el Tribunal de Justicia declaró que las consideraciones desarrolladas en la sentencia PNR no podían trasladarse a los tratamientos contemplados en la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO 2006, L 105, p. 54). El Tribunal de Justicia justificó esta conclusión por el hecho de que la Directiva 2006/24, a diferencia de la Decisión examinada en la sentencia PNR, regía únicamente las actividades de los proveedores de servicios en el mercado interior, sin regular las actividades de los poderes públicos para fines represivos. Mediante este razonamiento, el Tribunal de Justicia parece haber afirmado que, *a contrario*, la conclusión extraída en la sentencia PNR se podía trasladar a disposiciones relativas al acceso a los datos conservados o a su utilización por estas autoridades.

94 Sentencia Tele2 Sverige, apartados 67 a 81.

95 Directiva del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO 2002, L 201, p. 37).

96 Dado que la Directiva 2002/58 concreta las exigencias de la Directiva 95/46, actualmente derogada por el RGPD, que reproduce ampliamente su contenido, considero que la jurisprudencia relativa a la interpretación del artículo 1, apartado 3, de la Directiva 2002/58 es aplicable por analogía a la interpretación del artículo 2, apartado 2, del RGPD. Véanse, en este sentido, las sentencias de Tele2 Sverige, apartado 69, y Ministerio Fiscal, apartado 32.

97 Sentencia Ministerio Fiscal (apartados 34, 35 y 37).

98 Esta misma cuestión se ha planteado en el marco de otras tres peticiones de decisión prejudicial pendientes ante el Tribunal de Justicia. Véanse el asunto C-623/17, Privacy International (DO 2018, C 22, p. 29), así como los asuntos acumulados C-511/18 y C-512/18, La Quadrature du Net y otros y French Data Network y otros (DO 2018, C 392, p. 7).

fines de protección de la seguridad nacional,[99] en el sentido de que está limitada a los supuestos en los que los datos se hayan conservado *en virtud de una obligación legal* establecida con arreglo al artículo 15, apartado 1, de la Directiva 2002/58. En cambio, esta conclusión no se aplicaría al contexto fáctico distinto de la sentencia PNR, que se refería a la transferencia a una autoridad estadounidense competente en materia de seguridad interior de datos conservados por las compañías aéreas, con una finalidad comercial, por propia iniciativa.

219. Según un *segundo enfoque*, que recomienda la Comisión y que considero más convincente, el razonamiento adoptado en las sentencias Tele2 Sverige y Ministerio Fiscal justificaría la aplicabilidad del Derecho de la Unión a una normativa nacional que obligue a los proveedores de servicios de comunicaciones electrónicas a proporcionar asistencia a las autoridades responsables de la seguridad nacional para que estas puedan acceder a determinados datos, *con independencia de que estas normas vengan o no acompañadas de una obligación de conservación previa de los datos*.

220. El elemento central de este razonamiento se basa, en efecto, no en el objeto de las disposiciones de que se trataba, como en la sentencia PNR, sino en el hecho de que estas disposiciones regulaban las actividades de los proveedores obligándoles a realizar un tratamiento de datos. Estas actividades no constituían actividades del Estado en los ámbitos contemplados en el artículo 1, apartado 3, de la Directiva 2002/58 y en el artículo 3, apartado 2, de la Directiva 95/46, cuyo contenido reproduce esencialmente el artículo 2, apartado 2, del RGPD.

221. Así pues, en la sentencia Tele2 Sverige, el Tribunal de Justicia observó que «el acceso a los datos conservados por [los] proveedores, es una medida que tiene por objeto el tratamiento de datos personales *por estos últimos*, tratamientos que están comprendidos en el ámbito de aplicación de esta Directivas».[100] De la misma manera, en la sentencia Ministerio Fiscal declaró que las medidas legales que obligan a los proveedores a conceder a las autoridades competentes el acceso a los datos conservados «implican necesariamente un tratamiento de dichos datos *por esos proveedores*».[101]

222. Pues bien, la puesta a disposición de datos por parte del responsable del tratamiento en beneficio de una autoridad pública se enmarca en la definición de «tratamiento» establecida en el artículo 4, apartado 2, del RGPD.[102] Lo mismo sucede en relación con el filtrado previo de los datos mediante criterios de búsqueda con el fin de aislar aquellos a los que las autoridades públicas han solicitado acceso.[103]

99 En la sentencia Tele2 Sverige, aunque el Tribunal de Justicia se concentró en el examen de la justificación de las injerencias derivadas de las medidas de conservación y de acceso en cuestión en relación con el objetivo de la lucha contra las infracciones penales, la conclusión a la que llegó también es aplicable, *mutatis mutandis*, cuando tales medidas persiguen un objetivo de protección de la seguridad nacional. En efecto, el artículo 15, apartado 1, de la Directiva 2002/58 menciona, entre los objetivos que pueden justificar tales medidas, tanto la lucha contra las infracciones penales como la protección de la seguridad nacional. Asimismo, el artículo 1, apartado 3, de la Directiva 2002/58 y el artículo 2, apartado 2, del RGPD excluyen del ámbito de aplicación de estos instrumentos las actividades del Estado tanto en materia de seguridad nacional como en el ámbito penal. Además, las medidas examinadas en el asunto que dio lugar a la sentencia Tele2 Sverige también perseguían un fin relacionado con la seguridad nacional. En el apartado 119 de dicha sentencia, el Tribunal de Justicia abordó expresamente la justificación de medidas relativas a la conservación y al acceso a los datos de tráfico y de localización en relación con el objetivo de la protección de la seguridad nacional en la medida en que abarca la lucha contra el terrorismo.

100 Sentencia Tele2 Sverige, apartado 78 (el subrayado es mío). Como pone de manifiesto el uso del término «por lo demás», el Tribunal de Justicia señaló en el apartado 79 de esta sentencia, únicamente con el fin de corroborar su conclusión relativa a la aplicabilidad de la Directiva 2002/58, la relación intrínseca que existe entre la obligación de conservación de los datos de que se trata en el asunto que dio lugar a dicha sentencia y las disposiciones relativas al acceso de las autoridades nacionales a los datos conservados.

101 Sentencia Ministerio Fiscal, apartado 37 (el subrayado es mío).

102 Véase, en este sentido, la sentencia Ministerio Fiscal, apartado 38.

103 Véase, en este sentido, la sentencia de 13 de mayo de 2014, Google Spain y Google (C-131/12, EU:C:2014:317), apartado 28.

223. De todo ello concluyo que, siguiendo el razonamiento adoptado por el Tribunal de Justicia en las sentencias Tele2 Sverige y Ministerio Fiscal, el RGPD y, por tanto, la Carta son aplicables a una normativa nacional que obligue a los proveedores de servicios de comunicaciones electrónicas a ofrecer su colaboración a las autoridades responsables de la seguridad nacional poniendo datos a su disposición, en su caso tras haberlos filtrado, incluso con independencia de cualquier obligación legal de conservación de dichos datos.

224. Por añadidura, esta interpretación parece deducirse, al menos de forma implícita, de la sentencia Schrems. Como han señalado el DPC, los Gobiernos austriaco y polaco y la Comisión, el Tribunal de Justicia, en el marco del examen de la validez de la Decisión de puerto seguro, declaró que el Derecho del tercer país al que se refiere una decisión de adecuación debe establecer garantías sustancialmente equivalentes a las derivadas, en particular, de los artículos 7, 8 y 47 de la Carta frente a las injerencias de sus autoridades públicas en los derechos fundamentales de los interesados con fines de seguridad nacional. [104]

225. De ello resulta, de manera más específica, que una medida nacional que obligue a los proveedores de servicios de comunicaciones electrónicas a responder a una petición de acceso, procedente de las autoridades competentes en materia de seguridad nacional, a determinados datos conservados por dichos proveedores en el marco de sus actividades comerciales, con independencia de cualquier obligación legal, identificando previamente los datos solicitados mediante la aplicación de selectores (como en el marco del Programa PRISM), no está amparada por el artículo 2, apartado 2, del RGPD. Lo mismo sucedería en el caso de una medida nacional que exija a las empresas que explotan la «red troncal» de las telecomunicaciones que den acceso a las autoridades responsables de la seguridad nacional a datos que circulan por las infraestructuras que operan (como en el marco del Programa Upstream).

226. En cambio, una vez que los datos en cuestión han llegado a manos de las autoridades estatales, su conservación y su utilización posteriores por parte de estas autoridades con fines de seguridad nacional están cubiertas, en mi opinión y por los mismos motivos que se mencionan en el punto 211 de las presentes conclusiones, por la excepción prevista en el artículo 2, apartado 2, del RGPD, de forma que no están comprendidas en el ámbito de aplicación de este Reglamento ni, en consecuencia, de la Carta.

227. Para resumir todas las consideraciones anteriores, estimo que el control de la validez de la Decisión sobre el «Escudo de la privacidad» en relación con las limitaciones de los principios enunciados en esta que pueden derivarse de las actividades de las autoridades de inteligencia estadounidenses exige una doble verificación.

228. *En primer lugar*, se debe examinar si los Estados Unidos garantizan un nivel de protección sustancialmente equivalente al que se deriva de las disposiciones del RGPD y de la Carta frente a las limitaciones resultantes de la aplicación del artículo 702 de la FISA, en la medida de que esta disposición permite a la NSA obligar a los proveedores a poner datos personales a su disposición.

229. *En segundo lugar*, las disposiciones del CEDH constituyen el marco de referencia pertinente para evaluar si las limitaciones que podría suponer la aplicación del EO 12333, en la medida en que autoriza a las autoridades de inteligencia a recoger ellas mismas datos personales, sin la colaboración de operadores privados, ponen en entredicho la adecuación del nivel de protección garantizado en los Estados Unidos. Estas disposiciones también proporcionan los estándares de comparación que permiten valorar el carácter adecuado de este nivel de protección en relación con la conservación y la utilización de los datos adquiridos por las referidas autoridades con fines de seguridad nacional.

104 Sentencia Schrems, apartados 91 a 96. Además, en los considerandos 90, 124 y 141 de la Decisión sobre el «Escudo de la privacidad», la Comisión hace referencia a las disposiciones de la Carta, aceptando de este modo el principio según el cual las limitaciones de los derechos fundamentales que persiguen un objetivo de protección de la seguridad nacional deben ser conformes con la Carta.

230. No obstante, también se debe determinar si una declaración de adecuación supone que la recogida de datos con arreglo al EO 12333 va acompañada de un nivel de protección sustancialmente equivalente al que debe garantizarse en la Unión, *incluso en la medida en que esta recogida tenga lugar fuera del territorio de los Estados Unidos*, durante la fase de tránsito de los datos desde la Unión a ese tercer país.

2) Sobre la necesidad de garantizar un nivel adecuado de protección durante la fase de tránsito de los datos

231. Ante el Tribunal de Justicia se han defendido tres posturas distintas en lo referente a la necesidad o no de que la Comisión tenga en cuenta, para evaluar la adecuación del nivel de protección garantizado en un tercer país, las medidas nacionales relativas al acceso a los datos por parte de las autoridades de ese tercer país, fuera de su territorio, durante la fase de tránsito de los datos desde la Unión hacia este territorio.

232. En primer término, Facebook Ireland y los Gobiernos estadounidense y del Reino Unido sostienen, en esencia, que la existencia de tales medidas es irrelevante en el marco de una declaración de adecuación. En apoyo de este enfoque, estos últimos invocan la imposibilidad de que un tercer Estado controle el conjunto de las vías de comunicación situadas fuera de su territorio por las que circulan los datos procedentes de la Unión, de modo que teóricamente no se podría garantizar jamás que otro tercer Estado no recoja secretamente datos durante su tránsito.

233. En segundo término, el DPC, el Sr. Schrems, el EPIC, los Gobiernos austriaco y neerlandés, el Parlamento y el CEPD alegan que el imperativo de continuidad del nivel de protección, establecido en el artículo 44 del RGPD, supone que este nivel debe ser adecuado durante toda la transferencia, inclusive cuando los datos circulen por cables submarinos antes de alcanzar el territorio del tercer país de destino.

234. Aun reconociendo este principio, la Comisión sostiene, en tercer término, que el objeto de una declaración de adecuación se limita a la protección garantizada por el tercer país de que se trate *dentro de sus fronteras*, de manera que el hecho de que no se garantice un nivel adecuado de protección *durante el tránsito* a este tercer país no pone en entredicho la validez de una decisión de adecuación. Con todo, de conformidad con el artículo 32 del RGPD, corresponde al responsable del tratamiento velar por la seguridad de la transferencia protegiendo en la medida de lo posible los datos personales durante la fase de tránsito hacia dicho tercer país.

235. A este respecto, he de señalar que el artículo 44 del RGPD supedita las transferencias hacia un tercer país al respeto de las condiciones establecidas en las disposiciones del capítulo V de este Reglamento en la medida en que los datos pueden ser objeto de un tratamiento «tras su transferencia». Estos términos podrían interpretarse en el sentido de que significan, bien, como sostuvo el Gobierno estadounidense en su respuesta escrita a las preguntas del Tribunal de Justicia, que estas condiciones deben respetarse *una vez que los datos hayan llegado a su destino*, bien que se imponen *después de que haya comenzado la transferencia* (inclusive durante la fase de tránsito).

236. Dado que el tenor literal del artículo 44 del RGPD no es concluyente, una interpretación teleológica me lleva a asumir como propia la segunda de estas interpretaciones y, por tanto, a suscribir el segundo de los enfoques antes mencionados. En efecto, si se considerara que la exigencia de continuidad del nivel de protección previsto en esta disposición solo ampara las medidas de vigilancia aplicadas en el interior del territorio del tercer país de destino, dicha exigencia se podría eludir cuando ese tercer país aplicara tales medidas fuera de su territorio durante la fase de tránsito de los datos. Para evitar este riesgo, la evaluación de la adecuación del nivel de protección garantizado por un tercer país debe referirse al conjunto de las disposiciones, en particular en materia de seguridad

nacional, del ordenamiento jurídico de este tercer país,[105] entre las que figuran tanto las relativas a la vigilancia aplicadas en su territorio como las que permiten la vigilancia de los datos en tránsito hacia ese territorio.[106]

237. Dicho esto, nadie niega que, como ha señalado el CEPD, la evaluación del carácter adecuado del nivel de protección tiene únicamente por objeto, tal como se desprende del artículo 45, apartado 1, del RGPD, las disposiciones del ordenamiento jurídico *del tercer país de destino de los datos*. La imposibilidad que alegan Facebook Ireland y los Gobiernos estadounidense y del Reino Unido, de garantizar que otro tercer Estado no recopile en secreto esos datos durante su tránsito no afecta a esta evaluación. A mayor abundamiento, tal riesgo no puede excluirse aun después de que los datos hayan llegado al territorio del tercer Estado de destino.

238. Asimismo, también es cierto que, cuando evalúa la adecuación del nivel de protección garantizado por un tercer país, la Comisión puede encontrarse, en su caso, con que dicho tercer país no le desvela la existencia de determinados programas de vigilancia secretos. Sin embargo, de ello no se desprende que, *cuando se le informe de la existencia de tales programas*, la Comisión pueda abstenerse de tenerlos en cuenta en el marco de su examen de adecuación. Del mismo modo, si, tras la adopción de una decisión de adecuación, se le revela la existencia de determinados programas de vigilancia secretos, aplicados por el tercer país en cuestión en su territorio o durante el tránsito hacia este, la Comisión deberá revisar su conclusión relativa a la adecuación del nivel de protección garantizado por este tercer país si tal revelación genera dudas al respecto.[107]

3) Sobre la toma en consideración de las constataciones de hecho realizadas por la Comisión y por el órgano jurisdiccional remitente sobre el Derecho estadounidense

239. Si bien no se discute que el Tribunal de Justicia no es competente para realizar una interpretación del Derecho de un tercer país que sea vinculante en el ordenamiento jurídico de este, la validez de la Decisión sobre el «Escudo de la privacidad» depende de la procedencia de las apreciaciones realizadas por la Comisión respecto del nivel de protección, garantizado por el Derecho y la práctica de los Estados Unidos, de los derechos fundamentales de las personas cuyos datos se transfieren a este tercer país. En efecto, la Comisión debía motivar su declaración de adecuación en relación con los elementos mencionados en el artículo 45, apartado 2, del RGPD, relativos, en particular, al contenido del Derecho de dicho tercer país.[108]

240. La High Court (Tribunal Superior) expuso en su sentencia de primera instancia de 3 de octubre de 2017 unas apreciaciones detalladas que describían los aspectos pertinentes del Derecho estadounidense tras haber valorado las pruebas aportadas por las partes en el litigio.[109] Esta exposición coincide en gran medida con las conclusiones alcanzadas por la Comisión, en la Decisión sobre el «Escudo de la privacidad», relativas al contenido de las normas referidas a la recogida y el acceso de las autoridades de inteligencia estadounidenses a los datos transferidos, así como a las vías de recurso y a los mecanismos de supervisión relativos a estas actividades.

105 Véase, en este sentido, la sentencia Schrems, apartados 74 y 75.

106 Véase, en este sentido, CEPD, EU-US Privacy Shield — Second Annual Joint Review, de 22 de enero de 2019 (p. 17, apartado 86).

107 Véase el artículo 45, apartado 5, del RGPD. Véase también la sentencia Schrems, apartado 76.

108 Así, se declaró la invalidez de la Decisión de puerto seguro basándose en que, en esa Decisión, la Comisión no había manifestado que los Estados Unidos garantizaran efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales (sentencia Schrems, apartado 97). En particular, la Comisión no apreció la existencia de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de los interesados (sentencia Schrems, apartado 88) ni de una protección jurídica eficaz contra tales injerencias (sentencia Schrems, apartado 89).

109 Los puntos 54 a 73 de las presentes conclusiones resumen estas apreciaciones.

241. El órgano jurisdiccional remitente, al igual que varias de las partes e interesados que han presentado observaciones al Tribunal de Justicia, cuestionan en mayor medida las consecuencias jurídicas que extrajo la Comisión de estas apreciaciones —a saber, la conclusión según la cual los Estados Unidos garantizan un nivel adecuado de protección de los derechos fundamentales de las personas cuyos datos se transfieren con arreglo a esta Decisión— que la descripción que presentó del contenido del Derecho estadounidense.

242. En estas condiciones, evaluaré esencialmente la validez de la Decisión sobre el «Escudo de la privacidad» a la luz de las apreciaciones efectuadas por la propia Comisión en lo referente al contenido del Derecho estadounidense al examinar si estas justificaban la adopción de dicha decisión de adecuación.

243. A este respecto, no suscribo el punto de vista, defendido por el DPC y el Sr. Schrems, según el cual las apreciaciones realizadas por la High Court (Tribunal Superior) acerca del Derecho estadounidense vinculan al Tribunal de Justicia en el marco del examen de la validez de la Decisión sobre el «Escudo de la privacidad». Estos últimos alegan que, dado que el Derecho extranjero constituye una cuestión de hecho en virtud del Derecho procesal irlandés, el órgano jurisdiccional remitente es el único competente para establecer su contenido.

244. Es cierto que reiterada jurisprudencia reconoce a los órganos jurisdiccionales nacionales la competencia exclusiva para establecer los elementos de hecho pertinentes, así como para interpretar el Derecho de un Estado miembro y aplicarlo al litigio del que conoce.[110] Esta jurisprudencia refleja el reparto de funciones entre el Tribunal de Justicia y el órgano jurisdiccional remitente en el marco del procedimiento establecido en el artículo 267 TFUE. Aunque el Tribunal de Justicia es el único competente para interpretar el Derecho de la Unión y para pronunciarse sobre la validez del Derecho derivado, corresponde al órgano jurisdiccional nacional que deba resolver un litigio concreto del que conozca establecer su contexto fáctico y normativo para que el Tribunal de Justicia pueda darle una respuesta útil.

245. No creo que la razón de ser de esta competencia exclusiva del órgano jurisdiccional remitente sea extrapolable a la determinación del Derecho de un tercer país como elemento que puede influir en la conclusión que alcance el Tribunal de Justicia sobre la validez de un acto de Derecho derivado.[111] Comoquiera que una declaración de invalidez de tal acto tiene valor *erga omnes* en el ordenamiento jurídico de la Unión,[112] la conclusión del Tribunal de Justicia no puede depender del origen del procedimiento prejudicial. Pues bien, tal como han señalado Facebook Ireland y el Gobierno estadounidense, dependería de dicho origen si el Tribunal de Justicia estuviera vinculado por las apreciaciones del órgano jurisdiccional remitente relativas al Derecho de un tercer Estado, ya que estas pueden variar en función del órgano jurisdiccional nacional que las realice.

110 Véanse, en particular, las sentencias de 4 de mayo de 1999, Sürül (C-262/96, EU:C:1999:228), apartado 95; de 11 de septiembre de 2008, Eckelkamp y otros (C-11/07, EU:C:2008:489), apartado 32, y de 26 de octubre de 2016, Senior Home (C-195/15, EU:C:2016:804), apartado 20.

111 Véase, a este respecto, la sentencia de la Supreme Court (Tribunal Supremo) de 31 de mayo de 2019, apartado 6.18.

112 Véase la sentencia de 13 de mayo de 1981, International Chemical Corporation (66/80, EU:C:1981:102), apartados 12 y 13.

246. A la vista de las consideraciones precedentes, estimo que, cuando la respuesta a una cuestión prejudicial referida a la validez de un acto de la Unión implique la evaluación del contenido del Derecho de un tercer Estado, el Tribunal de Justicia no está vinculado por las apreciaciones efectuadas por el órgano jurisdiccional remitente relativas al Derecho de dicho tercer Estado, aunque puede tenerlas en cuenta. En su caso, el Tribunal de Justicia puede apartarse de ellas o completarlas tomando en consideración, dentro del respeto del principio de contradicción, otras fuentes para establecer los elementos necesarios para la evaluación de la validez del acto en cuestión. [113]

4) Sobre el alcance del estándar de la «equivalencia sustancial»

247. Debo recordar que la validez de la Decisión sobre el «Escudo de la privacidad» depende de si el ordenamiento jurídico de los Estados Unidos garantiza, en beneficio de las personas cuyos datos se transfieren de la Unión a este tercer país, un nivel de protección que sea «sustancialmente equivalente» al ofrecido en los Estados miembros con arreglo al RGPD y a la Carta, así como, en las materias excluidas del ámbito de aplicación del Derecho de la Unión, a sus compromisos en virtud del CEDH.

248. Como destacó el Tribunal de Justicia en la sentencia Schrems, [114] este estándar no significa que el nivel de protección deba ser «idéntico» al exigido en la Unión. Si bien los medios de los que se sirve un tercer país para proteger los derechos de los interesados pueden diferir de los que establece el RGPD, interpretado a la luz de la Carta, «[dichos medios] deben ser eficaces en [principio] para garantizar una protección sustancialmente equivalente a la garantizada en la Unión».

249. A mi entender, también se deduce de ello que el Derecho del tercer Estado de destino puede reflejar su propia escala de valores en función de la cual el peso respectivo de los diversos intereses en juego puede divergir del que se les atribuye en el ordenamiento jurídico de la Unión. A mayor abundamiento, la protección de los datos personales existente en la Unión responde a un estándar particularmente elevado en comparación con el nivel de protección en vigor en el resto del mundo. Por lo tanto, considero que el criterio de la «equivalencia sustancial» debe aplicarse de forma que se mantenga una cierta flexibilidad para tener en cuenta diferentes tradiciones jurídicas y culturales. No obstante, este criterio implica, si no se quiere vaciarlo de su esencia, que determinadas garantías mínimas y requisitos generales de protección de los derechos fundamentales derivados de la Carta y del CEDH tengan su equivalente en el ordenamiento jurídico del tercer país de destino. [115]

250. A este respecto, con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades consagrados por esta deberá estar establecida por la ley, respetar su contenido esencial y, dentro del respeto del principio de proporcionalidad, ser necesaria y responder efectivamente a un objetivo de interés general reconocido por la Unión o a la necesidad de protección de los derechos y libertades de los demás. Estos requisitos se corresponden esencialmente con los establecidos en el artículo 8, apartado 2, del CEDH. [116]

251. De conformidad con el artículo 52, apartado 3, de la Carta, en la medida en que los derechos garantizados en sus artículos 7, 8 y 47 se corresponden con los consagrados en los artículos 8 y 13 del CEDH, comparten su sentido y su alcance, en el bien entendido de que, no obstante, el Derecho de la Unión puede concederles una protección más amplia. Desde este punto de vista, tal como pondrá de

113 Véase, a este respecto, la sentencia de 22 de marzo de 2012, GLS (C-338/10, EU:C:2012:158), apartados 15, 33 y 34, en la que, con el fin de apreciar la validez de un reglamento por el que se establecía un derecho antidumping, el Tribunal de Justicia tuvo en cuenta unas estadísticas de Eurostat aportadas por la Comisión a solicitud del Tribunal de Justicia. Véase también la sentencia de 22 de octubre de 1991, Nölle (C-16/90, EU:C:1991:402), apartados 17, 23 y 24. Asimismo, en la sentencia Schrems, apartado 90, al examinar la validez de la Decisión de puerto seguro, el Tribunal de Justicia tomó en consideración ciertas comunicaciones de la Comisión.

114 Sentencia Schrems, apartados 73 y 74.

115 Véase, en este sentido, Grupo 29, «Adequacy Referential (updated)», 28 de noviembre de 2017, WP. 254 (pp. 3, 4 y 9).

116 Sin embargo, el artículo 8, apartado 2, del CEDH no hace referencia al concepto de «contenido esencial» del derecho al respeto de la vida privada. Véase, a este respecto, la nota a pie de página 161 de las presentes conclusiones.

manifiesto mi exposición, los estándares resultantes de los artículos 7, 8 y 47 de la Carta, según los ha interpretado el Tribunal de Justicia, son en ciertos aspectos más estrictos que los derivados del artículo 8 del CEDH, según la interpretación de esta disposición realizada por el Tribunal Europeo de Derechos Humanos (TEDH).

252. También debo señalar que existen asuntos pendientes ante cada uno de estos órganos jurisdiccionales que los invitan a reconsiderar determinados aspectos de sus respectivas jurisprudencias. Así pues, por una parte, dos sentencias recientes del TEDH en materia de vigilancia de las comunicaciones electrónicas —a saber, las sentencias Centrüm för Rättvisa c. Suecia [117] y Big Brother Watch c. Reino Unido [118]— han sido objeto de remisión para su reexamen ante la Gran Sala. Por otra parte, tres órganos jurisdiccionales nacionales han planteado al Tribunal de Justicia peticiones de decisión prejudicial que abren el debate sobre la necesidad o no de una modificación de su jurisprudencia derivada de la sentencia Tele2 Sverige. [119]

253. Una vez hechas estas precisiones, examinaré a continuación la validez de la Decisión sobre el «Escudo de la privacidad» en relación con el artículo 45, apartado 1, del RGPD, interpretado a la luz de la Carta y del CEDH en la medida en que, por un lado, garantizan los derechos al respeto de la vida privada y a la protección de los datos personales [sección b)], y, por otro, a la tutela judicial efectiva [sección c)].

b) Sobre la validez de la Decisión sobre el «Escudo de la privacidad» en relación con los derechos al respeto de la vida privada y a la protección de los datos personales

254. En el marco de su cuarta cuestión prejudicial, el órgano jurisdiccional remitente cuestiona, en esencia, la equivalencia sustancial entre el nivel de protección garantizado por los Estados Unidos y aquel del que disfrutan los interesados, dentro de la Unión, sobre la base de sus derechos fundamentales al respeto de la vida privada y a la protección de los datos personales.

1) Sobre la existencia de injerencias

255. En los considerandos 67 a 124 de la Decisión sobre el «Escudo de la privacidad», la Comisión menciona la posibilidad de que las autoridades públicas estadounidenses accedan a los datos transferidos desde la Unión y los utilicen a efectos de seguridad nacional en el marco de programas basados, entre otros, en el artículo 702 de la FISA o en el EO 12333.

256. La aplicación de estos programas supone intromisiones por parte de los servicios de inteligencia estadounidenses que, si procedieran de las autoridades de un Estado miembro, se calificarían como injerencias en el ejercicio del derecho al respeto de la vida privada garantizado en el artículo 7 de la Carta y en el artículo 8 del CEDH. Expone igualmente a los interesados al riesgo de que sus datos personales sufran tratamientos que no respeten los requisitos establecidos en el artículo 8 de la Carta. [120]

117 TEDH, sentencia de 19 de junio de 2018 (CE:ECHR:2018:0619JUD003525208; en lo sucesivo, «sentencia Centrüm för Rättvisa»).

118 TEDH, sentencia de 13 de septiembre de 2018 (CE:ECHR:2018:0913JUD005817013; en lo sucesivo, «sentencia Big Brother Watch»).

119 Véanse los asuntos citados en la nota a pie de página 98 de las presentes conclusiones, así como el asunto C-520/18, Ordre des barreaux francophones et germanophones y otros (DO 2018, C 408, p. 39).

120 Si bien un tratamiento puede infringir a la vez los artículos 7 y 8 de la Carta, el marco de análisis pertinente para aplicar el artículo 8 es estructuralmente diferente del relativo al artículo 7. El derecho a la protección de los datos personales implica, según el artículo 8, apartado 2, de la Carta que «estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley» y que «toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación». La vulneración de este derecho supone que unos datos personales sean objeto de un tratamiento efectuado ignorando estos requisitos. Así sucede, en particular, cuanto el tratamiento no se basa en el consentimiento del interesado, *ni en ningún otro fundamento legítimo previsto por la ley*. En tal situación, si bien la cuestión de la existencia de una injerencia y la de su justificación son conceptualmente distintas en el marco del artículo 7, se equiparan por lo que respecta al artículo 8 de la Carta.

257. De entrada, debo precisar que los derechos al respeto de la vida privada y a la protección de los datos personales incluyen la protección no solo del contenido de las comunicaciones sino también de los datos de tráfico [121] y de localización (denominados conjuntamente mediante el término «metadatos»). En efecto, tanto el Tribunal de Justicia como el TEDH han reconocido que los metadatos, al igual que los datos de contenido, pueden revelar información muy precisa sobre la vida privada de un individuo. [122]

258. Según la jurisprudencia del Tribunal de Justicia, para demostrar la existencia de una injerencia en el ejercicio del derecho garantizado en el artículo 7 de la Carta, carece de relevancia que los datos de que se trate tengan o no carácter sensible y que los interesados hayan sufrido o no inconvenientes en razón de la medida de vigilancia en cuestión. [123]

259. Una vez recordado este extremo, los programas de vigilancia basados en el artículo 702 de la FISA implican, en primer término, injerencias en el ejercicio de los derechos fundamentales de las personas cuyas comunicaciones respondan a los selectores escogidos por la NSA y, en consecuencia, sean transmitidas a esta por los proveedores de servicios de comunicaciones electrónicas. [124] Más concretamente, la obligación de los proveedores de *poner* los datos *a disposición* de la NSA, en la medida en que establece una excepción al principio de confidencialidad de las comunicaciones, [125] implica en sí misma una injerencia aun cuando las autoridades de inteligencia no consulten o utilicen posteriormente dichos datos. [126] La *conservación* y el *acceso* efectivos por parte de estas autoridades a los metadatos y al contenido de las comunicaciones puestas a su disposición, al igual que la *utilización* de esos datos, constituyen todas ellas injerencias adicionales. [127]

260. Es más, según las apreciaciones del órgano jurisdiccional remitente [128] y de otras fuentes como el Informe del PCLOB sobre los programas ejecutados en virtud del artículo 702 de la FISA puesto en conocimiento del Tribunal de Justicia por el Gobierno estadounidense, [129] en el marco del programa Upstream la NSA ya tiene *acceso para su filtrado* a grandes conjuntos («paquetes») de datos que forman parte de los flujos de comunicaciones que circulan por la «red troncal» de las telecomunicaciones y que incluyen comunicaciones que no contienen los selectores identificados por la NSA. Al parecer, la NSA solo puede examinar estos conjuntos de datos para determinar rápidamente, de manera automatizada, si contienen esos selectores. Según afirma dicho informe, únicamente las comunicaciones filtradas de este modo se almacenan posteriormente en las bases de datos de la NSA. En mi opinión, este acceso a los datos para su filtrado constituye también una injerencia en el ejercicio del derecho al respeto de la vida privada de los interesados, cualquiera que sea la utilización posterior de los datos retenidos. [130]

121 El artículo 2, párrafo segundo, letra b), de la Directiva 2002/58 define el concepto de «datos de tráfico» como «cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma».

122 Véanse la sentencia de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, en lo sucesivo, «sentencia Digital Rights Ireland», EU:C:2014:238), apartado 27, y la sentencia Tele2 Sverige, apartado 99. Véanse también TEDH, sentencias de 2 de agosto de 1984, Malone c. Reino Unido (CE:ECHR:1984:0802JUD000869179), § 84, y de 8 de febrero de 2018, Ben Faiza c. Francia (CE:ECHR:2018:0208JUD003144612), § 66.

123 Véanse la sentencia Digital Rights Ireland, apartado 33; el dictamen 1/15, apartado 124, y la sentencia Ministerio Fiscal, apartado 51.

124 Véanse los considerandos 78 a 81, así como el anexo VI, apartado II, de la Decisión sobre el «Escudo de la privacidad».

125 Véase, a este respecto, la sentencia Digital Rights Ireland, apartado 32.

126 Véase, en este sentido, el dictamen 1/15, apartados 124 y 125, del que se desprende que la comunicación de datos a un tercero constituye una injerencia en el ejercicio de los derechos fundamentales de los interesados, cualquiera que sea su utilización posterior.

127 Véanse, en este sentido, la sentencia Digital Rights Ireland, apartado 35; la sentencia Schrems, apartado 87, y el dictamen 1/15, apartados 123 a 126.

128 Véase el punto 60 de las presentes conclusiones.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2 de julio de 2014 (en lo sucesivo, «Informe del PCLOB», pp. 84 y 111). Véase también Grupo 29, EU-US Privacy Shield — First Annual Joint Review, 28 de noviembre de 2017, WP. 255 (letra B.1.1, p. 15).

130 Véase la nota a pie de página 126 de las presentes conclusiones.

261. Asimismo, la puesta a disposición y el filtrado de los datos en cuestión,[131] el acceso a estos datos por parte de los servicios de inteligencia, al igual que la conservación, el análisis y la utilización eventuales de dichos datos están comprendidos en el concepto de «tratamiento» en el sentido del artículo 4, apartado 2, del RGPD y del artículo 8, apartado 2, de la Carta. Por lo tanto, estos tratamientos deben cumplir los requisitos establecidos en esta última disposición.[132]

262. La vigilancia en virtud del EO 12333, por su parte, podría implicar el acceso directo, por parte de las autoridades de inteligencia, a los datos en tránsito, lo que supone una injerencia en el ejercicio del derecho garantizado en el artículo 8 del CEDH. A esta injerencia se añadiría la constituida por la posible utilización posterior de esos datos.

2) Sobre el carácter «establecido por la ley» de las injerencias

263. En virtud de la jurisprudencia del Tribunal de Justicia[133] y del TEDH,[134] el requisito de que toda injerencia en el ejercicio de los derechos fundamentales debe estar «establecida por la ley», en el sentido del artículo 52, apartado 1, de la Carta y del artículo 8, apartado 2, del CEDH, implica no solo que la medida que prevea la injerencia debe tener una base jurídica en el Derecho interno, sino también que dicha base jurídica debe presentar ciertas cualidades de accesibilidad y de previsibilidad de manera que se evite el riesgo de arbitrariedad.

264. A este respecto, las partes e interesados que han presentado observaciones al Tribunal de Justicia discrepan, esencialmente, sobre si el artículo 702 de la FISA y el EO 12333 cumplen el requisito relativo a la previsibilidad de la ley.

265. Este requisito, según lo interpretan el Tribunal de Justicia[135] y el TEDH,[136] exige que una normativa que constituya una injerencia en el ejercicio del derecho al respeto de la vida privada establezca reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas, de modo que se ofrezcan a los interesados garantías suficientes para proteger sus datos contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de estos. Tales normas deben, en particular, indicar en qué circunstancias y con arreglo a qué requisitos las autoridades públicas pueden conservar los datos personales, acceder a ellos y utilizarlos.[137] Además, la propia base jurídica que permite la injerencia debe definir el alcance de la limitación al ejercicio del derecho al respeto de la vida privada.[138]

131 Véase, a este respecto, el punto 222 de las presentes conclusiones.

132 Véase el dictamen 1/15, apartado 123 y jurisprudencia citada.

133 Véase, en particular, el dictamen 1/15, apartado 146.

134 Véanse, en particular, TEDH, sentencia de 2 de agosto de 1984, Malone c. Reino Unido (CE:ECHR:1984:0802JUD000869179), § 66; resolución de 29 de junio de 2006, Weber y Saravia c. Alemania (CE:ECHR:2006:0629DEC005493400; en lo sucesivo, «resolución Weber y Saravia»), § 84 y jurisprudencia citada, y sentencia de 4 de diciembre de 2015, Zakharov c. Rusia (CE:ECHR:2015:1204JUD004714306; en lo sucesivo, «sentencia Zakharov»), § 228.

135 Véanse, en particular, las sentencias Digital Rights Ireland, apartados 54 y 65; Schrems, apartado 91, y Tele2 Sverige, apartado 109, y el dictamen 1/15, apartado 141.

136 Véanse, en particular, la resolución Weber y Saravia (§§ 94 y 95); la sentencia Zakharov (§ 236), y TEDH, sentencia de 12 de enero de 2016, Szabó y Vissy c. Hungría (CE:ECHR:2016:0112JUD003713814; en lo sucesivo, «sentencia Szabó y Vissy»), § 59.

137 Véanse la sentencia Tele2 Sverige, apartado 117, y el dictamen 1/15, apartado 190. Véanse también, entre otras, TEDH, sentencias de 2 de agosto de 1984, Malone c. Reino Unido (CE:ECHR:1984:0802JUD000869179), § 67; Zakharov, § 229, y Szabó y Vissy, § 62. El TEDH precisa en estas sentencias que el requisito de la previsibilidad no tiene el mismo alcance en materia de interceptación de las comunicaciones que en otros ámbitos. En el contexto de las medidas de vigilancia secretas, «la exigencia de previsibilidad no puede significar que se deba permitir a un individuo que prevea si sus comunicaciones corren el riesgo de ser interceptadas por las autoridades y cuándo puede suceder esto, para que pueda regular su conducta en consecuencia».

138 Dictamen 1/15 (apartado 139). Véase también, en este sentido, TEDH, sentencia de 25 de marzo de 1983, Silver y otros c. Reino Unido (CE:ECHR:1983:0325JUD000594772), §§ 88 y 89.

266. Dudo, al igual que el Sr. Schrems y el EPIC, que el EO 12333, del mismo modo que la PPD 28, que establece garantías que acompañan a todas las actividades de inteligencia que versen sobre las transferencias de señales, [139] sean suficientemente previsibles para tener «rango de ley».

267. Estos instrumentos mencionan expresamente que no confieren derechos legalmente exigibles a los interesados. [140] Por consiguiente, estos últimos tampoco pueden invocar las garantías previstas por la PPD 28 ante los tribunales. [141] Asimismo, en la Decisión sobre el «Escudo de la privacidad» la Comisión consideró que las garantías establecidas en esta orden presidencial, si bien tienen arácter vinculante para los servicios de inteligencia, [142] «no se [formulan] en […] términos jurídicos». [143] El EO 12333 y la PPD 28 se parecen más a unas instrucciones administrativas internas que pueden ser revocadas o modificadas por el Presidente de los Estados Unidos. Pues bien, el TEDH ya ha declarado que las instrucciones administrativas internas no tienen rango de «ley». [144]

268. Por lo que respecta al artículo 702 de la FISA, el Sr. Schrems cuestiona el carácter previsible de esta disposición alegando que, a su entender, no limita la elección de los criterios de selección utilizados para filtrar los datos mediante garantías suficientes contra los riesgos de abuso. En la medida en que esta problemática también guarda relación con el carácter estrictamente necesario de las injerencias previstas en el artículo 702 de la FISA, la examinaré más adelante en mi exposición. [145]

269. La tercera cuestión prejudicial se solapa con la temática del respeto del requisito relativo al «rango de ley». Mediante esta cuestión, en esencia, el órgano jurisdiccional remitente trata de dilucidar si la adecuación del nivel de protección garantizado en un tercer país debe examinarse únicamente en relación con las normas jurídicamente vinculantes en vigor en ese tercer país y las prácticas que tienen por objeto garantizar su respeto, o bien también con los diversos instrumentos no vinculantes y mecanismos de control extrajudiciales que se aplican en este.

270. Al respecto, el artículo 45, apartado 2, letra a), del RGPD establece una lista no exhaustiva de circunstancias que la Comisión debe tener en cuenta para evaluar la adecuación del nivel de protección ofrecido por un tercer país. Entre estas circunstancias figuran la legislación aplicable y la manera en que se aplica. Esta disposición también menciona la influencia de otros tipos de normas, como las normas profesionales y las medidas de seguridad. Asimismo, exige que se tenga en cuenta 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». [146]

139 Los considerandos 69 a 77, así como el anexo VI, apartado I, de la Decisión sobre el «Escudo de la privacidad» contienen un resumen de la PPD 28. En ellos se especifica que esta orden presidencial se aplica tanto a las actividades de inteligencia basadas en el artículo 702 de la FISA como a las realizadas fuera del territorio de los Estados Unidos.

140 El apartado 3.7, letra c), del EO 12333 dispone: «this order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person». El artículo 6, letra d), de la PPD 28 establece también: «This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person».

141 Véase, en este sentido, CEPD, EU-US Privacy Shield — Second Annual Joint Review, de 22 de enero de 2019, apartado 99.

142 Véanse los considerandos 69 y 77 de la Decisión sobre el «Escudo de la privacidad».

143 Considerando 76 de la Decisión sobre el «Escudo de la privacidad».

144 Véase TEDH, sentencia de 25 de marzo de 1983, Silver y otros c. Reino Unido (CE:ECHR:1983:0325JUD000594772), §§ 26 y 86.

145 Véanse los puntos 295 a 301 de las presentes conclusiones. En la sentencia Tele2 Sverige, apartados 116 y 117, y el dictamen 1/15, apartados 140 y 141, el requisito de previsibilidad de la ley se presentó como intrínsecamente vinculado al requisito de necesidad y de proporcionalidad de la injerencia. De la misma manera, según la jurisprudencia del TEDH, la existencia de garantías efectivas frente a los riesgos de abuso está comprendida tanto en el requisito de «previsibilidad» de la injerencia como en el relativo a su carácter «necesario en una sociedad democrática», examinándose el respeto de estos dos requisitos de forma conjunta. Véanse, en particular, TEDH, sentencias de 18 de mayo de 2010, Kennedy c. Reino Unido (CE:ECHR:2010:0518JUD002683905), § 155; Zakharov, § 236; Centrüm för Rättvisa, § 107, y Big Brother Watch, § 322.

146 Véase también el considerando 104 del RGPD.

271. Leída en su conjunto y teniendo en cuenta el carácter no exhaustivo de la lista que contiene, en mi opinión dicha disposición implica que pueden tenerse en cuenta las prácticas o instrumentos no fundamentados en una base jurídica accesible y previsible en el marco de la evaluación de conjunto del nivel de protección garantizado por el tercer país en cuestión con el fin de corroborar unas garantías que a su vez tengan un fundamento jurídico con estas características. En cambio, tal como alegan en esencia el DPC, el Sr. Schrems, el Gobierno austriaco y el CEPD, las prácticas o instrumentos no pueden sustituir dichas garantías ni, por tanto, garantizar por sí mismos el nivel de protección exigido.

3) Sobre la inexistencia de un menoscabo del contenido esencial de los derechos fundamentales

272. El requisito, establecido en el artículo 52, apartado 1, de la Carta, según el cual cualquier limitación de los derechos y libertades garantizados por la Carta debe respetar el contenido esencial de estos implica que, cuando una injerencia atente contra tales derechos y libertades, ningún objetivo legítimo podrá justificarla. En ese caso, la injerencia se considera contraria a la Carta sin que deba examinarse si es adecuada para alcanzar el objetivo perseguido.

273. A este respecto, el Tribunal de Justicia ha declarado que una normativa nacional que autorice un acceso generalizado al *contenido* de las comunicaciones electrónicas por las autoridades públicas atenta contra la propia esencia del derecho al respeto de la vida privada garantizado en el artículo 7 de la Carta.[147] En cambio, aun señalando los riesgos asociados al acceso y al análisis de los *datos de tráfico y de localización*,[148] el Tribunal de Justicia consideró que el contenido esencial de este derecho no se ve afectado cuando una normativa nacional autoriza un acceso generalizado por parte de las autoridades estatales a dichos datos.[149]

274. A mi entender no puede considerarse que el artículo 702 de la FISA faculte a las autoridades de inteligencia estadounidenses a acceder de manera generalizada al contenido de las comunicaciones electrónicas.

275. En efecto, por una parte, el acceso a los datos por parte de las autoridades de inteligencia, con arreglo al artículo 702 de la FISA, *para su análisis y su utilización* eventuales, está limitado a los datos que cumplen los criterios de selección asociados a objetivos individuales.

276. Por otra parte, es cierto que el programa Upstream podría implicar un acceso generalizado al contenido de las comunicaciones electrónicas *con miras a su filtrado automatizado* en el supuesto de que se apliquen selectores no solo a los campos «de» y «a», sino también a la totalidad del contenido de los flujos de comunicaciones (búsqueda «relativa» al selector).[150] Sin embargo, como sostiene la

147 Véase la sentencia Schrems, apartado 94. Véanse también las sentencias Digital Rights Ireland, apartado 39, y Tele2 Sverige, apartado 101. Habida cuenta de la estrecha relación que existe entre los derechos al respeto a la vida privada y a la protección de los datos personales, una medida nacional que confiera a las autoridades públicas un acceso generalizado al contenido de las comunicaciones vulneraría también, a mi entender, el contenido esencial del derecho consagrado en el artículo 8 de la Carta.

148 Véase el punto 257 de las presentes conclusiones. En la sentencia Tele2 Sverige, apartado 99, el Tribunal de Justicia resaltó que los metadatos, en particular, proporcionan los medios para determinar el perfil de los interesados. En su dictamen 04/2014 sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional, de 10 de abril de 2014, WP. 215 (p. 5), el Grupo 29 observó que, debido a su naturaleza estructurada, los metadatos son más fáciles de concordar y analizar que los datos de contenido.

149 Véase la sentencia Tele2 Sverige, apartado 99. Algunos comentaristas se han planteado interrogantes sobre la procedencia de la distinción entre el acceso generalizado al contenido de las comunicaciones y el acceso generalizado a los metadatos, habida cuenta de la evolución de la tecnología y de los modos de comunicación. Véanse Falot, N. y Hijmans, H., «Tele2 de afweging tussen privacy en veiligheid nader omlijnd», *Nederlands Tijdschrift voor Europees Recht*, n.º 3, 2017 (p. 48), así como Ojanen, T., «Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter» (comentario a la sentencia Schrems), *European Constitutional Law Review*, 2016 (p. 5).

150 Véase la nota a pie de página 87 de la Decisión sobre el «Escudo de la privacidad». Sin embargo, según las observaciones del EPIC y la respuesta escrita del Gobierno estadounidense a las preguntas formuladas por el Tribunal de Justicia, en 2017 el FISC exigió la suspensión de las búsquedas «relativas» a un selector debido a irregularidades que habían afectado a las búsquedas de este tipo. No obstante, según dichas fuentes, en el acto de reautorización de la FISA adoptado en 2018, el Congreso previó la posibilidad de reintroducir este tipo de búsquedas con el consentimiento del FISC y del Congreso. Véase también CEPD, EU-US Privacy Shield — Second Annual Joint Review, 22 de enero de 2019 (p. 27, apartado 55).

Comisión y contrariamente a lo que alegan el Sr. Schrems y el EPIC, el acceso temporal de las autoridades de inteligencia a la totalidad del contenido de las comunicaciones electrónicas con el único fin de su filtrado mediante la aplicación de criterios de selección no puede asimilarse a un acceso generalizado a este contenido.[151] En mi opinión, la gravedad de la injerencia derivada de este acceso limitado en el tiempo con fines de filtrado automatizado no llega al punto de la de la injerencia que resulta de un acceso generalizado a este contenido por parte de las autoridades públicas con miras a su análisis y su posible utilización.[152] El acceso temporal con vistas al filtrado no permite a estas autoridades conservar los metadatos o el contenido de las comunicaciones que no respondan a los criterios de selección ni, en particular, como ha señalado el Gobierno estadounidense, determinar perfiles relativos a los individuos que no constituyan un objetivo de esos criterios.

277. Dicho esto, la cuestión de si el establecimiento de objetivos mediante selectores en el marco de los programas basados en el artículo 702 de la FISA limita de forma efectiva las facultades de las autoridades de inteligencia depende de la delimitación de la elección de los selectores.[153] El Sr. Schrems alega al respecto que, en ausencia de un control suficiente a tal efecto, el Derecho estadounidense no establece ninguna garantía contra un acceso generalizado al contenido de las comunicaciones ya en la fase del filtrado, de modo que atenta contra la propia esencia del derecho al respeto de la vida privada de los interesados.

278. Tal como expondré en mayor detalle a continuación,[154] me inclino a compartir estas dudas sobre el carácter suficiente de la delimitación de la elección de los selectores con el fin de cumplir los criterios de previsibilidad y proporcionalidad de las injerencias. Sin embargo, la existencia de esta delimitación, aunque sea imperfecta, se opone a la conclusión según la cual el artículo 702 de la FISA autoriza un acceso generalizado por parte de las autoridades públicas al contenido de las comunicaciones electrónicas y, por tanto, equivale a una vulneración de la propia esencia del derecho consagrado en el artículo 7 de la Carta.

279. También debo señalar que, en el dictamen 1/15, el Tribunal de Justicia consideró que el contenido esencial del derecho a la protección de los datos personales, garantizado en el artículo 8 de la Carta, está protegido cuando las finalidades del tratamiento están circunscritas y el tratamiento viene acompañado de normas destinadas a garantizar, entre otros aspectos, la seguridad, la confidencialidad y la integridad de esos datos, y a protegerlos contra los accesos y los tratamientos ilegales.[155]

280. En la Decisión sobre el «Escudo de la privacidad», la Comisión declaró que tanto el artículo 702 de la FISA como la PPD 28 delimitan las finalidades para las que pueden recogerse los datos en el marco de los programas aplicados en virtud del artículo 702 de la FISA.[156] La Comisión también señaló en dicha Decisión que la PPD 28 prevé normas que delimitan el acceso a los datos, así como

151 Desde esta perspectiva, el órgano jurisdiccional remitente, en los apartados 188 y 189 de su sentencia de primera instancia de 3 de octubre de 2017, distingue la búsqueda «en bloque» de la adquisición, la recogida o la retención «en bloque». En esencia, este órgano jurisdiccional considera que, si bien el Programa Upstream implica una búsqueda «en bloque» en el conjunto de los flujos de datos que circulan por la «red troncal» de las telecomunicaciones, la adquisición, recogida y retención son selectivas en el sentido de que solo tienen por objeto los datos que contienen los selectores en cuestión.

152 Véase, en este sentido, la sentencia de la Supreme Court (Tribunal Supremo) de 31 de mayo de 2019, apartados 11.2 y 11.3. Este órgano jurisdiccional señala en ella: «It is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term "processing" covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis.»

153 Véase el dictamen 1/15, apartado 122. Véase también el Informe de la Comisión Europea para la Democracia por el Derecho (Comisión de Venecia) sobre el control democrático de las agencias de recogida de inteligencia de señales, de 15 de diciembre de 2015, estudio n.º 719/2013 [CDL-AD(2015)011, p. 11]: «En la práctica, la cuestión de si este proceso limita adecuadamente las intrusiones superfluas en las comunicaciones personales inocentes supone determinar si el selector es suficientemente pertinente y específico y si la calidad del algoritmo del programa informático empleado para identificar los datos pertinentes en el marco de los parámetros escogidos es satisfactoria […]».

154 Véanse los puntos 297 a 301 de las presentes conclusiones.

155 Dictamen 1/15, apartado 150.

156 Véanse los considerandos 70, 103 y 109 de la Decisión sobre el «Escudo de la privacidad».

su almacenamiento y su difusión, para garantizar su seguridad y protegerlos contra los accesos no autorizados.[157] Como se mostrará en mi exposición a continuación,[158] albergo dudas, en particular, sobre si las finalidades de los tratamientos en cuestión están definidas con suficiente claridad y precisión para garantizar un nivel de protección sustancialmente equivalente al que existe en el ordenamiento jurídico de la Unión. Sin embargo, a mi entender, estas posibles deficiencias no bastan para permitir llegar a la conclusión de que, si se desplegaran en la Unión, semejantes programas vulnerarían el contenido esencial del derecho a la protección de los datos personales.

281. Asimismo, debo recordar que el carácter adecuado del nivel de protección garantizado en el marco de actividades de vigilancia con arreglo al EO 12333 debe evaluarse en relación con las disposiciones del CEDH. A este respecto, de la Decisión sobre el «Escudo de la privacidad» se desprende que las únicas restricciones que afectan a la aplicación de las medidas basadas en el EO 12333 para recopilar los datos relativos a personas no estadounidenses son las que establece la PPD 28.[159] Esta orden presidencial dispone que la utilización de la inteligencia exterior debe ser «lo más adaptada posible». No obstante, menciona expresamente la posibilidad de recoger datos «en bloque», fuera del territorio estadounidense, a los efectos de la persecución de determinados objetivos de seguridad nacional específicos.[160] A juicio del Sr. Schrems, las disposiciones de la PPD 28, que, por lo demás, no concede derechos a las personas físicas, no protegen a los interesados frente al riesgo de un acceso generalizado al contenido de sus comunicaciones electrónicas.

282. Al respecto, me limitaré a observar que, en su jurisprudencia relativa al artículo 8 del CEDH, el TEDH no ha empleado el concepto de vulneración del contenido esencial, o de la propia esencia, del derecho al respeto de la vida privada.[161] Hasta la fecha, este último tribunal no ha considerado que los regímenes que permiten la interceptación de las comunicaciones electrónicas, incluso de forma masiva, *excedan como tales del margen de apreciación de los Estados miembros*. El TEDH considera que tales regímenes son compatibles con el artículo 8, apartado 2, del CEDH siempre y cuando vengan acompañados de cierto número de garantías mínimas.[162] En estas circunstancias, no me parece apropiado concluir que un régimen de vigilancia como el previsto por el EO 12333 sobrepase el margen de apreciación de los Estados miembros sin realizar un cierto examen de las posibles garantías que van asociadas a este.

157 Véanse los considerandos 83 a 87, así como el anexo VI, apartado I, letra c), de la Decisión sobre el «Escudo de la privacidad». Debo señalar que, según el Informe del PCLOB (pp. 51 a 66), los procedimientos de «minimización» de la NSA con arreglo al artículo 702 de la FISA solo se refieren, en la mayor parte de sus aspectos, a las personas estadounidenses. La PPD 28 tenía por objeto ampliar las garantías aplicables a las personas no estadounidenses. Véase PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, disponible en la dirección de Internet https://www.pclob.gov/reports/report-PPD28/(p. 2). Dicho esto, el almacenamiento y la utilización de los datos con fines de seguridad nacional después de que hayan sido obtenidos por las autoridades públicas, en mi opinión, no están comprendidos en el ámbito de aplicación del Derecho de la Unión (véase el punto 226 de las presentes conclusiones). Por lo tanto, la adecuación del nivel de protección garantizado en el marco de estas actividades debe apreciarse en relación con el artículo 8 del CEDH.

158 Véanse los puntos 283 a 289 de las presentes conclusiones.

159 En particular, en el considerando 127 de la Decisión sobre el «Escudo de la privacidad», la Comisión declaró que la Cuarta Enmienda de la Constitución de los Estados Unidos no se extiende a los ciudadanos no estadounidenses.

160 Véanse los considerandos 73 y 74, así como el anexo VI, apartado I, letra b), de la Decisión sobre el «Escudo de la privacidad». Estos objetivos incluyen la lucha contra el espionaje y contra otras amenazas y actividades dirigidas por poderes extranjeros contra los Estados Unidos y sus intereses; contra las amenazas terroristas; contra las amenazas derivadas del desarrollo, la posesión, la proliferación o la utilización de armas de destrucción masiva; contra las amenazas relacionadas con la ciberseguridad; contra las amenazas a las fuerzas armadas de los Estados Unidos o de sus aliados y contra las amenazas de la criminalidad transnacional. A tenor de la nota a pie de página 5 de la PPD 28, la limitación de los objetivos que justifican la utilización de los datos recogidos «en bloque» no se aplica cuando tal recogida es solo temporal y está destinada a facilitar una recogida selectiva.

161 Aunque las disposiciones del CEDH no mencionan el «contenido esencial» de los derechos fundamentales, en la jurisprudencia del TEDH relativa a algunas de estas disposiciones aparece el concepto equivalente de la «propia esencia» de un derecho fundamental. Véanse, en lo referente a la propia esencia del derecho a un proceso equitativo garantizado en el artículo 6 del CEDH, en particular, TEDH, sentencias de 25 de mayo de 1985, Ashingdane c. Reino Unido (CE:ECHR:1985:0528JUD000822578), §§ 57 y 59; de 21 de diciembre de 2000, Heaney and McGuinness c. Irlanda (CE:ECHR:2000:1221JUD003472097), §§ 55 y 58, y de 23 de junio de 2016, Baka c. Hungría (CE:ECHR:2016:0623JUD002026112), § 121. En lo tocante a la propia esencia del derecho a contraer matrimonio consagrado en el artículo 12 del CEDH, véase TEDH, sentencia de 11 de julio de 2002, Christine Goodwin c. Reino Unido (CE:ECHR:2002:0711JUD002895795), §§ 99 y 101. Por lo que respecta a la propia esencia del derecho a la educación garantizado en el artículo 2 del Protocolo n.º 1 al CEDH, véase TEDH, sentencia de 23 de julio de 1968, asunto «relativo a determinados aspectos del régimen lingüístico de la enseñanza en Bélgica» (CE:ECHR:1968:0723JUD000147462), § 5.

162 Véanse, en particular, las sentencias Centrüm för Rättvisa, §§ 112 a 114 y jurisprudencia citada, y Big Brother Watch, § 337.

4) Sobre la persecución de un objetivo legítimo

283. Según el artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos que consagra debe responder efectivamente a un objetivo de interés general reconocido por la Unión. El artículo 8, apartado 2, de la Carta dispone también que cualquier tratamiento de datos personales que no se base en el consentimiento del interesado deberá basarse en un «fundamento legítimo previsto por la ley». Por su parte, el artículo 8, apartado 2, del CEDH enumera los fines que permiten justificar una injerencia en el ejercicio del derecho al respeto de la vida privada.

284. En virtud de la Decisión sobre el «Escudo de la privacidad», la adhesión a los principios que establece puede limitarse con el fin de cumplir obligaciones relativas a la seguridad nacional, al interés público y al cumplimiento de la ley.[163] Los considerandos 67 a 124 de esta Decisión examinan más concretamente las limitaciones derivadas del acceso a los datos y de su utilización por las autoridades públicas estadounidenses a efectos de la seguridad nacional.

285. Se admite generalmente que la protección de la seguridad nacional constituye un objetivo legítimo que puede justificar excepciones a las exigencias derivadas del RGPD,[164] así como a los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta,[165] al igual que en el artículo 8, apartado 2, del CEDH. Sin embargo, el Sr. Schrems, el Gobierno austriaco y el EPIC han señalado que los objetivos perseguidos en el marco de los programas de vigilancia basados en el artículo 702 de la FISA y en el EO 12333 exceden de la mera seguridad nacional. En efecto, estos instrumentos tienen por objeto la obtención de «inteligencia exterior», un concepto que abarca diversos tipos de información que incluyen la relativa a la seguridad nacional sin necesariamente limitarse a esta.[166] Así, están comprendidos en el concepto de «inteligencia exterior», en el sentido del artículo 702 de la FISA, los datos relativos a la administración de los asuntos exteriores del país.[167] El EO 12333, por su parte, define este concepto en el sentido de que comprende la información relativa a las capacidades, intenciones o actividades de los gobiernos extranjeros, las organizaciones extranjeras y las personas extranjeras.[168] El Sr. Schrems cuestiona la legitimidad del objetivo al que se hace referencia de este modo en la medida en que excede de la seguridad nacional.

286. En mi opinión, el ámbito de la seguridad nacional puede incluir, en cierta medida, la protección de intereses relativos a la administración de los asuntos exteriores.[169] Asimismo, no es descartable que algunas de las finalidades distintas de la protección de la seguridad nacional que engloba el concepto de «inteligencia exterior», según se define en el artículo 702 de la FISA y en el EO 12333, se correspondan con objetivos importantes de interés público que permitan justificar una injerencia en

163 Véase el punto 197 de las presentes conclusiones.

164 Véase el artículo 23, apartado 1, letra a), del RGPD.

165 Véase la sentencia Schrems, apartado 88. El Tribunal de Justicia ha considerado el concepto relacionado de «seguridad pública», en el sentido de las disposiciones del TFUE que autorizan excepciones a las libertades fundamentales que garantiza, como un concepto autónomo del Derecho de la Unión que comprende la seguridad tanto interior como exterior de los Estados miembros [véanse, en particular, las sentencias de 26 de octubre de 1999, Sirdar (C-273/97, EU:C:1999:523), apartado 17, y de 13 de septiembre de 2016, CS (C-304/14, EU:C:2016:674), apartado 39 y jurisprudencia citada]. Mientras que la seguridad interior puede verse afectada, en particular, por una amenaza directa a la tranquilidad y la seguridad física de la población del Estado miembro de que se trate, la seguridad exterior puede verse amenazada, en particular, por el riesgo de una perturbación grave de las relaciones exteriores o de la coexistencia pacífica de los pueblos. Si bien no puede determinar unilateralmente el contenido de estos conceptos, cada Estado miembro dispone de un cierto margen de apreciación para definir sus intereses esenciales en cuanto a la seguridad. Véase, en particular, la sentencia de 2 de mayo de 2018, K. y H. F. (Derecho de residencia y alegaciones de crímenes de guerra) (C-331/16 y C-366/16, EU:C:2018:296), apartados 40 a 42 y jurisprudencia citada. En mi opinión, estas consideraciones son extrapolables a la interpretación del concepto de «seguridad nacional» como un interés cuya protección puede justificar restricciones de las disposiciones del RGPD y de los derechos garantizados en los artículos 7 y 8 de la Carta.

166 Véanse, a este respecto, el considerando 89 y la nota a pie de página 97 de la Decisión sobre el «Escudo de la privacidad».

167 Véase el punto 55 de las presentes conclusiones.

168 Véase el punto 61 de las presentes conclusiones.

169 En la sentencia Centrüm för Rättvisa, § 111, el TEDH declaró que las actividades de vigilancia que tenían por objeto apoyar la política exterior, la política de defensa y la política de seguridad de Suecia, así como detectar las amenazas exteriores organizadas en Suecia, perseguían objetivos legítimos relativos a la seguridad nacional.

los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales. Estos objetivos tendrían menos relevancia que la salvaguardia de la seguridad nacional en el marco de una ponderación entre los derechos fundamentales de los interesados y el fin que persigue la injerencia. [170]

287. Sin embargo, con arreglo al artículo 52, apartado 1, de la Carta, también es preciso que mediante las medidas que establecen las injerencias en cuestión se persiga efectivamente la seguridad nacional u otro objetivo legítimo. [171] Asimismo, las finalidades de las injerencias deben definirse de manera que cumplan los requisitos de claridad y precisión. [172]

288. Pues bien, según el Sr. Schrems, la finalidad de las medidas de vigilancia previstas en el artículo 702 de la FISA y en el EO 12333 no se establece con una precisión suficiente para cumplir las garantías de previsibilidad y proporcionalidad. Así sucede, en particular, en la medida en que esos instrumentos definen el concepto de «inteligencia exterior» de un modo particularmente amplio. Además, la Comisión dejó constancia en el considerando 109 de la Decisión sobre el «Escudo de la privacidad» de que el artículo 702 de la FISA exige que la recogida de información en materia de inteligencia exterior constituya «uno de los principales fines» de la recopilación, formulación que no excluye, a primera vista y como ha señalado el EPIC, que se persigan otros objetivos no determinados.

289. Por estas razones, sin que pueda excluirse que las medidas de vigilancia con arreglo al artículo 702 de la FISA o al EO 12333 respondan a objetivos legítimos, cabe preguntarse si estos se definen de forma suficientemente clara y precisa para evitar el riesgo de abuso y para permitir el control de la proporcionalidad de las injerencias que se derivan de ello. [173]

5) Sobre el carácter necesario y proporcionado de las injerencias

290. El Tribunal de Justicia ha señalado de forma reiterada que los derechos consagrados en los artículos 7 y 8 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. [174] Como destacó Facebook Ireland, entre estos otros derechos figura el derecho a la seguridad garantizado en el artículo 6 de la Carta.

291. A este respecto, según una jurisprudencia también consolidada, toda injerencia en el ejercicio de los derechos garantizados en los artículos 7 y 8 de la Carta debe ser objeto de un control estricto de proporcionalidad. [175]

170 Véanse, a este respecto, las sentencias Tele2 Sverige, apartado 115, y Ministerio Fiscal, apartado 55. El Tribunal de Justicia destacó en ellas la relación entre la gravedad de una injerencia y la del interés invocado para justificarla.

171 El Grupo 29, en su Documento de Trabajo sobre la vigilancia de las comunicaciones electrónicas a efectos de inteligencia y seguridad nacional, de 5 de diciembre de 2014, WP. 228 (p. 27), ha insistido en la importancia de evaluar de forma crítica si la vigilancia se realiza efectivamente con fines de seguridad nacional.

172 Véase el dictamen 1/15, apartado 181, en el que el Tribunal de Justicia declaró que el tenor literal de las disposiciones legislativas que preveían las injerencias no cumplía los requisitos de claridad y precisión, de manera que dichas injerencias no estaban limitadas a lo estrictamente necesario. Desde este mismo punto de vista, el Abogado General Bot consideró, en sus conclusiones presentadas en el asunto Schrems (C-362/14, EU:C:2015:627), puntos 181 a 184, que los objetivos de las medidas de vigilancia estaban formulados de forma demasiado general para ser considerados objetivos de interés general, salvo en lo tocante a la seguridad nacional.

173 El SEPD expresó dudas similares en su dictamen 4/2016 relativo al «Escudo de la privacidad UE-EE. UU.» (Privacy Shield) — Proyecto de decisión de adecuación, de 30 de mayo de 2016 (p. 8).

174 Véanse la sentencia 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; el dictamen 1/15, apartado 136, y la sentencia de 24 de septiembre de 2019, Google (Alcance territorial del derecho a la retirada de enlaces) (C-507/17, EU:C:2019:772), apartado 60.

175 Véanse, en particular, las sentencias de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia (C-73/07, EU:C:2008:727), apartado 56; Digital Rights Ireland, apartados 48 y 52; Schrems, apartados 78 y 92, y el dictamen 1/15, apartados 139 y 140. Véase también el considerando 140 de la Decisión sobre el «Escudo de la privacidad».

292. En particular, de la sentencia Schrems se desprende que «no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos […] sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización». [176]

293. El Tribunal de Justicia también ha declarado que, salvo en casos de urgencia debidamente justificados, el acceso debe estar sujeto a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo que sea estrictamente necesario para la realización del objetivo perseguido. [177]

294. El artículo 23, apartado 2, del RGPD establece actualmente una serie de garantías que un Estado miembro debe prever cuando establezca excepciones a las disposiciones de este Reglamento. La normativa que permite tal excepción debe contener disposiciones relativas, en particular, a la finalidad del tratamiento, al alcance de la excepción, a las garantías para prevenir los abusos, a los plazos de conservación, así como al derecho de los interesados de ser informados sobre la excepción, salvo si puede ser perjudicial a los fines de esta.

295. En el presente asunto, el Sr. Schrems sostiene que el artículo 702 de la FISA no incluye garantías suficientes contra los riesgos de abuso y de acceso ilícito a los datos. En particular, a su entender, la elección de los criterios de selección no está suficientemente delimitada, de manera que esta disposición no ofrece garantías contra un acceso generalizado al contenido de las comunicaciones.

296. Por el contrario, el Gobierno estadounidense y la Comisión alegan que el artículo 702 de la FISA limita mediante criterios objetivos la elección de los selectores, dado que esta disposición permite únicamente la recogida de los datos de comunicaciones electrónicas de personas no estadounidenses situadas fuera de los Estados Unidos con el fin de obtener información en materia de inteligencia exterior.

297. En mi opinión, cabe dudar del carácter suficientemente claro y preciso de estos criterios, así como de la existencia de garantías suficientes para prevenir los riesgos de abusos.

298. En primer lugar, el considerando 109 de la Decisión sobre el «Escudo de la privacidad» indica que ni el FISC ni ningún otro órgano judicial o administrativo independiente aprueban los selectores de forma individual con carácter previo a su aplicación. La Comisión hizo constar en dicho considerando que «el FISC no autoriza medidas de vigilancia individuales, sino programas de vigilancia […] sobre la base de certificaciones anuales», extremo que confirmó el Gobierno estadounidense ante el Tribunal de Justicia. Este considerando precisa que «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» que puedan recogerse. La Comisión señala en dicho considerando que «el FISC no valora —sobre la base de la existencia de indicios razonables o de cualquier otra norma— si los objetivos fijados son adecuados para recabar información de inteligencia exterior», si bien controla la condición de que «uno de los principales fines de la recopilación de datos sea obtener ese tipo de información».

299. En segundo lugar, con arreglo a dicho considerando, el artículo 702 de la FISA permite a la NSA recabar comunicaciones «únicamente cuando existan motivos fundados para pensar que un determinado medio de comunicación está siendo utilizado para transmitir información de inteligencia exterior». El considerando 70 de la Decisión sobre el «Escudo de la privacidad» añade que la

176 Sentencia Schrems (apartado 93). Véase también, en este sentido, la sentencia Digital Rights Ireland (apartado 60).

177 Véanse la sentencia Tele2 Sverige, apartado 120, y el dictamen 1/15, apartado 202.

determinación de los selectores se desarrolla a la luz del Marco de Prioridades de Inteligencia Nacional (National Intelligence Priorities Framework, NIPF). Esta Decisión no menciona requisitos de motivación o justificación más precisos de la determinación de los selectores en virtud de estas prioridades administrativas que deba cumplir la NSA. [178]

300. Por último, el considerando 71 de la Decisión sobre el «Escudo de la privacidad» hace referencia al requisito, previsto en la PPD 28, según el cual la recopilación de inteligencia exterior debe ser «lo más adaptada posible». Aparte del hecho de que esta orden presidencial no otorga derechos a las personas físicas, no me parece en absoluto evidente la equivalencia sustancial entre el criterio de una actividad «lo más adaptada posible» y el de la «estricta necesidad» que impone el artículo 52, apartado 1, de la Carta para justificar una injerencia en el ejercicio de los derechos garantizados en sus artículos 7 y 8. [179]

301. A la vista de estas consideraciones, no está claro que, sobre la base de los elementos expuestos en la Decisión sobre el «Escudo de la privacidad», las medidas de vigilancia basadas en el artículo 702 de la FISA vengan acompañadas de garantías, relativas a la limitación de las personas que pueden ser objeto de una medida de vigilancia y de los objetivos para los que se pueden recopilar datos, que sean sustancialmente equivalentes a las que se exigen en virtud del RGPD, interpretado a la luz de los artículos 7 y 8 de la Carta. [180]

302. Asimismo, en lo referente a la evaluación del carácter adecuado del nivel de protección que rodea a la vigilancia en virtud del EO 12333, el TEDH reconoce a los Estados miembros un amplio margen de apreciación para elegir los medios para proteger su seguridad nacional, si bien dicho margen está limitado por el requisito de que se establezcan garantías adecuadas y suficientes contra los abusos. [181] En su jurisprudencia relativa a las medidas de vigilancia secreta, el TEDH comprueba si el Derecho interno en el que se basan estas medidas contiene garantías y salvaguardias suficientes que permitan cumplir los requisitos de «previsibilidad» y de «necesidad en una sociedad democrática». [182]

303. A este respecto, el TEDH establece un cierto número de garantías mínimas. Estas garantías se refieren a la indicación clara de la naturaleza de las infracciones que pueden dar lugar a una orden de interceptación, la definición de las categorías de personas cuyas comunicaciones pueden ser interceptadas, la fijación de un límite a la duración de la ejecución de la medida, el procedimiento que debe seguirse para el análisis, la utilización y la conservación de los datos recogidos, las precauciones que se deben tomar para la comunicación de los datos a otras partes y las circunstancias en las que se puede o se debe proceder al borrado o la destrucción de las grabaciones. [183]

178 El Informe del PCLOB (p. 45) especifica: «With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to "identify" the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification.»

179 Véanse, en este sentido, Grupo 29, Opinion 1/2016 on the EU-US Privacy Shield draft adequacy decision, 13 de abril de 2016, WP. 238 (apartado 3.3.1, p. 38); la Resolución del Parlamento de 6 de abril de 2017 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., P. 8_TA(2017)0131 (apartado 17), así como el Informe del Parlamento sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, de 20 de febrero de 2017, A8-0044/2017 (apartado 17).

180 Véanse, en este sentido, Grupo 29, EU-US Privacy Shield — First Annual Joint Review, 28 de noviembre de 2017, WP. 255 (p. 3); la Resolución del Parlamento Europeo de 5 de julio de 2018 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., P. 8_TA(2018)0315 (apartado 22), y CEPD, EU-US Privacy Shield — Second Annual Joint Review, 22 de enero de 2019 (apartados 81 a 83 y 87).

181 Véanse, en particular, las sentencias Zakharov, § 232, y Szabó y Vissy, § 57.

182 Véanse, en particular, las sentencias Zakharov, § 237; Centrüm för Rättvisa, § 111, y Big Brother Watch, § 322.

183 Véanse, en particular, la resolución Weber y Saravia, § 95; TEDH, sentencia de 28 de junio de 2007, Association pour l'intégration européenne et les droits de l'homme y Ekimdjiev (CE:ECHR:2007:0628JUD006254000), § 76, y la sentencia Zakharov, § 231.

304. El carácter adecuado y efectivo de las garantías que delimitan la injerencia depende de todas las circunstancias del caso, incluyendo la naturaleza, el alcance y la duración de las medidas, las razones que se exigen para ordenarlas, las autoridades competentes para permitirlas, ejecutarlas y controlarlas y el tipo de recursos que ofrece el Derecho interno.[184]

305. En particular, para evaluar la justificación de una medida de vigilancia secreta, el TEDH tiene en cuenta el conjunto de los controles efectuados «cuando se ordena», «mientras se ejecuta» y «después de su cese».[185] Por lo que respecta a la primera de estas fases, el TEDH exige que tal medida sea autorizada por un organismo independiente. Aunque, a juicio del Tribunal, el Poder Judicial ofrece las mejores garantías de independencia, imparcialidad y regularidad del procedimiento, el organismo en cuestión no debe pertenecer necesariamente a la judicatura.[186] Un control judicial en profundidad efectuado en una fase posterior puede compensar los posibles defectos del procedimiento de autorización.[187]

306. En el presente caso, de la Decisión sobre el «Escudo de la privacidad» se desprende que las únicas garantías que limitan la recogida y el uso de datos fuera del territorio de los Estados Unidos figuran en la PPD 28, ya que el artículo 702 de la FISA no se aplica fuera de dicho territorio. No estoy convencido de que estas garantías puedan bastar para cumplir los requisitos de «previsibilidad» y de «necesidad en una sociedad democrática».

307. En primer lugar, ya he señalado que esta orden presidencial no otorga derechos a las personas físicas. En segundo lugar, dudo que el requisito de garantizar una vigilancia «lo más adaptada posible» esté formulado en términos suficientemente claros y precisos para proteger adecuadamente a los interesados frente a los riesgos de abuso.[188] Por último, la Decisión sobre el «Escudo de la privacidad» no establece que la vigilancia basada en el EO 12333 esté sujeta a un control previo por un organismo independiente o que pueda ser objeto de un control judicial *a posteriori*.[189]

308. En estas condiciones, albergo dudas sobre la procedencia de la conclusión según la cual los Estados Unidos garantizan, en el marco de las actividades de sus servicios de inteligencia con arreglo al artículo 702 de la FISA y al EO 12333, un nivel adecuado de protección en el sentido del artículo 45, apartado 1, del RGPD, interpretado a la luz de los artículos 7 y 8 de la Carta y del artículo 8 del CEDH.

c) Sobre la validez de la Decisión sobre el «Escudo de la privacidad» en relación con el derecho a la tutela judicial efectiva

309. Mediante la quinta cuestión prejudicial se solicita al Tribunal de Justicia que determine si las personas cuyos datos se transfieren a los Estados Unidos disfrutan en dicho país de una protección jurisdiccional sustancialmente equivalente a la que se debe garantizar en la Unión con arreglo al artículo 47 de la Carta. Mediante su décima cuestión prejudicial, el órgano jurisdiccional remitente le pregunta, en esencia, si la quinta cuestión prejudicial debe responderse en sentido afirmativo, habida cuenta de la introducción de la figura del Defensor del Pueblo en la Decisión sobre el «Escudo de la privacidad».

184 Véanse, en particular, la resolución Weber y Saravia, § 106; la sentencia Zakharov, § 232, y la sentencia Centrüm för Rättvisa, § 104.

185 Véanse, en particular, TEDH, sentencias de 6 de septiembre de 1978, Klass y otros c. Alemania (CE:ECHR:1978:0906JUD000502971), § 55; Zakharov, (§ 233), y Centrüm för Rättvisa, § 105.

186 Véanse, en particular, la sentencia Klass, § 56; TEDH, sentencia de 18 de mayo de 2010, Kennedy c. Reino Unido (CE:ECHR:2010:0518JUD002683905), § 167, y la sentencia Zakharov, §§ 233 y 258.

187 Véanse las sentencias Szabó y Vissy, § 77, y Centrüm för Rättvisa, § 133.

188 Esto es cierto, con mayor motivo, a la vista de las consideraciones expuestas en el punto 281 de las presentes conclusiones.

189 Véanse los puntos 330 y 331 de las presentes conclusiones.

310. De entrada, quisiera señalar que, en el considerando 115 de esta Decisión, la Comisión reconoce que el ordenamiento jurídico estadounidense presenta lagunas en la protección jurisdiccional de las personas físicas.

311. A tenor de este considerando, en primer término, «no están cubiertas todas las bases jurídicas que pueden invocar los servicios de inteligencia estadounidenses (por ejemplo, el EO 12333)» por las posibilidades de recurso jurisdiccional. En efecto, el EO 12333 y la PPD 28 no confieren derechos a los interesados y estos no pueden invocarlos ante los tribunales. Pues bien, la tutela judicial efectiva presupone, como mínimo, que los particulares tengan derechos que puedan invocarse ante la justicia.

312. En segundo término, «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 […] se declararán improcedentes cuando [estos] no puedan demostrar su legitimación, lo que restringe el acceso a los órganos jurisdiccionales ordinarios».

313. De los considerandos 116 a 124 de la Decisión sobre el «Escudo de la privacidad» se desprende que la creación del Defensor del Pueblo pretende compensar estas limitaciones. La Comisión concluye, en el considerando 139 de dicha Decisión, que «*en su conjunto*, los mecanismos de *recurso* y *supervisión* previstos por el Escudo de la privacidad […] ofrecen al interesado la posibilidad de ejercer acciones en Derecho para acceder a los datos personales que le conciernen y, en último término, obtener su rectificación o supresión» (el subrayado es mío).

314. Teniendo en cuenta los principios generales desarrollados por la jurisprudencia del Tribunal de Justicia y del TEDH relativa al derecho de recurso contra las medidas de vigilancia de las comunicaciones, examinaré si los recursos judiciales previstos en el Derecho estadounidense, tal como se describen en la Decisión sobre el «Escudo de la privacidad», permiten garantizar una protección jurisdiccional adecuada de los interesados [sección 1)]. A continuación, determinaré si la introducción del mecanismo extrajudicial del Defensor del Pueblo permite, en su caso, colmar las posibles lagunas que presenta la protección jurisdiccional de estas personas [sección 2)].

1) Sobre la efectividad de los recursos judiciales previstos en el Derecho estadounidense

315. En primer lugar, el artículo 47, párrafo primero, de la Carta consagra el derecho a la tutela judicial efectiva de toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados.[190] A tenor del párrafo segundo de este artículo, toda persona tiene derecho a que su causa sea oída por un juez independiente e imparcial.[191] El acceso a un tribunal independiente está comprendido en el contenido esencial del derecho garantizado en el artículo 47 de la Carta.[192]

190 A este respecto, las Explicaciones sobre la Carta establecen que «en el Derecho de la Unión la protección [prevista en el artículo 47 de esta] es más amplia [que la conferida por el artículo 13 del CEDH], ya que garantiza un derecho a un recurso efectivo ante un juez». Véanse también las conclusiones del Abogado General Wathelet presentadas en el asunto Berlioz Investment Fund (C-682/15, EU:C:2017:2), punto 37.

191 Para dilucidar si nos encontramos ante un «órgano jurisdiccional» en el marco de la aplicación del artículo 47 de la Carta deben tomarse en consideración su origen legal, el carácter permanente del mismo, la obligatoriedad de su jurisdicción, la naturaleza contradictoria del procedimiento y la aplicación de normas jurídicas por parte del órgano, así como la independencia de este. Véase la sentencia de 27 de febrero de 2018, Associação Sindical dos Juízes Portugueses (C-64/16, EU:C:2018:117), apartado 38 y jurisprudencia citada.

192 Véanse, entre otras, las sentencias de 25 de julio de 2018, Minister for Justice and Equality (Deficiencias del sistema judicial) (C-216/18 PPU, EU:C:2018:586), apartados 59 y 63; de 5 de noviembre de 2019, Comisión/Polonia (Independencia de los tribunales ordinarios) (C-192/18, EU:C:2019:924), apartado 106, y de 19 de noviembre de 2019, A. K. y otros (Independencia de la Sala Disciplinaria del Tribunal Supremo) (C-585/18, C-624/18 y C-625/18, EU:C:2019:982), apartado 120.

316. Este derecho a la protección jurisdiccional individual se añade a la obligación, que recae sobre los Estados miembros en virtud de los artículos 7 y 8 de la Carta, de someter cualquier medida de vigilancia, salvo en casos de urgencia debidamente justificados, a un control previo de un tribunal o de una autoridad administrativa independiente. [193]

317. Es innegable, tal como han alegado los Gobiernos alemán y francés, que el derecho a la tutela judicial efectiva no constituye una garantía absoluta, [194] ya que este derecho puede limitarse por razones de seguridad nacional. Sin embargo, solo se autorizan excepciones en la medida en que no menoscaben su contenido esencial y en que sean estrictamente necesarias para la consecución de un objetivo legítimo.

318. A este respecto, el Tribunal de Justicia declaró, en la sentencia Schrems, que una normativa que no prevea *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 consagrado en el artículo 47 de la Carta. [195]

319. Debo destacar que este derecho de acceso implica la posibilidad de que una persona obtenga de las autoridades públicas, sin perjuicio de las excepciones estrictamente necesarias para la búsqueda de un interés legítimo, *la confirmación del hecho de que tratan o no datos personales que le conciernan*. [196] Este es, en mi opinión, el alcance práctico del derecho de acceso cuando la persona interesada ignora si las autoridades públicas han conservado datos personales referidos a ella sobre todo después de un proceso de filtrado automatizado de los flujos de comunicaciones electrónicas.

320. Asimismo, de la jurisprudencia se desprende que, en principio, las autoridades de un Estado miembro están obligadas a notificar el acceso a los datos *siempre que la notificación ya no pueda comprometer las investigaciones que llevan a cabo*. [197] En efecto, tal notificación constituye un requisito previo para el ejercicio del derecho de recurso con arreglo al artículo 47 de la Carta. [198] Esta obligación se recoge actualmente en el artículo 23, apartado 2, letra h), del RGPD.

193 Véase el punto 293 de las presentes conclusiones. El artículo 45, apartado 3, letra a), del RGPD prevé que, en la evaluación de la adecuación del nivel de protección proporcionado por un tercer Estado, se tendrán en cuenta los «recursos administrativos y *acciones judiciales*» que los interesados puedan interponer de forma efectiva (el subrayado es mío). De la misma manera, según el considerando 104 del RGPD, la adopción de una decisión de adecuación debe supeditarse a la condición de que se reconozca a los interesados, en el tercer país de que se trata, «acciones administrativas *y judiciales* efectivas» (el subrayado es mío). Véanse también Grupo 29, EU-U.S. Privacy Shield — First Annual Joint Review, 28 de noviembre de 2017, WP. 255 (apartado B.3); la Resolución del Parlamento de 5 de julio de 2018 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., P. 8_TA(2018)0315 (apartados 25 y 30), y CEPD, EU-US Privacy Shield — Second Annual Joint Review, 22 de enero de 2019 (apartados 94 a 97).

194 Véase, en este sentido, la sentencia de 28 de febrero de 2013, Reexamen Arango Jaramillo y otros/BEI (C-334/12 RX-II, EU:C:2013:134), apartado 43.

195 Sentencia Schrems, apartado 95.

196 El artículo 15 del RGPD, titulado «Derecho de acceso del interesado», dispone, en su apartado 1, que dicho interesado «tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales». El «principio de acceso» establecido en el anexo II, apartado II.8, letra a), de la Decisión sobre el «Escudo de la privacidad» tiene el mismo significado.

197 Sentencia Tele2 Sverige, apartado 121, y dictamen 1/15, apartado 220. Como ha señalado Facebook Ireland, por tanto, la notificación del acceso de las autoridades a los datos no puede exigirse de forma sistemática. A este respecto, el TEDH ha considerado que «puede que en la práctica no sea posible exigir una notificación *a posteriori*», en la medida en que la amenaza que es objeto de las medidas de vigilancia «puede subsistir durante años, incluso décadas» tras el levantamiento de estas medidas, de forma que la notificación puede «comprometer el objetivo a largo plazo que motivó en origen la vigilancia», así como «revelar los métodos de trabajo de los servicios de inteligencia, sus ámbitos de actividad y […] la identidad de sus agentes» [sentencia Zakharov, § 287 y jurisprudencia citada]. En ausencia de una notificación, aunque por ello resulte imposible utilizar las vías de recurso individuales, otras garantías pueden bastar para proteger el derecho al respeto de la vida privada en caso de violación de las exigencias legales (véase también la sentencia Centrüm för Rättvisa, §§ 164 a 167 y 171 a 178). Véase el punto 330 de las presentes conclusiones.

198 Véase, a este respecto, la nota a pie de página 210 de las presentes conclusiones.

321. Los considerandos 111 a 135 de la Decisión sobre el «Escudo de la privacidad» exponen de forma sucinta todas las vías de recurso a disposición de las personas cuyos datos se transfieran cuando teman que dichos datos hayan sido tratados por los servicios de inteligencia estadounidenses después de la transferencia. Estas vías de recurso también se describieron en la sentencia de primera instancia de la High Court (Tribunal Superior) de 3 de octubre de 2017, así como en las observaciones, en particular, del Gobierno estadounidense.

322. No es necesario recordar en detalle el tenor de estas exposiciones. En efecto, el órgano jurisdiccional remitente cuestiona la adecuación de las garantías relativas a la protección jurídica de los interesados alegando que, en esencia, los requisitos particularmente estrictos en materia de legitimación activa (*standing*),[199] combinados con la ausencia de una obligación de notificación a las personas que hayan sido objeto de una medida de vigilancia *aun cuando la notificación ya no ponga en peligro los objetivos*, hacen que, en la práctica, resulte exageradamente difícil hacer uso de las vías de recurso previstas en el Derecho estadounidense. El DPC, el Sr. Schrems, los Gobiernos austriaco, polaco y portugués y el CEPD comparten estas dudas.[200]

323. A este respecto, me limitaré a recordar que las normas en materia de legitimación activa no pueden atentar contra la tutela judicial efectiva,[201] así como a dejar constancia de que la Decisión sobre el «Escudo de la privacidad» no menciona ninguna exigencia de que se informe a los interesados del hecho de que han sido objeto de una medida de vigilancia.[202] Dado que puede impedir el ejercicio de las vías de recurso jurisdiccionales, la inexistencia de una obligación de notificar tal medida, incluso cuando el hecho de informar al interesado ya no perjudique a su eficacia, parece problemática a la vista de la jurisprudencia mencionada en el punto 320 de las presentes conclusiones.

324. La nota a pie de página 169 de la Decisión sobre el «Escudo de la privacidad» reconoce, además, que los procedimientos disponibles «exigen, bien la existencia de daños […], bien la demostración de que el Gobierno pretende utilizar o divulgar información obtenida […] de la vigilancia electrónica de la persona interesada contra dicha persona». Tal como han destacado el órgano jurisdiccional remitente, el DPC y el Sr. Schrems, este requisito contrasta con la jurisprudencia del Tribunal de Justicia según la cual, para demostrar la existencia de una injerencia en el derecho al respeto de la vida privada del interesado, no es necesario que este haya sufrido posibles inconvenientes debido a la injerencia alegada.[203]

325. Además, el punto de vista expresado por Facebook Ireland y el Gobierno estadounidense, según el cual las deficiencias de las que adolece la protección jurisdiccional de las personas cuyos datos se transfieren a los Estados Unidos se ven compensadas mediante los controles previos y *a posteriori* efectuados por el FISC, así como por los múltiples mecanismos de supervisión establecidos en los Poderes Ejecutivo y Legislativo,[204] no me convence.

199 Véase el punto 67 de las presentes conclusiones.

200 Véase CEPD, EU-US Privacy Shield — Second Annual Joint Review, 22 de enero de 2019 (p. 18, apartado 97).

201 Véanse, en particular, las sentencias de 11 de julio de 1991, Verholen y otros (C-87/90 a C-89/90, EU:C:1991:314), apartado 24 y jurisprudencia citada, y de 28 de febrero de 2013, Reexamen Arango Jaramillo y otros/BEI (C-334/12 RX-II, EU:C:2013:134), apartado 43.

202 No obstante, el Gobierno estadounidense ha precisado, al igual que el órgano jurisdiccional remitente, que las medidas de vigilancia adoptadas con arreglo al artículo 702 de la FISA deben notificarse a sus objetivos si los datos recopilados se utilizan contra estos en el marco de un proceso judicial.

203 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), apartado 75; Digital Rights Ireland, apartado 33; Schrems, apartado 87, y dictamen 1/15, apartado 124.

204 Estos mecanismos se describen en los considerandos 95 a 110 de la Decisión sobre el «Escudo de la privacidad». La Comisión distingue en dicha Decisión, en la categoría de las normas relativas a la «tutela judicial efectiva», los mecanismos de supervisión (véanse los considerandos 92 a 110) de los recursos individuales (véanse los considerandos 111 a 124).

326. Ya he señalado que, por un lado, de conformidad con las conclusiones que figuran en la Decisión sobre el «Escudo de la privacidad», el FISC no controla las medidas individuales de vigilancia antes de su aplicación.[205] Según indica el considerando 109 de esta Decisión y como confirmó el Gobierno estadounidense en su respuesta escrita a las preguntas formuladas por el Tribunal de Justicia, por otro lado, el control *ex post* de la aplicación de los selectores tiene por objeto verificar, cuando una agencia de inteligencia comunique al FISC un incidente relativo al posible incumplimiento de los procedimientos de fijación de objetivos y de minimización,[206] el respeto de los requisitos que rigen la determinación de los selectores previstos en la certificación anual. Por lo tanto, no me parece que el procedimiento ante el FISC ofrezca una vía de recurso individual efectiva a las personas cuyos datos se transfieren a los Estados Unidos.

327. Considero que, si bien los mecanismos de control extrajudicial mencionados en los considerandos 95 a 110 de la Decisión sobre el «Escudo de la privacidad» podrían, en su caso, reforzar eventuales vías de recurso jurisdiccionales, no son suficientes para garantizar un nivel de protección adecuado en relación con el derecho de recurso de los interesados. En particular, los inspectores generales, que pertenecen a la estructura interna de cada agencia, no constituyen, a mi parecer, mecanismos de control independientes. La supervisión efectuada por el PCLOB y por las comisiones de inteligencia del Congreso, por su parte, no equivale a un mecanismo de recurso individual contra medidas de vigilancia.

328. Por consiguiente, procede examinar si la figura del Defensor del Pueblo subsana estas deficiencias al proporcionar a los interesados una vía de recurso efectiva ante un órgano independiente e imparcial.[207]

329. En segundo lugar, para evaluar la procedencia de la declaración de adecuación efectuada en la Decisión sobre el «Escudo de la privacidad» en relación con las vías de recurso de que disponen las personas que creen haber sido objeto de una vigilancia basada en el EO 12333, debo recordar que el marco de referencia pertinente lo conforman las disposiciones del CEDH.

330. Como se ha expuesto anteriormente,[208] para evaluar si una medida de vigilancia cumple los requisitos de «previsibilidad» y de «necesidad en una sociedad democrática» en el sentido del artículo 8, apartado 2, del CEDH,[209] el TEDH efectúa un examen de conjunto de los mecanismos de control y de supervisión aplicados «antes, durante y después» de su ejecución. Cuando el ejercicio de un recurso individual se ve impedido por el hecho de que no es posible la notificación de la medida

205 Véase el punto 298 de las presentes conclusiones.

206 A tenor del considerando 109 de la Decisión sobre el «Escudo de la privacidad», «el fiscal general y el director de [la NSA] verifican el cumplimiento y los servicios tienen la obligación de notificar cualesquiera incumplimientos detectados al FISC […], que podrá modificar la autorización en función de estos».

207 Véanse los puntos 333 a 340 de las presentes conclusiones.

208 Véase el punto 305 de las presentes conclusiones.

209 En su jurisprudencia relativa a las medidas de vigilancia de las telecomunicaciones, el TEDH ha tratado la cuestión de las vías de recurso en el marco del examen del «rango de ley» y de la necesidad de una injerencia en el ejercicio del derecho garantizado en el artículo 8 del CEDH [véanse, en particular, las sentencias Zakharov, § 236, y Centrüm för Rättvisa, § 107]. El TEDH, en la sentencia de 1 de julio de 2008, Liberty y otros c. Reino Unido (CE:ECHR:2008:0701JUD005824300), § 73, y en la sentencia Zakharov, § 307, tras haber apreciado la existencia de una infracción del artículo 8 del CEDH, no consideró necesario examinar de forma separada la alegación basada en el artículo 13 de este Convenio.

de vigilancia sin poner en peligro su eficacia,[210] esta laguna puede compensarse mediante la puesta en marcha de un control independiente de forma previa a la aplicación de la medida en cuestión.[211] Así pues, el TEDH, si bien estima que tal notificación es «deseable» tan pronto como pueda producirse sin alterar la eficacia de la medida de vigilancia, no ha declarado que sea un requisito imprescindible.[212]

331. A este respecto, la Decisión sobre el «Escudo de la privacidad» no pone de manifiesto que las medidas de vigilancia basadas en el EO 12333 sean notificadas a las personas afectadas o limitadas por mecanismos de control jurisdiccional o administrativo en ninguna fase de su adopción o de su aplicación.

332. En estas condiciones, procede examinar si, a pesar de todo, el recurso al Defensor del Pueblo permite garantizar un control independiente de las medidas de vigilancia, incluyendo las basadas en el EO 12333.

2) Sobre la influencia de la figura del Defensor del Pueblo sobre el nivel de protección del derecho a la tutela judicial efectiva

333. A tenor del considerando 116 de la Decisión sobre el «Escudo de la privacidad», la figura del Defensor del Pueblo descrita en el anexo III A de esta Decisión tiene por objeto proporcionar vías de recurso adicionales a todas las personas cuyos datos se transfieren desde la Unión a los Estados Unidos.

334. Tal como ha señalado el Gobierno estadounidense, la admisibilidad de una reclamación presentada ante el Defensor del Pueblo no está supeditada al cumplimiento de normas en materia de legitimación activa similares a las que regulan el acceso a los tribunales estadounidenses. El considerando 119 de dicha Decisión precisa, a este respecto, que el recurso al Defensor del Pueblo no presupone que la persona interesada demuestre que el Gobierno estadounidense ha accedido a los datos personales referidos a ella.

335. Al igual que el DPC, el Sr. Schrems, los Gobiernos polaco y portugués y el EPIC, dudo de la capacidad de este mecanismo para compensar las insuficiencias de la protección judicial ofrecida a las personas cuyos datos se transfieren desde la Unión a los Estados Unidos.

336. En primer lugar, aunque un mecanismo de recurso extrajudicial puede constituir una vía de recurso efectiva en el sentido del artículo 47 TFUE, solo es así, en particular, si el órgano en cuestión tiene un origen legal y cumple el requisito de independencia.[213]

210 Según el TEDH, si bien la falta de notificación en cualquier fase no impide necesariamente que una medida de vigilancia cumpla el requisito de «necesidad en una sociedad democrática», compromete el acceso a los tribunales y, por lo tanto, la efectividad de los recursos [véanse, en particular, la sentencia de 6 de septiembre de 1978, Klass y otros c. Alemania (CE:ECHR:1978:0906JUD000502971), §§ 57 y 58; la resolución Weber y Saravia, § 135, y la sentencia Zakharov, § 302].

211 Véase, en este sentido, la sentencia Centrum för Rättvisa, § 105.

212 En la sentencia Big Brother Watch, § 317, el TEDH se negó a añadir, entre las garantías mínimas aplicables a un régimen de vigilancia caracterizado por una interceptación masiva de las comunicaciones electrónicas, un requisito de notificación de la vigilancia a los interesados. Véase también la sentencia Centrüm för Rättvisa, § 164. La remisión de estos asuntos a la Gran Sala del TEDH tiene por objeto, entre otras cosas, el reexamen de esta conclusión.

213 El concepto de independencia entraña un primer aspecto, externo, que supone que el órgano de que se trata esté protegido de injerencias o presiones externas que puedan hacer peligrar la independencia en el enjuiciamiento por sus miembros de los litigios que se les sometan. El segundo aspecto, interno, de este concepto se asocia a la «imparcialidad» y se refiere a la equidistancia que debe guardar el órgano de que se trate con respecto a las partes del litigio y a sus intereses respectivos en relación con el objeto de dicho litigio. Véanse, en particular, las sentencias de 19 de septiembre de 2006, Wilson (C-506/04, EU:C:2006:587), apartados 50 a 52; de 25 de julio de 2018, Minister for Justice and Equality (Deficiencias del sistema judicial) (C-216/18 PPU, EU:C:2018:586), apartados 63 y 65, y de 19 de noviembre de 2019, A. K. y otros (Independencia de la Sala Disciplinaria del Tribunal Supremo) (C-85/18, C-624/18 y C-625/18, EU:C:2019:982), apartados 121 y 122. De conformidad con el principio de separación de poderes, la independencia de los órganos jurisdiccionales debe garantizarse respecto del Poder Ejecutivo, entre otros. Véase la sentencia de 19 de noviembre de 2019, A. K. y otros (Independencia de la Sala Disciplinaria del Tribunal Supremo) (C-85/18, C-624/18 y C-625/18, EU:C:2019:982), apartado 127 y jurisprudencia citada.

337. Pues bien, de la Decisión sobre el «Escudo de la privacidad» se desprende que la figura del Defensor del Pueblo, que fue creada por la PPD 28,[214] no tiene origen en la ley. El Defensor del Pueblo es nombrado por el Secretario de Estado y forma parte integrante del Departamento de Estado de los Estados Unidos.[215] Esta Decisión no contiene ninguna indicación de que la destitución del Defensor del Pueblo o la anulación de su nombramiento vengan acompañadas de garantías específicas.[216] Aunque el Defensor del Pueblo se presenta como una figura independiente de los «servicios de inteligencia», rinde cuentas al Secretario de Estado y no es, por tanto, independiente del Poder Ejecutivo.[217]

338. En segundo lugar, opino que la efectividad de una vía de recurso extrajudicial depende también de la capacidad del órgano en cuestión para adoptar decisiones vinculantes y motivadas. Al respecto, la Decisión sobre el «Escudo de la privacidad» no contiene ninguna indicación de que el Defensor del Pueblo adopte tales decisiones. No establece que la institución del Defensor del Pueblo permita a los solicitantes acceder a los datos que les conciernen y exigir que se rectifiquen o supriman, ni que el Defensor del Pueblo conceda una indemnización a las personas perjudicadas por una medida de vigilancia. En particular, tal como se desprende del anexo III A, apartado 4, letra e), de esta Decisión, «el Defensor del Pueblo […] no confirmará ni negará si el individuo ha sido objeto de vigilancia ni tampoco confirmará la reparación concreta aplicada».[218] Aunque el Gobierno estadounidense se ha comprometido a que el servicio de inteligencia en cuestión esté obligado a corregir cualquier infracción de las normas aplicables detectada por el Defensor del Pueblo,[219] dicha Decisión no menciona garantías legales que acompañen este compromiso y que puedan invocar los individuos afectados.

339. Por consiguiente, en mi opinión, la figura del Defensor del Pueblo no proporciona una vía de recurso ante un órgano independiente que ofrezca a las personas cuyos datos se transfieren la posibilidad de invocar su derecho de acceso a los datos o de impugnar posibles incumplimientos de las normas aplicables por parte de los servicios de inteligencia.

340. Por último, según la jurisprudencia, el respeto del derecho garantizado en el artículo 47 de la Carta supone que la decisión de esta autoridad administrativa que no cumpla en sí misma el requisito de independencia esté sujeta al control ulterior de un órgano jurisdiccional competente para pronunciarse sobre todas las cuestiones pertinentes.[220] Sin embargo, según las indicaciones proporcionadas en la Decisión sobre el «Escudo de la privacidad», las decisiones del Defensor del Pueblo no son objeto de un control jurisdiccional independiente.

214 El anexo III A de la Decisión sobre el «Escudo de la privacidad» hace referencia, a este respecto, a la sección 4, letra d), de la PPD 28.

215 Véase el considerando 116 de la Decisión sobre el «Escudo de la privacidad».

216 En la sentencia de 31 de mayo de 2005, Syfait y otros (C-53/03, EU:C:2005:333), apartado 31, el Tribunal de Justicia destacó la importancia de tales garantías para cumplir el requisito de independencia. Véanse también, a este respecto, las sentencias de 24 de junio de 2019, Comisión/Polonia (Independencia del Tribunal Supremo) (C-619/18, EU:C:2019:531), apartado 76, y de 5 de noviembre de 2019, Comisión/Polonia (Independencia de los tribunales ordinarios) (C-192/18, EU:C:2019:924), apartado 113.

217 Véanse los considerandos 65 y 121, así como el anexo III A, apartado 1, de la Decisión sobre el «Escudo de la privacidad».

218 Además, el considerando 121 de la Decisión sobre el «Escudo de la privacidad» indica que «el Defensor del Pueblo tendrá que confirmar que: i) la reclamación se ha investigado correctamente, y que ii) se ha observado el Derecho estadounidense pertinente, incluidas en particular las limitaciones y salvaguardias previstas en el anexo VI o, en caso de incumplimiento, que este se ha subsanado».

219 En el marco de la tercera revisión anual del Escudo de la privacidad, la Comisión apreció que, a tenor de las declaraciones del Gobierno estadounidense, en el supuesto de que la investigación del Defensor del Pueblo revele la existencia de una violación de los procedimientos de fijación de objetivos y de minimización aprobados por el FISC, esta violación deberá comunicarse a dicho tribunal. Entonces, según la Comisión, el FISC llevará a cabo a una investigación independiente y, en caso necesario, ordenará a la agencia de inteligencia de que se trata subsanar dicha violación. Véase el Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, 23 de octubre de 2019, SWD(2019) 390 final, p. 28. La Comisión hace referencia en este al documento titulado «Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure», disponible en la dirección de Internet https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (pp. 4 y 5).

220 Véanse las sentencias de 16 de mayo de 2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373), apartado 55, y de 13 de diciembre de 2017, El Hassani (C-403/16, EU:C:2017:960), apartado 39.

341. En estas circunstancias, tal como alegan el DPC, el Sr. Schrems, el EPIC y los Gobiernos polaco y portugués, la equivalencia sustancial entre la protección jurisdiccional ofrecida en el ordenamiento jurídico de los Estados Unidos a las personas cuyos datos se transfieren desde la Unión y la que se deriva del RGPD, interpretado a la luz del artículo 47 de la Carta y del artículo 8 del CEDH, me parece cuestionable.

342. A la vista de todas las consideraciones precedentes, tengo ciertas dudas sobre la conformidad de la Decisión sobre el «Escudo de la privacidad» con el artículo 45, apartado 1, del RGPD, interpretado a la luz de los artículos 7, 8 y 47 de la Carta y del artículo 8 del CEDH.

V. Conclusión

343. Propongo al Tribunal de Justicia que responda de la siguiente manera a las cuestiones prejudiciales planteadas por la High Court (Tribunal Superior, Irlanda):

«El análisis de las cuestiones prejudiciales no ha revelado elementos que puedan afectar a la validez de la Decisión de la Comisión 2010/87/UE, de 5 de febrero de 2010, relativa 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.»