

SENTENCIA DEL TRIBUNAL (Sala Décima Ampliada)

3 de septiembre de 2025 (*)

Transferencia de datos personales a Estados Unidos – Decisión de Ejecución de la Comisión que determina la adecuación del nivel de protección de datos personales garantizado por Estados Unidos – Derecho a la tutela judicial efectiva – Derecho a la vida privada y familiar – Decisiones basadas exclusivamente en el tratamiento automatizado de datos personales – Seguridad del tratamiento de datos personales

En el asunto T-553/23,

Philippe Latombe, con domicilio en Nantes (Francia), representado por los Sres. ^{N.} Coutrelis, J.-B. Soufron y T. Lamballe, abogados,

solicitante,

contra

Comisión Europea, representada por los Sres. D. Calleja Crespo, A. Bouchagiar, H. Kranenborg y C. Ladenburger, en calidad de agentes,

acusado,

apoyado por

Irlanda, representada por las Sras. ^{M.} Browne, S. Finnegan y A. Joyce, en calidad de agentes, asistidas por las Sras. S. Brittain, Barrister, y ^{C.} Donnelly, SC,

y por

Estados Unidos de América, representados por los señores B. Walsh, S. Barton y A. Finlay, abogados, la Sra. ^{E.} Barrington, SC, y el Sr. D. Hardiman, abogado,

partes intervinientes,

EL TRIBUNAL (Sala Décima Ampliada),

compuesto por la Sra. ^{O.} Porchia, presidenta, MM. M. Jaeger (ponente), L. Madise, P. Nihoul y S. Verschuur, jueces,

Secretaria: Sra. ^{I.} Kurme, administradora,

Visto el auto de 12 de octubre de 2023, Latombe/Comisión (T-553/23 R, no publicado, EU:T:2023:621),

Vista la fase escrita del procedimiento,
tras la audiencia del 1 de abril^{de} 2025,
hace el presente

Detener

- 1 Mediante su recurso basado en el artículo 263 TFUE, el demandante, Sr. Philippe Latombe, solicita, en esencia, la anulación de la Decisión de Ejecución (UE) 2023/1795 de la Comisión, de 10 de julio de 2023, por la que se establece, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, el nivel adecuado de protección de los datos personales garantizado por el marco de protección de datos UE-EE. UU. (DO 2023, L 231, p. 118; en lo sucesivo, «Decisión impugnada»).

I. Antecedentes de la controversia

- 2 El solicitante es un ciudadano francés que alega que utiliza diversas plataformas informáticas para recopilar sus datos personales y transferirlos a Estados Unidos.
- 3 En lo que respecta a la transferencia de datos personales de la Unión Europea a Estados Unidos, en primer lugar, mediante la sentencia de 6 de octubre de 2015, Schrems (C-362/14, en lo sucesivo, «sentencia Schrems I», EU:C:2015:650), el Tribunal de Justicia declaró inválida la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección ofrecida por los principios de puerto seguro y las preguntas frecuentes al respecto, publicada por el Departamento de Comercio de los Estados Unidos de América (DO 2000, L 215, p. 7).
- 4 En segundo lugar, mediante sentencia de 16 de julio de 2020, Facebook Ireland y Schrems (C-311/18, en lo sucesivo, «sentencia Schrems II», EU:C:2020:559), el Tribunal de Justicia declaró inválida la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, de conformidad con la Directiva 95/46, relativa a la adecuación de la protección ofrecida por el Escudo de la privacidad UE-EE. UU. (DO 2016, L 207, p. 1; en lo sucesivo, «Decisión de adecuación del Escudo de la privacidad»).
- 5 En las sentencias Schrems I y Schrems II, el Tribunal de Justicia, tras una petición de decisión prejudicial sobre la validez del asunto, declaró en particular que, contrariamente a la apreciación de la Comisión Europea en las decisiones de adecuación mencionadas en los apartados 3 y 4 supra, el sistema de puerto seguro y el sistema de escudo de la privacidad (en lo sucesivo, «escudo de la privacidad»)

que regulan la transferencia de datos personales no garantizaban un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado por el Derecho de la Unión.

6 A raíz de la sentencia Schrems II, la Comisión entabló conversaciones con el Gobierno de los Estados Unidos con vistas a la adopción de una posible nueva decisión de adecuación que cumpliera los requisitos del artículo 45, apartado 2, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46 (Reglamento general de protección de datos) (DO 2016, L 119, p. 1; corrección de errores en DO 2018, L 127, p. 2; en lo sucesivo, «RGPD»), tal como lo interpreta el Tribunal de Justicia.

7 Así, el 7 de octubre de 2022, Estados Unidos de América adoptó la Orden Ejecutiva 14086 (Orden Presidencial n.º 14086, en adelante “OE 14086”), que refuerza la protección de la privacidad que rige las actividades de inteligencia de señales realizadas por las agencias de inteligencia establecidas en Estados Unidos. Este decreto fue complementado por la Orden del Fiscal General n.º 5517-2022 (Reglamento del Fiscal General n.º 5517-2022, en adelante “Reglamento del Fiscal General”), que añadió la Parte 201 al Título 28 del Código de Reglamentos Federales (CFR), que rige la creación y el funcionamiento del Tribunal de Revisión de Protección de Datos (en adelante “TPD”).

El 10 de julio de 2023, tras examinar estas novedades normativas en Estados Unidos, la Comisión adoptó, con fundamento en el artículo 45, apartado 3, del RGPD, la Decisión impugnada, que establece el nuevo marco transatlántico para el flujo de datos personales entre la Unión y Estados Unidos. El artículo 1.º de dicha Decisión establece que Estados Unidos de América garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión a organizaciones establecidas en dicho país e incluidas en la lista del «Marco de Protección de Datos UE-EE. UU.» («DPF»), mantenida y publicada por su Departamento de Comercio («organizaciones del DPF»).

II. Conclusiones de las partes

9 La demandante solicita al Tribunal que:

- anule la Decisión impugnada, en cuanto al fondo, en su totalidad;
- Condene en costas a la Comisión.

10 La Comisión, apoyada por Irlanda y los Estados Unidos de América, solicita al Tribunal que:

- desestimar el recurso por inadmisibile;
- subsidiariamente, desestimar el recurso por infundado;
- Condenar en costas a la demandante.

III. En derecho

A. *Sobre la excepción de inadmisibilidad*

11 Mediante escrito separado presentado en la Secretaría del Tribunal General el 1 de diciembre de 2023, la Comisión propuso una excepción de inadmisibilidad, con fundamento en el artículo 130 del Reglamento de Procedimiento del Tribunal General.

12 La Comisión sostiene que el recurso es inadmisibile porque el demandante carece de legitimación activa, de interés para ejercitar la acción y de que la parte de la Decisión impugnada cuya anulación solicita es inseparable del resto de dicha Decisión.

13 El demandante rebate las alegaciones de la Comisión y sostiene que su demanda es admisible.

14 Procede recordar que el Tribunal de Justicia de la Unión Europea está facultado para apreciar, en función de las circunstancias de cada caso, si la buena administración de la justicia justifica la desestimación de un recurso en cuanto al fondo, sin pronunciarse previamente sobre su admisibilidad (véase, en este sentido, la sentencia de 26 de febrero de 2002, Consejo/Boehringer, C-23/00 P, EU:C:2002:118, apartados 51 y 52).

15 Así pues, habida cuenta de las circunstancias del presente asunto, el Tribunal considera que, al ser, en cualquier caso y por las razones que se exponen en los apartados 16 a 204 siguientes, infundado el recurso, procede, en interés de una buena administración de justicia, examinar su fundamento, sin pronunciarse previamente sobre su admisibilidad (véanse, en este sentido, las sentencias de 10 de octubre de 2014, Marchiani/Parlamento, T-479/13, no publicada, EU:T:2014:866, apartado 23, y de 20 de diciembre de 2023, Naturstrom/Comisión, T-60/21, no publicada, EU:T:2023:839, apartado 74).

B. *Sobre el fondo*

16 En apoyo de su recurso de casación, la demandante invoca cinco motivos, basados:

- el primero, de la infracción de los artículos 3 y 4 del Reglamento n.º 1/1958 del Consejo, de 15 de abril de 1958, por el que se fija el régimen lingüístico de la Comunidad Económica Europea (DO 1958, 17, p. 385);
- el segundo, de la violación de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea;
- el tercero, de la infracción del artículo 47, párrafo segundo, de dicha carta y del artículo 45, apartado 2, del RGPD;
- el cuarto, de la infracción del artículo 22 del RGPD;
- el quinto, de la infracción del artículo 32 del RGPD, en relación con el artículo 45, apartado 2, del mismo reglamento.

17 En la vista, el demandante desistió de su primer motivo, relativo a la infracción de los artículos 3 y 4 del Reglamento n.º 1/1958. Por consiguiente, procede examinar únicamente sus motivos segundo a quinto.

1. Observaciones preliminares

18 En primer lugar, cabe señalar que el artículo 45, apartado 1, del RGPD establece que la transferencia de datos personales a un tercer país podrá autorizarse mediante una decisión de la Comisión según la cual dicho tercer país, un territorio o uno o más sectores específicos del mismo garanticen un nivel de protección adecuado. Esta disposición se incluye en el capítulo V de dicho Reglamento, que, como ha indicado el Tribunal de Justicia, tiene por objeto, en general, garantizar la continuidad del elevado nivel de protección de los datos personales, garantizado por el Derecho de la Unión en virtud de dicho Reglamento, cuando dichos datos se transfieran a un tercer país (véase, en este sentido, Schrems II, apartado 93).

19 A este respecto, el Tribunal de Justicia aclaró que, sin exigir que el tercer país de que se trate garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión, la expresión «nivel de protección adecuado» que figura en el artículo 45, apartado 1, del RGPD debe entenderse en el sentido de que exige que ese tercer país garantice efectivamente, mediante su Derecho interno o sus compromisos internacionales, un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado en la Unión por dicho Reglamento, interpretado a la luz de la Carta de los Derechos Fundamentales (véase, en este sentido, la sentencia Schrems II, apartados 94 y 162).

20 El Tribunal de Justicia también declaró que, si bien los medios utilizados por el tercer país para garantizar un nivel adecuado de protección de los datos personales pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento

de las exigencias derivadas de la Directiva 95/46, interpretada a la luz de la Carta de los Derechos Fundamentales, dichos medios deben, no obstante, resultar eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión (sentencia Schrems I, apartado 74).

21 Además, el Tribunal de Justicia consideró que, habida cuenta, por una parte, del importante papel que desempeña la protección de los datos personales en relación con el derecho fundamental al respeto de la vida privada y, por otra parte, del número considerable de personas cuyos derechos fundamentales corren el riesgo de verse vulnerados en caso de transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, el margen de apreciación de la Comisión en cuanto a la adecuación del nivel de protección garantizado por un tercer país se reducía, de modo que era necesario que el juez de la Unión efectuara un control estricto de la legalidad de una decisión de adecuación (sentencia Schrems I, apartado 78).

22 En segundo lugar, procede recordar que, según reiterada jurisprudencia, la legalidad de un acto de la Unión debe apreciarse en función de los elementos de hecho y de Derecho existentes en la fecha de su adopción, de modo que los actos posteriores a la adopción de una decisión no pueden afectar a su validez (véanse las sentencias de 17 de octubre de 2019, *Alcogroup y Alcodis/Comisión*, C-403/18 P, EU:C:2019:870, apartado 45 y jurisprudencia citada, y de 28 de enero de 2021, *Qualcomm y Qualcomm Europe/Comisión*, C-466/19 P, EU:C:2021:76, apartado 82 y jurisprudencia citada). Por consiguiente, en el presente caso, las apreciaciones realizadas por la Comisión sobre la legalidad de la Decisión impugnada deben examinarse únicamente sobre la base de la información de que disponía en el momento en que las formuló.

Es en este contexto que deben analizarse los argumentos formulados por la demandante examinando primero el tercer argumento, luego el segundo argumento, luego el cuarto argumento y finalmente el quinto argumento.

2. *Sobre el tercer motivo, basado en la supuesta infracción del artículo 47, párrafo segundo, de la Carta de los Derechos Fundamentales y del artículo 45, apartado 2, del RGPD*

24 Mediante su tercer motivo, el demandante sostiene que la Comisión infringió el artículo 47, párrafo segundo, de la Carta de los Derechos Fundamentales y el artículo 45, apartado 2, del RGPD, ya que, en la Decisión impugnada, consideró que la DPRC ofrecía un nivel adecuado de protección en lo que respecta al derecho de los ciudadanos de la Unión a acceder a un tribunal independiente e imparcial previamente establecido por la ley.

- 25 Con carácter preliminar, procede recordar que el artículo 47, párrafo segundo, de la Carta de los Derechos Fundamentales tiene el siguiente tenor:

Toda persona tiene derecho a una audiencia justa y pública, dentro de un plazo razonable, por un tribunal independiente e imparcial, establecido previamente por la ley. Toda persona tiene la oportunidad de ser asesorada, defendida y representada.

- 26 Según las Explicaciones relativas a la Carta de los Derechos Fundamentales (DO 2007, C 303, p. 17), el segundo párrafo del artículo 47 de dicha Carta se corresponde con el artículo 6, apartado 1, del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950 (en adelante, «CEDH»). Los términos de esta última disposición son los siguientes:

“En la determinación de sus derechos y obligaciones civiles o en el examen de cualquier acusación en materia penal contra ella, toda persona tiene derecho a una audiencia justa y pública dentro de un plazo razonable por un tribunal independiente e imparcial, establecido por la ley.”

- 27 A este respecto, procede recordar que, según la jurisprudencia, dado que el CEDH no constituye, hasta la adhesión de la Unión a él, un instrumento jurídico formalmente incorporado al ordenamiento jurídico de la Unión, el examen de la validez de un acto de Derecho derivado debe efectuarse únicamente en relación con los derechos fundamentales garantizados por la Carta de los Derechos Fundamentales (sentencia de 3 de septiembre de 2015, *Inuit Tapiriit Kanatami y otros/Comisión*, C-398/13 P, EU:C:2015:535, apartados 45 y 46).

- 28 Sin embargo, la jurisprudencia reconoce, por una parte, que, en virtud del artículo 6 TUE, apartado 3, los derechos fundamentales reconocidos por el CEDH forman parte del Derecho de la Unión como principios generales y, por otra parte, que del artículo 52, apartado 3, de la Carta de los Derechos Fundamentales se desprende que los derechos contenidos en la Carta, que corresponden a derechos garantizados por el CEDH, tienen el mismo sentido y alcance que los que les confiere este último (véase la sentencia de 31 de mayo de 2018, *Korwin-Mikke/Parlamento*, T-770/16, EU:T:2018:320, apartado 38 y jurisprudencia citada).

- 29 Por consiguiente, según la jurisprudencia, en aras de la coherencia y sin que ello menoscabe la autonomía del Derecho de la Unión ni del Tribunal de Justicia de la Unión Europea, los derechos recogidos en la Carta de los Derechos Fundamentales que corresponden a los garantizados por el CEDH deben interpretarse también a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos (en lo sucesivo, «TEDH») [véanse, en este sentido, las sentencias de 9 de noviembre de 2023, *Staatssecretaris van Justitie en Veiligheid* (Concepto de perjuicio grave), C-125/22,

EU:C:2023:843, apartado 59, y de 31 de mayo de 2018, Korwin-Mikke/Parlamento, T-770/16, EU:T:2018:320, apartado 38].

30 De ello se desprende, según la jurisprudencia, que el Tribunal de Justicia debe garantizar, en virtud del artículo 52, apartado 3, de la Carta de los Derechos Fundamentales, que su interpretación del artículo 47, párrafo segundo, de dicha Carta garantice un nivel de protección que no vulnere el garantizado por el artículo 6, apartado 1, del CEDH, tal como lo interpreta el TEDH (véase la sentencia de 6 de octubre de 2021, W.Ž. (Sala Extraordinaria de Revisión y Asuntos Públicos del Tribunal Supremo — Nombramiento), C-487/19, EU:C:2021:798, apartado 123 y jurisprudencia citada).

31 Cabe señalar también que el artículo 45(2) del RGPD establece que, al evaluar la adecuación del nivel de protección ofrecido por un tercer país, la Comisión tendrá en cuenta, en particular, lo siguiente:

“(a) [...] los derechos efectivos y exigibles de que gozan los interesados y los recursos administrativos y judiciales que los interesados cuyos datos personales son transferidos puedan efectivamente interponer;

b) la existencia y el funcionamiento efectivo de una o más autoridades de control independientes en el tercer país, o a las que esté sujeta una organización internacional, encargadas de garantizar el cumplimiento de las normas de protección de datos y de hacerlas cumplir, incluso mediante poderes adecuados para aplicar dichas normas, de ayudar y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de los Estados miembros.

Es a la luz de estos elementos que deben examinarse las dos alegaciones formuladas por la demandante en apoyo del presente motivo.

a) *Sobre la primera queja del tercer motivo, según la cual la DPRC no es un tribunal independiente e imparcial*

33 Mediante la primera alegación de su tercer motivo, el demandante sostiene que la DPRC no es un tribunal independiente e imparcial en el sentido del artículo 47, párrafo segundo, de la Carta de los Derechos Fundamentales, sino un órgano parajudicial dependiente del poder ejecutivo.

34 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate las alegaciones de la demandante.

35 Con carácter preliminar, procede recordar que, según la jurisprudencia, la exigencia de independencia judicial, inherente a la función jurisdiccional, forma parte del contenido esencial del derecho a la tutela judicial efectiva y del derecho

fundamental a un proceso equitativo, que reviste una importancia capital como garantía de la protección de todos los derechos que el Derecho de la Unión confiere a los justiciables y de la preservación de los valores comunes a los Estados miembros enunciados en el artículo 2 TUE, en particular el valor del Estado de Derecho (sentencia de 15 de julio de 2021, Comisión/Polonia (Régimen disciplinario de los jueces), C-791/19, EU:C:2021:596, apartado 58 y jurisprudencia citada). De conformidad con el principio de separación de poderes que caracteriza el funcionamiento de un Estado de Derecho, debe garantizarse, en particular, la independencia de los tribunales respecto de los poderes legislativo y ejecutivo (véase la sentencia de 18 de mayo de 2021, Asociația “Forumul Judecătorilor din România” y otros, C-83/19, C-127/19, C-195/19, C-291/19, C-355/19 y C-397/19, EU:C:2021:393, apartado 195 y jurisprudencia citada).

36 La jurisprudencia específica que el requisito de independencia de los tribunales tiene dos aspectos. El primero, el externo, exige que el órgano en cuestión ejerza sus funciones con total autonomía, sin estar sujeto a ningún vínculo jerárquico ni subordinación a nadie y sin recibir órdenes ni instrucciones de ninguna fuente, quedando así protegido contra intervenciones o presiones externas que puedan socavar la independencia de criterio de sus miembros e influir en sus decisiones. El segundo, el interno, es similar al concepto de «imparcialidad» y busca la igualdad de distancia entre las partes en la controversia y sus respectivos intereses en relación con el objeto de la misma. Este último aspecto exige el respeto de la objetividad y la inexistencia de cualquier interés en la resolución del litigio distinto de la estricta aplicación del Estado jurídico (véase la sentencia de 21 de diciembre de 2021, Euro Box Promotion y otros, C-357/19, C-379/19, C-547/19, C-811/19 y C-840/19, EU:C:2021:1034, apartado 224 y jurisprudencia citada).

37 Las garantías de independencia e imparcialidad exigidas por el Derecho de la Unión exigen la existencia de normas, en particular en lo relativo a la composición del órgano, el nombramiento, la duración del mandato y las causas de abstención, recusación y destitución de sus miembros, que permitan disipar cualquier duda legítima de los justiciables sobre la impermeabilidad de dicho órgano a los factores externos y su neutralidad respecto de los intereses en juego (véase la sentencia de 15 de julio de 2021, Comisión/Polonia (Régimen disciplinario de los jueces), C-791/19, EU:C:2021:596, apartado 59 y jurisprudencia citada).

Es en este contexto en el que deben examinarse los tres argumentos formulados por la demandante en apoyo de esta queja.

1) *Sobre el primer argumento, según el cual la DPRC no es un tribunal independiente e imparcial, ya que su misión es revisar las decisiones del Oficial de Protección de las Libertades Civiles del Director de Inteligencia Nacional*

- 39 Mediante su primer argumento, el demandante sostiene, en esencia, que la DPRC no es un tribunal independiente e imparcial, puesto que su misión es revisar las decisiones del Oficial de Protección de Libertades Civiles del Director de Inteligencia Nacional (en adelante, el “CLPO”, Estados Unidos), quien está adscrito a la oficina del Director de Inteligencia Nacional de los Estados Unidos (en adelante, el “Director de Inteligencia Nacional”).
- 40 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate el argumento del demandante.
- 41 En aras de la claridad, debe señalarse que el primer argumento de la primera queja del tercer motivo debe interpretarse en el sentido de que, en esencia, según la demandante, en primer lugar, al tramitar una reclamación en materia de datos personales presentada por un interesado en la Unión que desea alegar una infracción del Derecho de los Estados Unidos que regula las actividades de inteligencia de señales que afecta negativamente a sus intereses en la protección de la privacidad y las libertades civiles (en lo sucesivo, «reclamación en materia de datos personales»), la CLPO no está rodeada de garantías suficientes para asegurar su independencia, debido a que está adscrita a la Oficina del Director de Inteligencia Nacional, y, en segundo lugar, que la DPRC no es un tribunal independiente e imparcial debido a la insuficiencia de las garantías aplicables a la CLPO.
- 42 En primer lugar, cabe señalar que el examen de las garantías relativas a la independencia de la CLPO es irrelevante para evaluar si la DPRC constituye un tribunal independiente e imparcial. En efecto, la DPRC se creó como un órgano de supervisión independiente de la CLPO, ante el cual, como se desprende del considerando 184 de la Decisión impugnada, la persona que presentó la reclamación relativa a datos personales, así como cada componente de la comunidad de inteligencia, pueden solicitar la revisión de la decisión de la CLPO. La Orden Ejecutiva 14086 establece diversas garantías para que las decisiones de la CLPO puedan ser revisadas y, en su caso, reformadas de forma independiente e imparcial por la DPRC.
- 43 En primer lugar, de los considerandos 185 y 186 de la decisión impugnada se desprende, sin que el demandante lo haya cuestionado, que la DPRC está compuesta por al menos seis jueces nombrados por el Fiscal General (Fiscal General de los Estados Unidos, en adelante, «el Fiscal General»), previa consulta con la Junta de Supervisión de la Privacidad y las Libertades Civiles (Junta de Supervisión de la Privacidad y las Libertades Civiles de los Estados Unidos, en adelante, «la PCLOB»), el Secretario de Comercio (Secretario de Comercio de los Estados Unidos) y el Director de Inteligencia Nacional, por períodos renovables de cuatro años, aplicando los mismos criterios que los que se aplican a los jueces de la judicatura federal y teniendo en cuenta su experiencia judicial previa. Así pues, los jueces deben ser profesionales del derecho —miembros en activo y acreditados del Colegio de

Abogados, debidamente autorizados para ejercer la abogacía— y deben poseer la experiencia adecuada en derecho de la privacidad y la seguridad nacional. Además, el Fiscal General debe garantizar que al menos la mitad de los jueces tengan experiencia judicial previa, y todos los jueces deben poseer autorizaciones de seguridad para acceder a información clasificada relacionada con la seguridad nacional. Solo podrán ser nombrados para la DPRC las personas que cumplan con los requisitos anteriores y que no sean empleados del poder ejecutivo al momento de su nombramiento ni lo hayan sido en los dos años anteriores. Asimismo, durante su mandato, los jueces de la DPRC no podrán ocupar ningún cargo ni empleo oficial en el gobierno de los Estados Unidos.

44 En segundo lugar, de los considerandos 188 y 189 de la decisión impugnada se desprende, sin que el demandante lo discuta, que las decisiones de la CLPO son revisadas en su totalidad por un panel de tres jueces de la DPRC asistidos por un abogado especial. Sin embargo, durante dicha revisión, la DPRC no se basa únicamente en el expediente proporcionado por la CLPO, sino también en la información y las observaciones presentadas por el denunciante, por el abogado especial que asiste a sus jueces y por los servicios de inteligencia, así como, en su caso, en la información adicional solicitada durante la investigación de la denuncia relativa a datos personales. Además, durante dicha revisión, debe aplicar la jurisprudencia pertinente del Tribunal Supremo de los Estados Unidos.

45 En tercer lugar, de los considerandos 190 y 191 de la decisión impugnada se desprende claramente, sin que el demandante lo impugne, que la DPRC tiene la facultad de revisión, no está vinculada por la decisión de la CLPO y, en caso de desacuerdo con esta, puede adoptar su propia decisión sobre la reclamación relativa a los datos personales. Además, sea cual sea la decisión de la DPRC, esta es vinculante y definitiva. Por lo tanto, tanto las agencias de inteligencia como el gobierno de Estados Unidos están obligados a acatarla.

46 De lo anterior se desprende que las garantías previstas en la Orden Ejecutiva 14086 en relación con el funcionamiento y las competencias de la DPRC permiten una revisión independiente e imparcial de las decisiones adoptadas por la CLPO. Por lo tanto, la demandante no tiene fundamento para argumentar que la insuficiencia de las garantías aplicables a la CLPO afecte a la independencia e imparcialidad de la DPRC.

47 En todo caso, respecto de la supuesta insuficiencia de las garantías destinadas a asegurar la independencia del CLPO, cabe señalar lo siguiente.

48 Cabe señalar, como se desprende de los considerandos 176 a 181 de la Decisión impugnada, sin que la demandante lo haya rebatido, que la Orden Ejecutiva 14086, complementada por el Reglamento AG, estableció un mecanismo de recurso específico para tramitar las reclamaciones relativas a datos personales. Dicha

reclamación debe presentarse ante la autoridad de control responsable, en cada Estado miembro, de supervisar el tratamiento de datos personales, que la remitirá a la CLPO, siempre que contenga los elementos indicados en el apartado 178 de la Decisión impugnada, a saber, información sobre los datos personales que razonablemente se cree que han sido transferidos a Estados Unidos, los medios por los que cabe presumir que se han transferido, la identidad, si se conoce, de las entidades gubernamentales estadounidenses sospechosas de estar implicadas en la presunta infracción, el fundamento de la presunta infracción del Derecho estadounidense y la naturaleza de la reparación solicitada. En este contexto, la CLPO debe determinar si las agencias de inteligencia han infringido el Derecho estadounidense aplicable y, de ser así, puede ordenarles que apliquen medidas correctivas. La decisión de la CLPO sobre la reclamación es vinculante.

49 Es cierto que, en el considerando 179 de la Decisión impugnada, la Comisión afirma que la CLPO forma parte de la Oficina del Director de Inteligencia Nacional y que, además de su competencia específica para examinar las denuncias relativas a datos personales, está obligada, de forma más general, a garantizar que la protección de las libertades civiles y la privacidad se integre adecuadamente en las políticas y procedimientos de dicha oficina y de las agencias de inteligencia, y que estas cumplan los requisitos aplicables en materia de protección de la privacidad y las libertades civiles. Sin embargo, por una parte, cabe señalar que, como se menciona en dicho considerando, para garantizar la independencia de la CLPO, la Orden Ejecutiva 14086 establece que esta solo podrá ser destituida de su cargo por dicho Director y por causa justificada, es decir, en caso de acción ilícita, mala conducta, violación de la seguridad, negligencia o incapacidad. Por otra parte, como se desprende del considerando 180 de la Decisión impugnada, las agencias de inteligencia y el Director de Inteligencia Nacional tienen prohibido obstruir o influir indebidamente en la labor de la CLPO, que, al examinar la denuncia relativa a datos personales, debe aplicar la ley de manera imparcial, teniendo en cuenta tanto los intereses de seguridad nacional como la protección de la privacidad.

50 En estas circunstancias, este argumento debe ser rechazado.

2) *Sobre el segundo argumento, según el cual la DPRC no es un tribunal independiente e imparcial, ya que está compuesta por jueces designados por el Fiscal General después de consultar con la PCLOB*

51 Mediante su segundo argumento, el demandante sostiene, en esencia, que la DPRC no es un tribunal independiente e imparcial, ya que está integrado por jueces designados por el Procurador General previa consulta con la PCLOB, que es un órgano dependiente del poder ejecutivo.

52 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate el argumento del demandante.

53 En primer lugar, del considerando 110 de la Decisión impugnada se desprende que la PCLOB es un organismo independiente, establecido en el seno del poder ejecutivo. La independencia de dicho organismo se pone de manifiesto, en particular, en su composición. En efecto, está compuesta por una junta bipartidista de cinco miembros nombrados por el Presidente de los Estados Unidos, con la aprobación del Senado, por un período fijo de seis años. Dichos miembros deben ser seleccionados en función de sus cualificaciones profesionales, logros, prestigio público, experiencia en la protección de la privacidad y las libertades civiles, y experiencia, independientemente de su afiliación política. La PCLOB no puede tener más de tres miembros pertenecientes al mismo partido político. Una persona nombrada como miembro de la PCLOB no puede, durante su mandato, ser funcionario electo, funcionario público o empleado del Gobierno Federal, salvo en su calidad de miembro de la PCLOB.

54 De ello se desprende que, si bien la PCLOB se creó dentro del poder ejecutivo, su estatuto fundacional la concibió como una agencia independiente cuya misión es supervisar, de forma imparcial, la labor realizada por el poder ejecutivo con miras a proteger, en particular, la privacidad y las libertades civiles. Así pues, como se indica en el considerando 194 de la decisión impugnada, sin que el demandante lo impugne, debe supervisar anualmente si la CLPO y la DPRC han tramitado los casos recibidos dentro de los plazos prescritos, si han tenido acceso a toda la información necesaria, si han tenido en cuenta todas las garantías previstas en la Orden Ejecutiva 14086 y si las agencias de inteligencia han cumplido con sus decisiones. Tras esta verificación, debe certificar públicamente que la CLPO y la DPRC han respetado estas garantías. Además, debe presentar un informe al Presidente de los Estados Unidos, al Fiscal General, al Director de Inteligencia Nacional, a los jefes de las agencias de inteligencia, a la CLPO y a los comités de inteligencia del Congreso de los Estados Unidos. Este informe se publica en una versión no clasificada. El Fiscal General, el Director de Inteligencia Nacional, la Oficina de Protección Civil y los jefes de las agencias de inteligencia deben implementar todas las recomendaciones del informe.

En estas circunstancias, el hecho de que la PCLOB se haya creado dentro del poder ejecutivo no permite en sí mismo concluir que, debido a su consulta antes del nombramiento de los jueces de la DPRC, ésta no sea un tribunal independiente e imparcial.

56 En segundo lugar, cabe señalar que, para garantizar la independencia de los jueces de la DPRC respecto del poder ejecutivo, la Orden Ejecutiva 14086 establece que, al ser nombrados, el Fiscal General debe cumplir los criterios y condiciones indicados en el párrafo 43 supra. Además, como se desprende del considerando 187 de la decisión impugnada, los jueces de la DPRC solo pueden ser destituidos por el Fiscal General y únicamente por causas válidas, a saber, acción ilícita, mala conducta, peligro para la seguridad, negligencia o incapacidad, tras la debida

consideración de las normas aplicables a los jueces federales establecidas en el Reglamento de Conducta Judicial y el Procedimiento para la Incapacidad Judicial.

57 De ello se desprende que las normas relativas al nombramiento y destitución de los jueces de la DPRC no pueden poner en tela de juicio su independencia e imparcialidad.

En tercer lugar, cabe señalar que, en virtud del artículo 3, apartado 1, de la Decisión impugnada, la Comisión debe supervisar de forma continua la aplicación del marco jurídico en el que se basa dicha decisión, en particular las condiciones en las que se realizan las transferencias posteriores de datos personales, se ejercen los derechos individuales y las autoridades públicas de los Estados Unidos tienen acceso a los datos transferidos sobre la base de dicha decisión, con el fin de determinar si Estados Unidos de América sigue garantizando un nivel de protección adecuado. Así pues, de conformidad con el artículo 3, apartado 5, cuando disponga de pruebas que indiquen que ya no se garantiza un nivel de protección adecuado, la Comisión informará a las autoridades estadounidenses y, en su caso, decidirá suspender, modificar, derogar la Decisión impugnada o limitar su alcance. De ello se deduce que, si cambia el marco jurídico vigente en Estados Unidos en el momento de la adopción de la Decisión impugnada que llevó a la Comisión a considerar, en dicha Decisión, que la DPRC ofrecía una protección jurídica sustancialmente equivalente a la garantizada por el Derecho de la Unión, la Comisión decide, en su caso, suspender, modificar o derogar la Decisión impugnada o limitar su alcance.

En vista de todas estas consideraciones, este argumento debe ser rechazado.

3) Sobre el tercer argumento, según el cual la DPRC no es un tribunal independiente e imparcial, dado que el reglamento del Fiscal General no excluye la posibilidad de que sus jueces estén sujetos a formas de supervisión distintas a la diaria por parte del poder ejecutivo.

60 Mediante su tercer argumento, el demandante sostiene, en esencia, que la DPRC no es un tribunal independiente e imparcial, puesto que el Reglamento del AG no excluye la posibilidad de que sus jueces estén sujetos a formas de supervisión distintas de la supervisión diaria por parte del poder ejecutivo.

61 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate el argumento de la demandante.

62 Cabe señalar que, si bien del expediente se desprende claramente que, en virtud del artículo 201.7(d) del Reglamento del Fiscal General, los jueces de la DPRC no deben estar sujetos a la supervisión diaria del Fiscal General, el considerando 187 de la Decisión impugnada también establece que, en virtud de la Orden Ejecutiva 14086, las agencias de inteligencia y el Fiscal General no deben obstruir ni influir

indebidamente en la labor de la DPRC. Además, del expediente se desprende claramente que la Orden Ejecutiva 14086 y el Reglamento del Fiscal General limitan la posibilidad de que el ejecutivo influya en la labor de la DPRC al establecer que sus jueces solo pueden ser destituidos por el Fiscal General y únicamente por las causas indicadas en el apartado 56 supra.

63 En este contexto, procede rechazar esta alegación y, por tanto, la primera imputación del tercer motivo en su totalidad.

b) *Sobre la segunda queja del tercer motivo, según la cual la DPRC no es un tribunal previamente establecido por ley*

64 Mediante la segunda alegación de su tercer motivo, el demandante sostiene que la DPRC no fue creada previamente por ley, en el sentido del artículo 47, párrafo segundo, de la Carta de los Derechos Fundamentales, en la medida en que no fue creada por una ley adoptada por el Congreso de los Estados Unidos, sino por un acto del ejecutivo, a saber, una decisión del Procurador General.

65 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate los argumentos de la demandante.

66 En primer lugar, de la jurisprudencia del Tribunal, desarrollada a la luz de la del TEDH relativa al artículo 6(1) del CEDH (TEDH, 1^{de diciembre de} 2020, *Guðmundur Andri Ástráðsson c. Islandia*, CE:ECHR:2020:1201JUD002637418, §§ 231 y 233), se desprende que, si bien el derecho a un tribunal previamente establecido por ley constituye un derecho autónomo, guarda, no obstante, una estrecha relación con las garantías de independencia e imparcialidad contenidas en dicha disposición. Más concretamente, si bien todos los requisitos que imponen estos conceptos persiguen un objetivo específico que los convierte en garantías específicas de un juicio justo, estas garantías buscan respetar los mismos principios fundamentales del Estado de Derecho y la separación de poderes. En el centro de cada una de estas exigencias se encuentra, por tanto, el imperativo de preservar la confianza que el poder judicial debe inspirar en el ciudadano y la independencia de dicho poder respecto de los demás poderes (véanse las sentencias de 22 de febrero de 2022, *Openbaar Ministerie* (Tribunal de Justicia del Estado miembro emisor), C-562/21 PPU y C-563/21 PPU, EU:C:2022:100, apartado 56 y jurisprudencia citada, y de 29 de marzo de 2022, *Getin Noble Bank*, C-132/20, EU:C:2022:235, apartado 117 y jurisprudencia citada).

67 El Tribunal también aclaró, haciéndose eco de la jurisprudencia del TEDH (TEDH, 8 de julio de 2014, *Biagioli c. San Marino*, CE:ECHR:2014:0708DECOO0816213, §§ 72 a 74; véase también TEDH, 2 de mayo de 2019, *Pasquini c. San Marino*, CE:ECHR:2019:0502JUD005095616, §§ 100 y 101 y jurisprudencia citada), que la expresión “previamente establecida por la ley” pretende evitar que la

organización del sistema judicial quede a la discreción del ejecutivo y garantizar que esta materia se rija por una ley adoptada por el legislador de manera coherente con las normas que rigen el ejercicio de su jurisdicción. Esta expresión refleja, pues, el principio del Estado de Derecho y se refiere no solo a la base jurídica de la propia existencia del tribunal, sino también a la composición de la Sala en cada caso y a cualquier otra disposición de Derecho interno cuyo incumplimiento haga ilegal la participación de uno o varios jueces en el examen del asunto, lo que incluye, en particular, las disposiciones relativas a la independencia e imparcialidad de los miembros del tribunal de que se trate (véase la sentencia de 29 de marzo de 2022, *Getin Noble Bank*, C-132/20, EU:C:2022:235, apartado 121 y jurisprudencia citada).

68 En este contexto, el Tribunal de Justicia declaró que la constatación de la existencia de un incumplimiento de la obligación de contar con un tribunal previamente establecido por la ley y de las consecuencias de dicho incumplimiento estaba sujeta a una apreciación global de un conjunto de factores que, considerados en su conjunto, contribuyen a generar en los justiciables dudas legítimas en cuanto a la independencia e imparcialidad de los jueces (véase la sentencia de 22 de febrero de 2022, *Openbaar Ministerie* (Tribunal de Justicia del Estado miembro emisor), C-562/21 PPU y C-563/21 PPU, EU:C:2022:100, apartado 74 y jurisprudencia citada).

69 Así, el Tribunal de Justicia ha considerado que el hecho de que un órgano, como un consejo nacional del poder judicial, que participa en el proceso de nombramiento de jueces esté compuesto mayoritariamente por miembros elegidos por el poder legislativo no puede, en sí mismo, suscitar dudas sobre la independencia de los jueces nombrados al término de dicho proceso, pero que, sin embargo, la situación puede ser diferente cuando dicha circunstancia, combinada con otros factores pertinentes y las condiciones en las que se realizaron dichas elecciones, da lugar a tales dudas [véase la sentencia de 22 de febrero de 2022, *Openbaar Ministerie* (Tribunal de Justicia del Estado miembro emisor), C-562/21 PPU y C-563/21 PPU, EU:C:2022:100, apartado 75 y jurisprudencia citada].

70 Además, en su sentencia de 1^{de diciembre} de 2020, *Guðmundur Andri Ástráðsson c. Islandia* (CE:ECHR:2020:1201JUD002637418, §§ 207 y 212), el TEDH declaró que el nombramiento de jueces por el poder ejecutivo o por el legislativo es admisible, siempre que los jueces así nombrados estén libres de cualquier presión o influencia en el ejercicio de su función judicial.

71 De dicha jurisprudencia se desprende, en esencia, que, para apreciar si se cumplen las exigencias derivadas del artículo 47, párrafo segundo, de la Carta de los Derechos Fundamentales, no es necesario limitarse a apreciar la naturaleza formal del texto legal que crea un tribunal y define sus normas de funcionamiento, sino que es necesario comprobar si dicho texto legal ofrece garantías suficientes para

asegurar su independencia e imparcialidad frente a los demás poderes, en particular el poder ejecutivo.

72 En segundo lugar, cabe recordar que, como declaró el Tribunal de Justicia en las sentencias Schrems I y Schrems II, en el contexto de una decisión de adecuación, la Comisión no está obligada a garantizar que las disposiciones pertinentes del tercer país sean idénticas a las vigentes en la Unión Europea, sino que sean sustancialmente equivalentes a las garantizadas por el Derecho de la Unión en virtud del RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales (véanse los apartados 19 y 20 supra). De ello se desprende que, en el presente caso, el Tribunal General debe verificar el fundamento de la conclusión de adecuación realizada por la Comisión en la Decisión impugnada, según la cual las disposiciones del Derecho estadounidense relativas al establecimiento y funcionamiento del DPRC ofrecen garantías sustancialmente equivalentes a las previstas por el Derecho de la Unión en el artículo 47, párrafo segundo, de dicha Carta. Tales garantías se ofrecen, en particular, cuando el texto legal que crea este tribunal y define sus reglas de funcionamiento pretende asegurar su independencia e imparcialidad respecto de los demás poderes, en particular el poder ejecutivo, pese a que dicho texto no constituye, desde un punto de vista formal, una ley.

73 En el presente caso, del considerando 185 de la Decisión impugnada se desprende, sin que la demandante lo haya cuestionado, que la DPRC fue creada por el Reglamento del Fiscal General. De ello se desprende que la DPRC no se constituyó mediante una ley adoptada por el poder legislativo, es decir, el Congreso de los Estados Unidos, sino mediante una ley emanada del poder ejecutivo. El Fiscal General es, de hecho, el jefe del Departamento de Justicia de los Estados Unidos y el principal funcionario encargado de hacer cumplir la ley dentro del gobierno federal de los Estados Unidos. Es el principal asesor del Presidente de los Estados Unidos en todos los asuntos jurídicos y miembro de su gabinete.

En este contexto, procede verificar si, de manera sustancialmente equivalente al Derecho de la Unión, la EO 14086 y el Reglamento AG ofrecen garantías destinadas a asegurar la independencia e imparcialidad de la DPRC .

75 A este respecto, en primer lugar, procede señalar que del expediente se desprende, sin que haya sido controvertido, que:

- el Procurador General adoptó el Reglamento del Procurador General basándose en su autoridad estatutaria para emitir decisiones vinculantes sobre cuestiones de derecho de los EE. UU., incluidas las relacionadas con la transferencia de datos desde la Unión regidas por la Orden Ejecutiva 14086;
- al crear la DPRC, el Procurador General delegó en ella su poder para decidir sobre la legalidad de las actividades de inteligencia electrónica impugnadas

por un ciudadano de la Unión; por lo tanto, el Procurador General ya no está facultado de iure para ejercer el poder que delegó en la DPRC mientras esta exista;

- como se indica en la nota ³⁶⁶ de la página 63 de la decisión impugnada, la Corte Suprema de los Estados Unidos ha reconocido la posibilidad de que el Fiscal General establezca órganos independientes con poder de decisión, como la DPRC; además, ha considerado que la delegación de poderes hecha por el Fiscal General a su agente es vinculante para el poder ejecutivo; así, se desprende de la jurisprudencia de dicho tribunal que, mientras el Reglamento del Fiscal General permanezca en vigor, el poder ejecutivo está obligado por él y que ni las agencias de inteligencia ni el gobierno de los Estados Unidos pueden revisar o revocar sus decisiones.

76 En segundo lugar, por una parte, procede recordar que de la Decisión impugnada se desprende, en esencia, que:

- los jueces de la DPRC son nombrados por el Procurador General de la República con base en los criterios y en cumplimiento de las condiciones mencionadas en el punto 43 anterior;
- los jueces de la DPRC sólo podrán ser destituidos de su cargo por el Procurador General de la República por las únicas causas a que se refiere el punto 56 anterior y de conformidad con las normas aplicables a los jueces federales establecidas en las reglas relativas a la ética judicial y al procedimiento de incapacidad judicial;

La decisión adoptada por la DPRC es vinculante y definitiva. Por lo tanto, tanto el poder ejecutivo como las agencias de inteligencia están obligados a acatarla.

- los trabajos realizados por la DPRC están sujetos a la supervisión del PCLOB, dentro de los límites indicados en el punto 54 anterior.

77 Además, como se desprende de los considerandos 187 a 189 de la Decisión impugnada, los jueces de la DPRC deben respetar, en el ejercicio de sus funciones en el seno de ésta, las siguientes garantías procesales:

- deben examinar la reclamación de datos personales en un panel compuesto por tres jueces, incluido un juez presidente; para cada caso, la composición del panel de tres jueces es elegida, de forma rotatoria, por la Oficina de Libertades Civiles y Privacidad del Ministerio de Justicia, que es responsable de brindar apoyo administrativo a la DPRC, asegurando que cada panel incluya al menos un juez con experiencia judicial previa;

- al revisar la reclamación de datos personales, son asistidos por un asesor especial que es designado por el Procurador General, después de consultar con el Secretario de Comercio, el Director de Inteligencia Nacional y la PCLOB, por un período renovable de dos años; el asesor especial debe tener experiencia apropiada en privacidad y leyes de seguridad nacional, debe ser un abogado experimentado y un miembro activo y de buena reputación del colegio de abogados; además, al momento del nombramiento, no debe haber sido empleado del poder ejecutivo dentro de los dos años anteriores; el asesor especial tiene acceso a toda la información, incluida la información clasificada, y, aunque no representa los intereses del demandante ni tiene una relación abogado-cliente con el demandante, debe asegurar que, en cada caso, los intereses del demandante estén representados y que los jueces de la DPRC estén bien informados de todos los asuntos legales y fácticos relevantes;
- para tomar su decisión, deberán tener en cuenta el expediente de investigación, la información y las observaciones proporcionadas por el denunciante, por el fiscal especial, por los servicios de inteligencia y por la CLPO, así como, en su caso, la información adicional transmitida por la CLPO a petición de la DPRC;
- deberán adoptar una decisión sobre la reclamación relativa a datos personales por escrito y por mayoría de votos.

En tercer lugar, cabe señalar que se han subsanado las deficiencias identificadas por el Tribunal en la sentencia Schrems II relativas a la falta de garantías en relación con la revocación, por parte del ejecutivo, del escudo protector del Defensor del Pueblo y la falta de carácter vinculante de sus decisiones. De hecho, del expediente se desprende claramente que la Orden Ejecutiva 14086 limita las circunstancias en las que el Fiscal General puede destituir a los jueces de la DPRC y establece que sus decisiones son vinculantes.

79 En este contexto, procede desestimar la segunda imputación del tercer motivo.

80 Esta conclusión no puede ser puesta en tela de juicio por el hecho de que del expediente se desprende claramente que, al igual que otros tribunales del sistema jurídico de los Estados Unidos, si bien está facultado para decidir sobre cuestiones jurídicas, el DPRC no constituye una autoridad judicial establecida en virtud del Artículo III de la Constitución de los Estados Unidos.

81 En efecto, en la sentencia Schrems II, el Tribunal consideró que la tutela judicial efectiva podía ser garantizada no sólo por un tribunal perteneciente al sistema judicial, sino también por cualquier otro «organismo» que ofreciera a las personas cuyos datos se transfieren a Estados Unidos garantías sustancialmente equivalentes a las exigidas por el artículo 47 de la Carta de los Derechos Fundamentales (sentencia Schrems II, apartado 197).

82 En vista de todas las consideraciones anteriores, procede desestimar en su totalidad el tercer motivo.

3. *Sobre el segundo motivo, basado en la violación de los artículos 7 y 8 de la Carta de los Derechos Fundamentales*

83 Mediante su segundo motivo, el demandante alega que la Comisión infringió los artículos 7 y 8 de la Carta de los Derechos Fundamentales, en la medida en que, en la Decisión impugnada, consideró que Estados Unidos de América garantizaba un nivel de protección adecuado en lo que respecta a la recogida masiva de datos personales por parte de los servicios de inteligencia de dicho país.

(a) *Sobre el objeto del segundo motivo*

84 Cabe señalar que, en las páginas 2 y 23 de la demanda y en la página 4 de la réplica, al exponer el tenor de su segundo motivo, el demandante se refiere a la infracción por parte de la Comisión de los artículos 7 y 8 de la Carta de los Derechos Fundamentales, en relación no solo con la recogida masiva de datos personales, sino también con la recogida en masa. Sin embargo, en los desarrollos posteriores a la exposición del tenor de dicho motivo, el demandante centra sus argumentos únicamente en la recogida masiva de dichos datos.

85 De la nota a pie de página ²⁵⁰ de la página 46 de la Decisión impugnada, del considerando 141 de dicha Decisión, sin que haya sido rebatido, y de las respuestas dadas por las partes a las cuestiones planteadas mediante diligencia de ordenación del procedimiento y en la vista se desprende que:

- en los Estados Unidos, la recopilación de señales de inteligencia para fines de seguridad nacional, incluso con respecto a los datos transferidos desde la Unión, solo puede adoptar la forma de “recopilación dirigida”; este término no está definido en la legislación de los Estados Unidos, pero generalmente se utiliza para describir la recopilación de inteligencia dirigida a una persona específica, cuenta de comunicaciones u otro objetivo identificado que llevan a cabo las agencias de inteligencia en virtud de la Ley de Vigilancia de Inteligencia Extranjera (FISA) y la Orden Ejecutiva 14086.
- fuera de los Estados Unidos, incluso cuando los datos personales están en tránsito desde la Unión a las organizaciones de CPD, la recopilación de inteligencia de señales para fines de seguridad nacional se realiza principalmente a través de la recopilación dirigida; sin embargo, cuando sea necesario avanzar en una prioridad de inteligencia validada, como se define en la Sección 2(b)(iii) de la EO 14086, que no se puede lograr razonablemente a través de la recopilación dirigida, las agencias de inteligencia pueden realizar una “recopilación masiva” de datos personales; la recopilación masiva se define en la ley de los Estados

Unidos por la Sección 4(b) de la EO 14086 como la recopilación autorizada de grandes cantidades de inteligencia de señales que, por razones técnicas u operativas, se realiza sin el uso de discriminadores, por ejemplo, identificadores específicos o criterios de selección; La recopilación masiva se rige por la EO 14086 y la Orden Ejecutiva 12333, Actividades de Inteligencia de los Estados Unidos , modificada por las Órdenes Ejecutivas 13284 (2003), 13355 (2004) y 13470 (2008), que la someten a varias salvaguardas y limitaciones;

- la “recogida masiva” de datos personales a la que se refiere la Comisión en la nota a pie de página 250 de la Decisión impugnada como una recogida efectuada de manera generalizada e indiscriminada, sin restricciones ni garantías, no está autorizada en Estados Unidos y no puede efectuarse ni dentro ni fuera de su territorio .

86 De lo anterior se desprende que, dado que la recogida masiva no está permitida en Estados Unidos y que solo puede efectuarse fuera de Estados Unidos, el objeto del presente motivo se limita, en el presente caso, a la apreciación de la existencia de una infracción, por parte de la Comisión, de los artículos 7 y 8 de la Carta de los Derechos Fundamentales en lo que respecta a la recogida masiva, por parte de las agencias de inteligencia estadounidenses, de datos personales en tránsito desde la Unión hacia las organizaciones del CPD, con exclusión de cualquier recogida de datos personales realizada, en su caso, en el territorio de la Unión por las agencias de inteligencia de Estados Unidos o de los Estados miembros.

b) Sobre la primera queja del segundo motivo, según la cual las actividades de inteligencia realizadas al amparo del artículo 702 de la FISA no están sujetas a las garantías previstas en la Orden Ejecutiva 14086

87 Mediante la primera imputación de su segundo motivo, el demandante alega que la Comisión infringió los artículos 7 y 8 de la Carta de los Derechos Fundamentales, ya que, en la Decisión impugnada, consideró, en esencia, que Estados Unidos de América ofrecía un nivel de protección sustancialmente equivalente al garantizado por el Derecho de la Unión en virtud del RGPD, leído a la luz de dicha Carta, a pesar de que el artículo 702 de la FISA concede a las agencias de inteligencia estadounidenses la posibilidad de recopilar de forma masiva datos personales de nacionales de otros países.

88 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate los argumentos de la demandante.

Cabe señalar que la Sección 702 de la FISA no autoriza la recopilación masiva, sino sólo la recopilación selectiva de datos personales .

90 De ello se desprende que, en la medida en que el artículo 702 de la FISA no se refiere a la recopilación masiva de datos personales, es irrelevante en este caso.

91 Por consiguiente, procede desestimar la primera alegación del segundo motivo.

c) Sobre la segunda queja del segundo motivo, según la cual la EO 14086 no supedita la recogida masiva de datos personales a la autorización previa de una autoridad judicial o administrativa

92 Mediante la segunda imputación de su segundo motivo, el demandante alega que la Comisión infringió los artículos 7 y 8 de la Carta de los Derechos Fundamentales, puesto que, en la Decisión impugnada, consideró que Estados Unidos de América ofrecía un nivel de protección sustancialmente equivalente al garantizado por el Derecho de la Unión en virtud del RGPD, interpretado a la luz de dicha Carta, a pesar de que la EO 14086 no establece una obligación para las agencias de inteligencia estadounidenses de obtener, antes de la recogida masiva de datos personales, la autorización previa de una autoridad judicial o administrativa.

93 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate los argumentos de la demandante.

94 En el presente caso, de los autos se desprende, sin que las partes lo impugnen, que el Derecho estadounidense no establece una obligación para las agencias de inteligencia de obtener una autorización previa de una autoridad judicial o administrativa antes de proceder a una recogida masiva de datos personales en tránsito desde la Unión hacia las organizaciones del CPD.

95 Procede determinar si esta falta de autorización previa puede afectar a la legalidad de la Decisión impugnada, en la medida en que podría poner en tela de juicio la conclusión establecida en el artículo 1^{de} dicha Decisión, según la cual los Estados Unidos de América ofrecen un nivel adecuado de protección de los datos personales.

96 Con carácter preliminar, procede recordar que, como declaró el Tribunal de Justicia en la sentencia Schrems II, para apreciar la legalidad de una decisión de adecuación, es necesario apreciar si el Derecho del tercer país garantiza un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado en la Unión por el RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales (véase el apartado 19 supra).

97 Es en este contexto que deben examinarse los cuatro argumentos formulados por la demandante en apoyo de esta queja.

1) *Sobre el primer argumento, basado en la sentencia Schrems II*

- 98 Mediante su primer argumento, el demandante sostiene, en esencia, que, como sucedió con la decisión de adecuación relativa al escudo de privacidad anulada por el Tribunal en la sentencia Schrems II debido, en particular, a la falta de establecimiento de un control judicial, la recopilación masiva de datos personales realizada, en el presente caso, por las agencias de inteligencia de los Estados Unidos no está sujeta a control judicial y no se rige por reglas suficientemente claras y precisas.
- 99 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate el argumento del demandante.
- 100 Cabe señalar que, en la sentencia Schrems II, el Tribunal de Justicia declaró que los artículos 7 y 8 de la Carta de los Derechos Fundamentales formaban parte del nivel de protección exigido en la Unión, cuyo cumplimiento debía ser comprobado por la Comisión antes de adoptar una decisión de adecuación con arreglo al artículo 45, apartado 1, del RGPD. En efecto, según el Tribunal de Justicia, cualquier tratamiento de datos personales de una persona física, incluida su transferencia a un tercer país en el contexto de una decisión de adecuación, afecta tanto al derecho fundamental de dicha persona al respeto de la vida privada, garantizado en el artículo 7 de dicha Carta, como a su derecho a la protección de sus datos personales, consagrado en el artículo 8 de dicha Carta (sentencia Schrems II, apartados 169 a 171).
- 101 Sin embargo, el Tribunal aclaró que los derechos consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales no eran prerrogativas absolutas, sino que debían tomarse en consideración en relación con su función en la sociedad (sentencia Schrems II, apartado 172).
- 102 Así pues, de conformidad con el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales, cualquier limitación del ejercicio de los derechos y libertades reconocidos por los artículos 7 y 8 de dicha Carta debe estar prevista por ley y respetar la esencia de dichos derechos y libertades. Además, de conformidad con el principio de proporcionalidad, solo podrán imponerse limitaciones a dichos derechos y libertades si son necesarias y responden realmente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de terceros (Schrems II, apartado 174).
- 103 En este contexto, el Tribunal de Justicia declaró que la posibilidad otorgada por el Decreto Presidencial n.º 12333, en su versión modificada, a las agencias de inteligencia estadounidenses de acceder a datos personales en tránsito desde la Unión, sin que dicho acceso estuviera sujeto a control judicial alguno, no permitía definir un marco suficientemente claro y preciso para el alcance de la recopilación masiva de datos personales realizada por dichas agencias. Por consiguiente, consideró que dicho decreto presidencial no se ajustaba a los requisitos mínimos

vinculados, en el Derecho de la Unión, al principio de proporcionalidad y que los programas de vigilancia realizados con arreglo a dicho decreto no se limitaban a lo estrictamente necesario (Schrems II, apartados 183 y 184).

104 Es necesario aclarar la interpretación que debe darse a la expresión «cualquier supervisión judicial» que aparece en el apartado 183 de la sentencia Schrems II.

105 A este respecto, cabe señalar que nada en la sentencia Schrems II, en particular en su apartado 183 y en la expresión «cualquier supervisión judicial», sugiere que la recogida masiva de datos personales deba necesariamente ser objeto de una autorización previa emitida por una autoridad independiente. Por el contrario, de la lectura conjunta de dicha expresión y de los apartados 186 a 197 de dicha sentencia se desprende que la decisión que autoriza dicha recogida debe, como mínimo, estar sujeta a control judicial posterior.

106 En el presente caso, como se indica en los apartados 24 a 82 supra, la Orden Ejecutiva 14086 y el Reglamento AG someten las actividades de inteligencia de señales realizadas por las agencias de inteligencia estadounidenses, incluso cuando realizan la recopilación masiva de datos personales, a la supervisión judicial ex post de la DPRC, cuyas decisiones son definitivas y vinculantes tanto para el Gobierno estadounidense como para dichas agencias. Por consiguiente, contrariamente a lo que alega la demandante, no puede considerarse que la recopilación masiva de datos personales realizada por las agencias de inteligencia sobre la base de la decisión impugnada no cumpla los requisitos derivados de la sentencia Schrems II al respecto.

107 Además, en primer lugar, cabe recordar que, como se desprende del considerando 141 de la Decisión impugnada, sin que la demandante lo impugne, la Orden Ejecutiva 14086 establece que las agencias de inteligencia deben priorizar la recopilación selectiva de datos personales. Por lo tanto, la recopilación masiva solo se permite para promover una prioridad de inteligencia validada que no pueda lograrse razonablemente mediante la recopilación selectiva. A este respecto, cabe señalar que del considerando 135 de dicha Decisión se desprende que las prioridades de inteligencia validadas se establecen mediante un procedimiento especial diseñado para garantizar el cumplimiento de los requisitos legales aplicables, incluidos los relativos a la privacidad y las libertades civiles. Más concretamente, las prioridades de inteligencia son definidas por el Director de Inteligencia Nacional y están sujetas a la aprobación del Presidente de los Estados Unidos. No obstante, antes de proponer prioridades de inteligencia al Presidente de los Estados Unidos, el Director debe obtener, para cada prioridad, una evaluación de la CLPO. Al realizar esta evaluación, la CLPO debe determinar si la prioridad en cuestión promueve uno o más de los objetivos legítimos enumerados en la EO 14086, si no fue diseñada para la recopilación de inteligencia de señales para fines prohibidos y si se estableció después de la debida consideración de los aspectos de privacidad y libertades civiles

de todas las personas involucradas, independientemente de su nacionalidad y lugar de residencia.

108 En segundo lugar, procede señalar que, como se destaca en los considerandos 127 a 131, 134 y 135 de la Decisión impugnada, sin que la demandante lo cuestione, la EO 14086 establece requisitos fundamentales que se aplican a todas las actividades de inteligencia de señales, incluso cuando se llevan a cabo mediante la recopilación masiva de datos personales.

109 En primer lugar, las actividades de inteligencia de señales deben basarse en un estatuto o autorización presidencial y deben llevarse a cabo de conformidad con la legislación de los Estados Unidos, incluida su Constitución.

110 En segundo lugar, las actividades de inteligencia de señales solo pueden llevarse a cabo después de determinar, sobre la base de una evaluación razonable de todos los factores pertinentes, que son necesarias para perseguir una prioridad de inteligencia validada.

111 En tercer lugar, las actividades de inteligencia de señales deben llevarse a cabo de manera proporcional a la prioridad de inteligencia validada para la que fueron autorizadas, a fin de lograr un equilibrio justo entre la importancia de la prioridad de inteligencia perseguida y el impacto en la privacidad y las libertades civiles del individuo en cuestión, independientemente de su nacionalidad y lugar de residencia.

112 En cuarto lugar, la Orden Ejecutiva 14086 enumera los objetivos generales que no pueden perseguirse mediante actividades de inteligencia de señales. Estos incluyen los objetivos de obstruir la crítica, la disidencia o la libre expresión de ideas u opiniones políticas por parte de individuos o de la prensa; de discriminar a personas por motivos de etnia, raza, género, identidad de género, orientación sexual o religión; o de conferir una ventaja competitiva a empresas con sede en Estados Unidos.

113 En tercer lugar, del considerando 141 de la Decisión impugnada se desprende, sin que la demandante lo impugne, que la EO 14086 establece garantías específicas aplicables a la recogida masiva de datos personales.

114 En primer lugar, la EO 14086 establece que se deben aplicar métodos y medidas técnicas para limitar los datos recopilados a lo necesario para perseguir una prioridad de inteligencia validada, minimizando al mismo tiempo la recopilación de información irrelevante.

115 A continuación, la Orden Ejecutiva 14086 establece que la recopilación masiva de datos personales solo podrá llevarse a cabo para cumplir seis fines específicos (en adelante, los «fines específicos de la recopilación masiva»), a saber, la protección

contra el terrorismo, el espionaje, las armas de destrucción masiva, las ciberamenazas, las amenazas dirigidas contra el personal estadounidense o sus aliados, y la delincuencia transnacional. Prevé la posibilidad de que el Presidente de los Estados Unidos actualice dichos fines específicos si surgen nuevos imperativos de seguridad nacional, como amenazas nuevas o crecientes a la seguridad nacional para las que el Presidente considere que podría utilizarse la recopilación masiva de datos personales. Dichas actualizaciones deben, en principio, ser publicadas por el Director de Inteligencia Nacional, a menos que el Presidente de los Estados Unidos considere que esto en sí mismo constituiría un riesgo para la seguridad nacional de ese país.

116 Por último, la EO 14086 establece que cualquier interrogación de datos masivos de inteligencia de señales solo puede ocurrir si es necesaria para lograr una prioridad de inteligencia validada, en cumplimiento de los objetivos específicos de la recopilación masiva y de conformidad con políticas y procedimientos que tengan debidamente en cuenta el impacto de las interrogaciones de dichos datos en la privacidad y las libertades civiles de todas las personas involucradas, independientemente de su nacionalidad o lugar de residencia.

117 En estas condiciones, no puede afirmarse válidamente que la ejecución de la recogida masiva no esté regulada de forma suficientemente clara y precisa.

118 En vista de todas estas consideraciones, este argumento debe ser rechazado.

2) Sobre el segundo argumento, basado en la sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros* (C - 511/18, C - 512/18 y C - 520/18)

119 Mediante su segunda alegación, el demandante, refiriéndose expresamente al apartado 189 de la sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros* (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), alega que el Tribunal de Justicia ha establecido la obligación de que las agencias de inteligencia obtengan autorización previa de una autoridad judicial o administrativa antes de recopilar datos de conexión de los operadores que los poseían. En su opinión, la recopilación masiva de datos personales en tránsito desde la Unión por parte de las agencias de inteligencia estadounidenses no estaría sujeta, en el presente caso, a dicha autorización previa.

120 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate el argumento del demandante.

121 Procede recordar que, en la sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros* (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), el Tribunal de Justicia declaró, en particular, que el artículo 15, apartado 1, de la Directiva 2002/58/CE 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), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (DO 2009, L 337, p. 11), leído a la luz de los artículos 7, 8 y 11 y del artículo El artículo 52(1) de la Carta de los Derechos Fundamentales, debía interpretarse en el sentido de que no se oponía a una normativa nacional que obligara a los proveedores de servicios de comunicaciones electrónicas a recurrir a la recogida en tiempo real de datos de tráfico y de localización, cuando dicha recogida se limitaba a personas respecto de las cuales existía una sospecha razonable de que estaban implicadas en actividades terroristas y estaba sujeta a un control previo por parte de un tribunal o de un órgano administrativo independiente (apartado 192 de dicha sentencia).

122 De ello se desprende que la situación controvertida en el asunto que dio lugar a la sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros* (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), difiere de la controvertida en el presente asunto. En el presente caso, no se trata de evaluar la necesidad de someter la recopilación, por parte de los proveedores de servicios de comunicaciones electrónicas, de datos de tráfico y de localización de usuarios sospechosos de estar implicados de una u otra forma en actividades terroristas al control previo de una autoridad judicial o administrativa, sino de evaluar si el hecho de que el Derecho estadounidense no prevea la obligación de que las agencias de inteligencia obtengan, antes de la recopilación masiva de datos personales en tránsito hacia ese país, la autorización previa de una autoridad judicial o administrativa cuestiona el fundamento de la constatación de adecuación de la Comisión realizada en la Decisión impugnada.

123 En estas circunstancias, procede concluir que la remisión a la sentencia de 6 de octubre de 2020, *La Quadrature du Net y otros* (C-511/18, C-512/18 y C-520/18, EU:C:2020:791), no es pertinente en el presente asunto.

124 Esta conclusión no puede desvirtuarse teniendo en cuenta la sentencia de 30 de abril de 2024, *La Quadrature du Net ea* (Datos personales y lucha contra la falsificación) (C-470/21, EU:C:2024:370), sobre la que se invitó a las partes del presente asunto a pronunciarse mediante una diligencia de ordenación del procedimiento.

125 Lo que se discutía en el asunto que dio lugar a la sentencia de 30 de abril de 2024, *La Quadrature du Net y otros* (Datos personales y lucha contra la falsificación) (C-470/21, EU:C:2024:370), era la legalidad del acceso, por parte de una autoridad pública nacional responsable de la protección de los derechos de autor y derechos afines contra las vulneraciones de estos derechos cometidas en internet, a los datos almacenados por proveedores de servicios de comunicaciones electrónicas relativos a la identidad civil correspondiente a direcciones IP, con el fin de combatir

la falsificación. Más concretamente, dicho acceso estaba justificado en vista del objetivo de identificar al titular de una dirección IP que había realizado una actividad vulneradora de los derechos de autor o derechos afines, puesto que había puesto a disposición ilícitamente obras protegidas en internet para que otras personas las descargaran. En estas circunstancias, el Tribunal de Justicia dictaminó que la revisión previa por un tribunal o por un órgano administrativo independiente:

- no debe establecerse cuando la autoridad nacional competente haya tenido acceso a datos relativos a la identidad civil de una persona correspondiente a una dirección IP, con el único fin de identificar al usuario de que se trate y sin que dichos datos puedan asociarse a información relativa a las comunicaciones efectuadas, ya que la injerencia que haya supuesto dicho acceso no pueda calificarse de grave (apartados 133 y 134 de dicha sentencia);
- debían ponerse en marcha antes de que la autoridad nacional competente vinculara los datos de identidad civil de una persona correspondientes a una dirección IP y el fichero relativo a la obra puesta a disposición de forma ilícita en Internet para su descarga por otras personas y enviara al interesado un escrito en el que declarase que había cometido actos ilícitos (véase, en este sentido, el apartado 141 de dicha sentencia).

126 De ello se desprende que el asunto que dio lugar a la sentencia de 30 de abril de 2024, *La Quadrature du Net y otros (Datos personales y lucha contra la falsificación)* (C-470/21, EU:C:2024:370), se refiere al acceso por parte de las autoridades nacionales a una dirección IP con el fin de combatir la falsificación, y que dicho objeto es distinto de la recopilación masiva de datos personales en tránsito desde la Unión por parte de las agencias de inteligencia. Por consiguiente, no puede considerarse, a la luz de dicha sentencia, que la recopilación masiva de datos personales en tránsito desde la Unión por parte de las agencias de inteligencia estadounidenses requiera autorización previa.

127 Por consiguiente, este argumento debe rechazarse.

3) *Sobre el tercer argumento, basado en la sentencia del TEDH de 25 de mayo de 2021, Big Brother Watch y otros contra Reino Unido (CE:ECHR:2021:0525JUD005817013)*

128 Mediante su tercer argumento, el demandante alega, en esencia, que, en la sentencia del TEDH de 25 de mayo de 2021, *Big Brother Watch y otros contra el Reino Unido (CE:ECHR:2021:0525JUD005817013*, en adelante, «sentencia *Big Brother Watch*»), el TEDH declaró que la interceptación masiva de datos personales debe estar sujeta a la autorización previa de una autoridad independiente desde el momento en que se definen los objetivos y el alcance de la operación de vigilancia. En su opinión, la recopilación masiva de datos personales en tránsito desde la Unión

por parte de las agencias de inteligencia estadounidenses no está sujeta, en el presente caso, a dicha autorización previa.

129 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate el argumento del demandante.

130 Es preciso recordar que el asunto que dio lugar a la sentencia *Big Brother Watch* se refería, en particular, a la compatibilidad, a la luz del artículo 8 del CEDH, del régimen británico de vigilancia secreta que otorgaba a las agencias de inteligencia la facultad de interceptar en masa las comunicaciones electrónicas y los datos de comunicaciones asociados, es decir, los datos de tráfico relativos a las comunicaciones interceptadas, que en principio se llevaban a cabo fuera de las Islas Británicas.

131 Además, como se desprende de la jurisprudencia citada en el apartado 29 supra, dado que el artículo 8 del CEDH consagra, al igual que el artículo 7 de la Carta de los Derechos Fundamentales, el derecho al respeto de la vida privada y familiar, la jurisprudencia del TEDH relativa al artículo 8 del CEDH debe tenerse en cuenta al interpretar el alcance del artículo 7 de dicha Carta. De ello se desprende que, si el Tribunal General considerase pertinente la sentencia *Big Brother Watch* en el presente asunto, las consideraciones formuladas por el TEDH en dicha sentencia, en relación con el alcance del artículo 8 del CEDH, deberían tenerse en cuenta al interpretar el alcance del artículo 7 de dicha Carta.

132 A este respecto, cabe recordar que, en la sentencia *Big Brother Watch*, el TEDH se pronunció sobre la legalidad de las interceptaciones masivas por parte de los servicios de inteligencia británicos de comunicaciones electrónicas y de los datos de comunicaciones asociados que se llevaron a cabo en principio fuera de las Islas Británicas.

133 Sin embargo, como señalaron las partes en el presente asunto en su respuesta a la diligencia de ordenación del procedimiento y en la vista, las alegaciones formuladas por el TEDH en la sentencia *Big Brother Watch* son pertinentes en el presente caso, en la medida en que la interceptación masiva de datos personales de que se trataba en el asunto que dio lugar a dicha sentencia puede considerarse que incluye la recogida masiva que es objeto de la Decisión impugnada.

134 En primer lugar, cabe señalar que, mientras que la versión francesa de la sentencia *Big Brother Watch* utiliza la expresión «interceptación masiva» de datos, la versión inglesa utiliza la expresión «interceptación masiva», que corresponde con mayor precisión al concepto francés de «intercepción en vrac».

135 En segundo lugar, a diferencia de la interceptación selectiva, la interceptación de inteligencia controvertida en la sentencia *Big Brother Watch* fue definida por el

TEDH como aquella que no se dirigía a personas específicas y, por consiguiente, era probable que afectara a un gran número de personas y a los datos de comunicación asociados, por lo que tenía un alcance muy amplio, ya que permitía, en particular, recabar información en el contexto de inteligencia externa y detectar nuevas amenazas procedentes de actores conocidos o desconocidos. Además, según dicho Tribunal, debido a su finalidad vinculada a la protección de la seguridad nacional, la interceptación masiva era realizada generalmente por las autoridades competentes en secreto, lo que significaba que hacían pública poca o ninguna información sobre el funcionamiento del sistema (véase, en este sentido, la sentencia *Big Brother Watch*, apartado 322).

136 En tercer lugar, en la sentencia *Big Brother Watch*, el TEDH consideró que, si bien los regímenes de interceptación masiva no estaban todos diseñados según el mismo modelo y sus métodos de aplicación podían cambiar sin respetar siempre un orden cronológico estricto, la interceptación masiva era un proceso gradual que se desarrollaba, en esencia, en las cuatro etapas siguientes (en adelante, las «etapas de la interceptación»):

- a) la interceptación masiva y la retención inicial de comunicaciones electrónicas pertenecientes a un gran número de personas y de los datos de comunicaciones asociados;
- b) la aplicación de selectores específicos a las comunicaciones retenidas y a los datos de comunicaciones asociados con el fin de identificar las comunicaciones que probablemente sean de interés para los servicios de inteligencia;
- (c) la revisión por parte de analistas de comunicaciones seleccionadas y datos de comunicaciones asociados;
- d) la conservación posterior de los datos y su utilización con el fin de incluirlos en un informe de inteligencia, comunicarlos a otros servicios de inteligencia del país o transmitirlos a servicios de inteligencia extranjeros (véase, en este sentido, la sentencia *Big Brother Watch*, apartados 325 a 329).

137 De ello se desprende que una operación de recogida masiva de datos personales, como la que es objeto de la Decisión impugnada, está comprendida en el ámbito de aplicación de la primera de las etapas de interceptación identificadas por el TEDH en la sentencia *Big Brother Watch*, en la medida en que consiste en recoger, con fines de protección de la seguridad nacional, datos personales en tránsito desde la Unión de un gran número de personas.

138 En este contexto, las consecuencias de la sentencia *Big Brother Watch* deben extraerse en el contexto de la evaluación de la legalidad de una decisión de adecuación adoptada sobre la base del artículo 45(3) del RGPD, como la decisión impugnada.

139 A este respecto, en primer lugar, cabe señalar que, en la sentencia *Big Brother Watch*, el TEDH aclaró que el artículo 8 del CEDH no prohibía el uso de la interceptación masiva para proteger la seguridad nacional u otros intereses nacionales esenciales contra amenazas externas graves y que los Estados disfrutaban de un amplio margen de apreciación para determinar el tipo de régimen de interceptación que necesitaban (sentencia *Big Brother Watch*, apartado 347).

140 En segundo lugar, el TEDH indicó que la interceptación masiva de datos personales debe regirse por varias garantías de extremo a extremo que, en conjunto, constituyen la piedra angular de cualquier sistema de interceptación masiva, a saber:

- obtener la autorización de una autoridad independiente tan pronto como se hayan definido el objetivo y el alcance de la operación de vigilancia de que se trate (sentencia *Big Brother Watch*, apartado 350);
- el establecimiento de un sistema de supervisión y control judicial *ex post* independiente (véase, en este sentido, la sentencia *Big Brother Watch*, apartados 336 y 347);
- la previsión de normas jurídicas que permitieran garantizar, en cada una de las fases de la interceptación, la necesidad y la proporcionalidad de las medidas adoptadas (véase, en este sentido, la sentencia *Big Brother Watch*, apartado 350); a este respecto, el Tribunal recordó que una injerencia en los derechos garantizados por el artículo 8 del CEDH solo podía justificarse con arreglo al apartado 2 de dicho artículo si estaba prevista por la ley, perseguía uno o varios de los fines legítimos enumerados en dicho apartado y era necesaria, en una sociedad democrática, para alcanzar dichos fines; no obstante, en materia de vigilancia secreta, la previsibilidad de las medidas adoptadas implicaba que el Derecho interno era suficientemente claro para indicar adecuadamente a todos en qué circunstancias y bajo qué condiciones las autoridades públicas estaban legitimadas para recurrir a tales medidas (sentencia *Big Brother Watch*, apartados 332 y 333).

141 En tercer lugar, el TEDH sostuvo que, si bien el artículo 8 del CEDH se aplicaba a cada una de las etapas de la interceptación, la necesidad de establecer garantías aumentaba a medida que el proceso avanzaba por estas diferentes etapas y, en consecuencia, a medida que se intensificaba la injerencia en el derecho al respeto a la vida privada. Por lo tanto, en su opinión, es al final del proceso, cuando se analiza la información relativa a una persona en particular o un analista examina el contenido de las comunicaciones, cuando la presencia de garantías es más necesaria que nunca (véase, en este sentido, *Big Brother Watch*, apartados 330 y 331).

142 En cuarto lugar, el TEDH consideró que, dado que incluir todos los selectores empleados por las agencias de inteligencia para filtrar las comunicaciones recogidas

en el ámbito de aplicación de la autorización previa no era factible en la práctica, el ámbito de aplicación de dicha autorización debía limitarse para incluir al menos los tipos o categorías de selectores que debían utilizarse (sentencia *Big Brother Watch*, apartado 354).

143 En el presente caso, en primer lugar, procede recordar que, como declaró el Tribunal de Justicia en las sentencias *Schrems I* y *Schrems II*, la Comisión no está obligada, en el marco de una decisión de adecuación, a garantizar que las disposiciones pertinentes del tercer país sean idénticas a las vigentes en la Unión, sino que sean sustancialmente equivalentes (véanse los apartados 19 y 20 *supra*).

144 Por otra parte, cabe considerar que, dado que la recopilación masiva de datos personales realizada por las agencias de inteligencia estadounidenses, controvertida en el presente procedimiento, puede asimilarse a la interceptación de datos realizada en el contexto de la primera de las etapas de interceptación especificadas por el TEDH en la sentencia *Big Brother Watch*, la necesidad de prever, para esta fase específica de la recopilación masiva, garantías que limiten la discrecionalidad de las agencias de inteligencia es más limitada, teniendo en cuenta el contexto en el que se lleva a cabo la interceptación. En efecto, lo que se discute en el presente caso es únicamente la interceptación masiva inicial de datos personales por parte de las agencias de inteligencia, con exclusión de las actividades posteriores, que no son objeto de esta acción y que podrían consistir, según el caso, en la aplicación de selectores específicos, en el examen de los datos recopilados y en su posterior uso o divulgación.

145 De ello se desprende que la disposición sobre autorización previa no es la única salvaguardia que debe rodear la interceptación masiva de datos personales, sino que constituye uno de los elementos que, en conjunto, constituyen la piedra angular de cualquier régimen de interceptación masiva. A este respecto, cabe recordar que el Derecho estadounidense vigente establece normas jurídicas que regulan de forma suficientemente clara y precisa la ejecución, por parte de las agencias de inteligencia estadounidenses, de la recopilación masiva de datos personales (véanse los apartados 107 a 116 *supra*) y otorga a las personas afectadas por la transferencia de sus datos el derecho a un recurso judicial efectivo ante la DPRC (véanse los apartados 33 a 63 *supra*). Además, los considerandos 162 a 169 de la Decisión impugnada indican, sin que la demandante lo discuta, que las actividades de inteligencia llevadas a cabo por las agencias de inteligencia están controladas por la PCLOB, que, como se desprende del apartado 54 *supra*, fue concebida por su estatuto constitutivo como una agencia independiente. Asimismo, estas actividades están sujetas a supervisión, en primer lugar, por los oficiales jurídicos y delegados que, dentro de cada agencia de inteligencia, son responsables de vigilar y asegurar el cumplimiento de esta ley; en segundo lugar, por el Inspector General independiente encargado de supervisar las actividades de inteligencia exterior de cada agencia de inteligencia; y en tercer lugar, por la Junta de Supervisión de Inteligencia (Estados

Unidos), establecida dentro de la Junta Asesora de Inteligencia del Presidente (Estados Unidos) y requerida para supervisar el cumplimiento de la ley por parte de las autoridades de los Estados Unidos; y en cuarto lugar, por los comités especiales establecidos dentro del Congreso de los Estados Unidos que ejercen funciones de supervisión respecto de todas las actividades de inteligencia exterior de este país.

146 A la luz de estas consideraciones, no puede concluirse que el hecho de no prever una autorización previa aplicable a la recogida masiva inicial, por parte de las agencias de inteligencia estadounidenses, de datos personales en tránsito desde la Unión sea suficiente para considerar que el Derecho estadounidense no ofrece, a la luz de las enseñanzas extraídas de la sentencia *Big Brother Watch*, garantías sustancialmente equivalentes a las previstas por el Derecho de la Unión.

147 Por consiguiente, este argumento debe rechazarse.

4) *Sobre el cuarto argumento, basado en el Dictamen 5/2023 del Supervisor Europeo de Protección de Datos*

148 En su cuarto argumento, la demandante alega que, en su Dictamen 5/2023, de 28 de febrero de 2023, sobre el proyecto de Decisión de Ejecución de la Comisión por la que se establece el nivel adecuado de protección de datos personales garantizado por el marco de protección de datos UE-EE. UU. («Dictamen 5/2023»), el Comité Europeo de Protección de Datos («SEPD») destacó la importancia de que la recopilación masiva de datos personales esté sujeta a autorización previa. En su opinión, la recopilación masiva de datos personales en tránsito desde la Unión por parte de las agencias de inteligencia estadounidenses no está, en el presente caso, sujeta a autorización previa.

149 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate el argumento del demandante.

150 Cabe señalar que el SEPD emitió el Dictamen 5/2023 con fundamento en el artículo 70, apartado 1, letra s), del RGPD. Esta disposición establece que, por iniciativa propia o a petición de la Comisión, el SEPD podrá emitir, en beneficio de esta última, un dictamen sobre la evaluación de la adecuación del nivel de protección garantizado por un tercer país.

151 Sin embargo, al actuar sobre la base del artículo 70, apartado 1, del RGPD, el SEPD se limita a ejercer una función consultiva mediante la elaboración de dictámenes, directrices, recomendaciones y recomendaciones de mejores prácticas que no producen efectos jurídicos vinculantes (véase, en este sentido, el auto del Presidente del Tribunal de Justicia de 29 de noviembre de 2023, SEPD/CRU, C-413/23 P, no publicado, EU:C:2023:1036, apartado 11). Por lo tanto, dicho dictamen no es vinculante para la Comisión, que sigue teniendo libertad para

evaluar si el Derecho de dicho país ofrece, en general, un nivel de protección sustancialmente equivalente al garantizado por el Derecho de la Unión en lo que respecta a la recogida masiva de datos personales. En cualquier caso, cabe señalar que, en dicho dictamen, el SEPD no indicó que la falta de establecimiento de un control previo en relación con la recogida masiva de datos personales socavara necesariamente la evaluación positiva de la Comisión sobre la adecuación del nivel de protección de los datos personales ofrecido por el DPC. Por el contrario, señaló, en el párrafo 165 de dicha opinión, que dicha evaluación dependía de todas las circunstancias del caso y, en particular, del establecimiento por los Estados Unidos de un control judicial ex post y de un mecanismo de revisión.

152 En este contexto, el Dictamen 5/2023 no permite concluir que la recogida masiva por parte de las agencias de inteligencia estadounidenses de datos personales en tránsito desde la Unión deba estar sujeta a autorización previa y que la protección ofrecida por dicho país no sea sustancialmente equivalente a la garantizada por el Derecho de la Unión.

153 Por consiguiente, debe rechazarse este argumento y, en consecuencia, la segunda queja del segundo motivo en su totalidad.

(d) Sobre la tercera queja del segundo fundamento, según la cual la Orden Ejecutiva 14086 otorga al Presidente de los Estados Unidos la facultad de autorizar una actualización secreta de los objetivos específicos de la recopilación masiva

154 Mediante la tercera alegación de su segundo motivo, el demandante sostiene que la Comisión infringió los artículos 7 y 8 de la Carta de los Derechos Fundamentales al considerar, en la Decisión impugnada, que Estados Unidos de América ofrecía un nivel de protección sustancialmente equivalente al garantizado por el Derecho de la Unión en virtud del RGPD, interpretado a la luz de dicha Carta, a pesar de que la EO 14086 otorga al Presidente de los Estados Unidos, por razones de seguridad nacional, la facultad de autorizar una actualización secreta de los fines específicos de la recogida masiva. Más concretamente, considera que, contrariamente a lo establecido en la sentencia del TEDH de 4 de diciembre de 2015, *Roman Zakharov c. Rusia* (CE:ECHR:2015:1204JUD004714306, en adelante, la “sentencia Zakharov”), la concesión del poder de actualizar estos fines específicos a dicho Presidente no permite a las personas afectadas por una transferencia de datos personales identificar, de manera precisa, el marco legal en el que se procesan sus datos personales en Estados Unidos.

155 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate los argumentos del demandante.

156 Cabe señalar que, en la sentencia Zakharov, el TEDH sostuvo que una injerencia en el derecho fundamental al respeto de la vida privada y familiar solo podía

justificarse en virtud del artículo 8(2) del CEDH si estaba prescrita por ley (sentencia Zakharov, apartado 227). Sin embargo, según dicho Tribunal, la expresión «prescrita por ley» significaba que la medida en cuestión debía ser accesible a la persona interesada y que sus efectos debían ser previsibles (sentencia Zakharov, apartado 228). En el caso de la interceptación de comunicaciones, la «previsibilidad» no significaba que una persona tuviera que poder prever cuándo era probable que las autoridades interceptaran sus comunicaciones, sino que, en esencia, las limitaciones a su derecho al respeto de la vida privada y familiar debían resultar de normas claras (sentencia Zakharov, apartado 229).

157 Asimismo, procede recordar que, de conformidad con la jurisprudencia citada en el apartado 29 supra, en la medida en que el artículo 8 del CEDH consagra, al igual que el artículo 7 de la Carta de los Derechos Fundamentales, el derecho al respeto de la vida privada y familiar, la jurisprudencia del TEDH relativa al artículo 8 del CEDH, incluida por tanto la sentencia Zakharov, debe tenerse en cuenta al interpretar, como en el presente caso, el artículo 7 de dicha Carta.

158 A este respecto, del artículo 2(c)(ii)(C) de la Orden Ejecutiva 14086 se desprende claramente que la facultad otorgada al Presidente de los Estados Unidos para actualizar la lista de fines específicos para la recopilación masiva no es ilimitada, sino que se limita a los casos en que dicha actualización sea necesaria debido a la aparición de nuevos imperativos de seguridad nacional, como nuevas o mayores amenazas a la seguridad nacional para las que se podría utilizar la recopilación masiva de datos personales. Asimismo, de dicha disposición se desprende, y fue confirmado por los Estados Unidos de América en la audiencia, que la actualización por parte del Presidente de dichos fines específicos no es secreta, sino que es objeto de publicidad por parte del Director de Inteligencia Nacional, a menos que dicho Presidente considere que dicha publicidad constituye en sí misma un riesgo para la seguridad nacional de su país. Asimismo, incluso en esta hipótesis, la recopilación masiva está sujeta a todas las garantías y limitaciones previstas en la Orden Ejecutiva 14086 y, si un titular de los datos presenta una queja relativa a sus datos personales, esta está sujeta a la supervisión de la CLPO y, de ser necesario, a la revisión de la DPRC.

159 En este contexto, no se puede considerar que el poder otorgado al Presidente de los Estados Unidos para actualizar la lista de propósitos específicos de la recolección masiva sea contrario a los requisitos identificados por el TEDH en la sentencia Zakharov.

160 Por consiguiente, procede desestimar la tercera alegación del segundo motivo y, en consecuencia, dicho motivo en su totalidad.

4. *Sobre el cuarto motivo, basado en la infracción del artículo 22 del RGPD*

161 Mediante su cuarto motivo, la demandante alega que la Comisión infringió el artículo 22 del RGPD en la medida en que, en la Decisión impugnada, no incluyó una disposición que establezca el derecho de los interesados a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado de datos personales, incluida la elaboración de perfiles, que produzcan efectos jurídicos sobre ellos o les afecten significativamente (en lo sucesivo, «decisiones totalmente automatizadas»).

162 Como punto preliminar, cabe señalar que los términos del artículo 22 del RGPD son los siguientes:

1. El interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de forma similar.

2. El apartado 1 no se aplicará cuando la decisión:

(a) sea necesario para la celebración o ejecución de un contrato entre el interesado y el responsable del tratamiento;

b) esté autorizado por el Derecho de la Unión o de los Estados miembros al que esté sujeto el responsable del tratamiento y que también establezca medidas adecuadas para salvaguardar los derechos y libertades del interesado y sus intereses legítimos; o

(c) se basa en el consentimiento explícito del interesado.

163 Cabe señalar también que el término «elaboración de perfiles», que aparece en el artículo 22(1) del RGPD, se define en el artículo 4(4) del mismo reglamento como «cualquier forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales relacionados con una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de dicha persona».

164 De ello se desprende que, en virtud del artículo 22 del RGPD, todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos personales, incluso cuando esta medida consista en analizar y predecir determinados aspectos de su comportamiento.

165 Sin embargo, de la Decisión impugnada se desprende claramente que no aborda específicamente la cuestión relativa a las decisiones totalmente automatizadas.

166 Por tanto, procede decidir si tal omisión puede afectar a la legalidad de la Decisión impugnada, en la medida en que podría poner en tela de juicio la conclusión establecida en el artículo 1^{de} dicha Decisión, según la cual los Estados Unidos de América ofrecen un nivel adecuado de protección de datos personales.

167 Es en este contexto en el que procede analizar las tres alegaciones formuladas por el demandante en apoyo de su cuarto motivo, comenzando por la primera y la tercera alegaciones, que deben examinarse conjuntamente.

a) *Sobre las alegaciones primera y tercera del cuarto motivo de casación, según las cuales, por una parte, el hecho de que las decisiones totalmente automatizadas sean adoptadas generalmente por responsables del tratamiento que, estando establecidos en la Unión, están sujetos al RGPD no ofrece una garantía con respecto a otros casos y, por otra parte, el establecimiento, por el Derecho de los Estados Unidos, de protecciones sectoriales en los casos en que la adopción de decisiones totalmente automatizadas no entra en el ámbito de aplicación de dicho Reglamento es irrelevante en el presente caso.*

168 Mediante las alegaciones primera y tercera de su cuarto motivo, el demandante alega, en primer lugar, que el hecho de que las decisiones totalmente automatizadas sean adoptadas generalmente por responsables del tratamiento de datos que, al estar establecidos en la Unión, están sujetos al RGPD, no ofrece garantías con respecto a otros casos. En segundo lugar, señala que el hecho de que el Derecho estadounidense ofrezca protecciones sectoriales en caso de que la adopción de dichas decisiones no esté comprendida en el ámbito de aplicación de dicho Reglamento es irrelevante en el presente caso, ya que dicha circunstancia no permite concluir que, en general, la protección que ofrece dicho país respecto a todas las decisiones totalmente automatizadas sea equivalente a la garantizada por el artículo 22 de dicho Reglamento.

169 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate los argumentos de la demandante.

170 Es preciso señalar que del considerando 33 de la Decisión impugnada se desprende claramente que, en caso de transferencia de datos personales de la Unión a los Estados Unidos, deben distinguirse tres supuestos en lo que respecta a la adopción de decisiones totalmente automatizadas.

171 En primer lugar, es posible que las decisiones totalmente automatizadas sean adoptadas por un responsable del tratamiento establecido en la Unión que haya recopilado, en la Unión, los datos personales de los interesados. A este respecto, cabe señalar que el artículo 4, apartado 7, del RGPD define al responsable del tratamiento como la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento

de datos personales. En este caso, en la medida en que, de conformidad con el artículo 3, apartado 1, de dicho Reglamento, el responsable del tratamiento esté sujeto al mismo Reglamento, deberá cumplir los requisitos establecidos en el artículo 22 de dicho Reglamento en relación con dichas decisiones.

172 En segundo lugar, puede ocurrir que las decisiones totalmente automatizadas sean adoptadas bien por un encargado del tratamiento establecido en un tercer país, que actúe en nombre del responsable del tratamiento establecido en la Unión que le transfirió los datos personales que recopiló en la Unión, o bien por un subencargado del tratamiento, que actúe en nombre del encargado del tratamiento establecido en la Unión que le transfirió los datos que recopiló en la Unión. A este respecto, cabe señalar que el artículo 4, apartado 8, del RGPD define al encargado del tratamiento como la persona física o jurídica, autoridad pública, agencia u otro organismo que trate datos personales por cuenta del responsable del tratamiento. En estos casos, en la medida en que los encargados extranjeros actúen por cuenta del responsable o del encargado en la Unión, estarán sujetos a dicho reglamento en virtud de su artículo 3, apartado 1. Por lo tanto, con respecto a dichas decisiones, el responsable y el encargado del tratamiento deberán cumplir los requisitos previstos en el artículo 22 del mismo reglamento.

173 En tercer lugar, puede ocurrir que un responsable o encargado del tratamiento no establecido en la Unión adopte decisiones totalmente automatizadas, pero que se dirige a interesados que se encuentran en ella ofreciéndoles bienes o servicios o monitorizando su comportamiento. En este caso, el artículo 3, apartado 2, del RGPD establece que el responsable y el encargado extranjeros están sujetos a dicho reglamento. Por lo tanto, en el caso de decisiones totalmente automatizadas, deben cumplir los requisitos establecidos en el artículo 22 de dicho reglamento.

174 De ello se desprende que de la Decisión impugnada se desprende que los casos en los que las decisiones totalmente automatizadas no entran en el ámbito de aplicación del artículo 22 del RGPD son residuales y se limitan al caso en que las organizaciones de CPD recopilan datos personales directamente en la Unión, sin ofrecer, no obstante, a los ciudadanos de la Unión bienes o servicios y sin supervisar su comportamiento, en el sentido del artículo 3, apartado 2, de dicho Reglamento.

175 Sin embargo, de los considerandos 35 y 36 de la Decisión impugnada se desprende, sin que la demandante lo cuestione, que, en esos casos, el Derecho de los Estados Unidos ofrece protecciones sectoriales similares a las previstas por el RGPD en ámbitos como la concesión de créditos, las ofertas de préstamos inmobiliarios, las decisiones de contratación, el empleo, la vivienda y los seguros, en los que es más probable que las organizaciones de CPD adopten decisiones totalmente automatizadas.

- 176 Así, en materia de crédito al consumo, la Ley de Informes Crediticios Justos y la Ley de Igualdad de Oportunidades de Crédito contienen salvaguardas que otorgan a los consumidores un derecho a una explicación y a impugnar decisiones totalmente automatizadas. Estas leyes se aplican a una amplia gama de áreas, como crédito, empleo, vivienda y seguros. Además, el Título VII de la Ley de Derechos Civiles y la Ley de Vivienda Justa protegen a las personas de los patrones utilizados en decisiones totalmente automatizadas que podrían resultar en discriminación basada en ciertas características y les otorgan el derecho a impugnar dichas decisiones. Asimismo, con respecto a la información sanitaria, las normas adoptadas por las autoridades estadounidenses en virtud de la Ley de Portabilidad y Responsabilidad del Seguro Médico exigen que los proveedores de servicios médicos reciban información que les permita informar a las personas sobre los sistemas de toma de decisiones totalmente automatizadas utilizados en el sector médico.
- 177 En este contexto, contrariamente a lo que alega la demandante, no puede considerarse que las protecciones sectoriales previstas por el Derecho de los Estados Unidos sean irrelevantes en el presente caso, ya que no tienen el mismo alcance general que el artículo 22 del RGPD.
- 178 A este respecto, procede recordar que, en las sentencias Schrems I y Schrems II, el Tribunal de Justicia declaró que, sin exigir al tercer país de que se trate que garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión, la expresión «nivel de protección adecuado», que figura en el artículo 45, apartado 1, del RGPD, debe entenderse en el sentido de que exige que ese tercer país garantice efectivamente, mediante su Derecho interno o sus compromisos internacionales, un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado en la Unión por dicho Reglamento, interpretado a la luz de la Carta de los Derechos Fundamentales (véanse los apartados 19 y 20 supra).
- 179 Además, en la sentencia Schrems I, el Tribunal de Justicia consideró que, si bien los medios utilizados por el tercer país para garantizar un nivel adecuado de protección de los datos personales pueden ser diferentes de los aplicados en la Unión, dichos medios deben, no obstante, resultar eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión (véase el apartado 20 supra).
- 180 En vista de todas estas consideraciones, procede desestimar las alegaciones primera y tercera del cuarto motivo.
- b) *Sobre la segunda alegación del cuarto motivo, según la cual el estudio encargado por la Comisión en 2018, que demostró el carácter residual de los casos en los que las organizaciones establecidas en Estados Unidos que se habían adherido*

al escudo de protección adoptaron decisiones totalmente automatizadas, es irrelevante en el presente caso

181 Mediante la segunda alegación de su cuarto motivo, el demandante alega que el hecho de que el estudio sobre decisiones totalmente automatizadas, citado en el considerando 34 de la Decisión impugnada, que la Comisión encargó en 2018 y cuyos resultados se exponen en el punto 4.1.5 del Informe COM(2018) 860 final de la Comisión al Parlamento Europeo y al Consejo, de 19 de diciembre de 2018, sobre la segunda revisión anual del funcionamiento del Escudo de la privacidad (en lo sucesivo, «estudio de 2018»), concluyera que no existían pruebas de la existencia de decisiones totalmente automatizadas adoptadas por organizaciones establecidas en Estados Unidos que se habían adherido al Escudo de la privacidad es irrelevante en el presente caso. En particular, alega que dicho estudio se refiere a la decisión de adecuación relativa al Escudo de la privacidad que fue anulada por el Tribunal de Justicia en la sentencia Schrems II y que no tiene en cuenta la situación actual, que se caracteriza por un desarrollo extremadamente rápido de servicios totalmente automatizados basados en inteligencia artificial.

182 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate los argumentos del demandante.

183 Del estudio de 2018 se desprende en particular que, por una parte, en ese momento no existían datos que permitieran pensar que las empresas establecidas en Estados Unidos que se habían adherido al escudo de protección hubieran adoptado decisiones totalmente automatizadas y, por otra parte, Estados Unidos de América había aplicado una legislación sectorial en ámbitos como el crédito al consumo, el empleo, la vivienda, los seguros y la salud, en los que era más probable que se adoptaran decisiones totalmente automatizadas.

184 A este respecto, en primer lugar, cabe señalar que el estudio de 2018 no se cita en la decisión de adecuación relativa al Escudo de Privacidad y fue encargado por la Comisión tras la entrada en vigor de dicha decisión. Por lo tanto, el hecho de que el Tribunal anulara dicha decisión en el asunto Schrems II es irrelevante en el presente caso. Además, en el asunto Schrems II, el Tribunal no anuló dicha decisión basándose en los elementos indicados en dicho estudio.

185 En segundo lugar, es cierto que el estudio de 2018 no tuvo en cuenta la situación fáctica y jurídica de Estados Unidos en 2023, fecha de adopción de la decisión impugnada, sino la situación en 2018, cuando se llevó a cabo. Sin embargo, el carácter residual de los casos en los que las organizaciones establecidas en Estados Unidos que se habían adherido al Escudo de la Privacidad habían adoptado decisiones totalmente automatizadas fue confirmado por el informe COM(2019) 495 final de la Comisión al Parlamento Europeo y al Consejo, de 23 de octubre de 2019, sobre la tercera revisión anual del funcionamiento del Escudo de la

Privacidad. En efecto, en dicho informe se afirmaba, entre otras cosas, que el número de organizaciones establecidas en Estados Unidos que participaban en el Escudo de la Privacidad que habían adoptado decisiones totalmente automatizadas era limitado y que las decisiones adoptadas por dichas organizaciones, por lo general, no tenían efectos jurídicos ni producían otros efectos respecto de los interesados.

186 En tercer lugar, debe señalarse que, en sus alegaciones, el demandante no ha aportado ninguna prueba que sugiera que, tras la realización del estudio de 2018, las organizaciones establecidas en Estados Unidos adoptaron decisiones totalmente automatizadas y no ha explicado de manera jurídica suficiente por qué el desarrollo de la inteligencia artificial haría que dicho estudio fuera irrelevante.

187 En este contexto, procede desestimar la segunda imputación del cuarto motivo y, por tanto, dicho motivo en su totalidad.

5. Sobre el quinto motivo, basado en la infracción del artículo 32 del RGPD, en relación con el artículo 45, apartado 2, del mismo Reglamento

188 Mediante su quinto motivo, la demandante alega que la Comisión infringió el artículo 32 del RGPD, en relación con el artículo 45, apartado 2, de dicho Reglamento, en la medida en que, en la Decisión impugnada, consideró que Estados Unidos de América ofrecía un nivel de protección sustancialmente equivalente al garantizado en la Unión Europea en lo que respecta a la aplicación, por parte de los responsables y encargados del tratamiento establecidos en Estados Unidos, de medidas técnicas y organizativas adecuadas para garantizar la seguridad del tratamiento de datos personales transferidos desde la Unión Europea a dicho país.

189 A este respecto, en primer lugar, la demandante alega que el punto II.4, letra a), del anexo 1 de la Decisión impugnada se limita a establecer que las organizaciones de CPD deben adoptar medidas de seguridad razonables y adecuadas exclusivamente cuando creen, mantengan, utilicen o difundan datos personales. Por lo tanto, no se exigen medidas de seguridad cuando dichas organizaciones consultan datos personales procedentes de la Unión. La demandante sostiene, no obstante, que la consulta es una de las operaciones incluidas en el concepto de «tratamiento» de datos personales del artículo 4, apartado 2, del RGPD.

190 En segundo lugar, la demandante sostiene que el punto III.6, letra f), del anexo 1 de la Decisión impugnada establece una obligación para las organizaciones establecidas en Estados Unidos que abandonan la DPC de seguir cumpliendo los principios establecidos en dicha Decisión, incluidos los relativos a la seguridad del tratamiento, mientras almacenen, utilicen o divulguen datos personales transferidos de la Unión a Estados Unidos, pero no establece tal obligación cuando esas mismas organizaciones consulten datos personales.

191 La Comisión, apoyada por Irlanda y los Estados Unidos de América, rebate los argumentos del demandante.

192 A modo de punto preliminar, en primer lugar, conviene recordar que los términos del artículo 32 del RGPD son los siguientes:

1. Teniendo en cuenta el estado de la técnica, los costes de implementación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos, cuya probabilidad y gravedad varían, para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, entre otras, según corresponda:

(a) seudonimización y cifrado de datos personales;

b) medios para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de procesamiento;

(c) medios para restablecer la disponibilidad y el acceso a los datos personales dentro de plazos adecuados en caso de un incidente físico o técnico;

(d) un procedimiento para probar, analizar y evaluar periódicamente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar el nivel adecuado de seguridad, se tendrán especialmente en cuenta los riesgos que presente el tratamiento, en particular la destrucción, pérdida, alteración, divulgación o acceso no autorizados, accidentales o ilícitos, de datos personales transmitidos, conservados o tratados de otro modo.

193 A continuación, el término «tratamiento», que aparece en el artículo 32 del RGPD, se define en el artículo 4, apartado 2, del mismo reglamento 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, el registro, la organización, la estructuración, la conservación, la adaptación o la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, la difusión o cualquier otra forma de habilitación de acceso, el cotejo o la interconexión, la limitación, la supresión o la destrucción».

194 Según la jurisprudencia, de la expresión «cualquier operación» que figura en el artículo 4, apartado 2, del RGPD se desprende, en particular, que el legislador de la Unión quiso dar al concepto de «tratamiento» un alcance amplio, lo que se corrobora por el carácter no exhaustivo, expresado por la expresión «como», de las operaciones enumeradas en dicha disposición (véase la sentencia de 7 de marzo de

2024, Endemol Shine Finland, C-740/22, EU:C:2024:216, apartado 29 y jurisprudencia citada).

195 Por último, cabe señalar que, entre los factores que la Comisión debe tener en cuenta al evaluar, de conformidad con el artículo 45(2)(a) del RGPD, el nivel de protección ofrecido por un tercer país, se encuentran las medidas de seguridad relativas a los datos personales implementadas por dicho país.

196 Es en este contexto que procede examinar conjuntamente los dos argumentos formulados por la demandante en apoyo del presente motivo.

197 A este respecto, procede recordar que el tenor del punto II.4, letra a), del anexo 1 de la Decisión impugnada es el siguiente:

“Las organizaciones que crean, gestionan, utilizan o difunden datos personales deben adoptar medidas razonables y adecuadas para evitar la pérdida, el uso indebido, el acceso ilícito, la divulgación, la alteración y la destrucción de dichos datos, teniendo debidamente en cuenta los riesgos asociados al tratamiento y la naturaleza de los datos personales”.

198 Además, los términos del punto III.6, letra f), del anexo 1 de la Decisión impugnada son los siguientes:

Una organización debe aplicar los Principios a todos los datos personales recibidos de la Unión en virtud del [CPD]. El compromiso de adhesión a los Principios no tiene límite temporal respecto a los datos personales recibidos durante el periodo en que la organización se beneficia del [CPD]; dicho compromiso implica que continuará aplicando los Principios a dichos datos mientras los almacene, utilice o divulgue, incluso si posteriormente abandona el [CPD] por cualquier motivo.

199 De ello se desprende que los puntos II.4, letra a), y III.6, letra f), del anexo 1 de la Decisión impugnada no se refieren a ningún tipo de tratamiento de datos personales, en el sentido del artículo 4, apartado 2, del RGPD. Por el contrario, por una parte, el primero de estos puntos limita la obligación de las organizaciones del CPD de adoptar medidas de seguridad únicamente a los casos en que creen, gestionen, utilicen o difundan datos personales. Por otra parte, el segundo de estos puntos establece que las organizaciones que abandonen el CPD deben seguir aplicando los principios establecidos en la Decisión impugnada mientras almacenen, utilicen o divulguen datos personales transferidos de la Unión Europea a Estados Unidos.

200 Sin embargo, en primer lugar, cabe recordar que, en las sentencias Schrems I y Schrems II, el Tribunal de Justicia declaró que no era necesario que el tercer país garantizara una protección jurídica idéntica a la garantizada en el ordenamiento jurídico de la UE (véanse los apartados 19 y 20 supra). De ello se desprende que, si en la Decisión impugnada la Comisión considera que el Derecho estadounidense

vigente en el momento de su adopción garantiza un nivel de protección sustancialmente equivalente al previsto en el Derecho de la UE, no es necesario que dicha decisión contenga exactamente los mismos términos que los que figuran en el RGPD.

- 201 En segundo lugar, los principios enunciados en el punto II.4, letra a), del anexo 1 de la Decisión impugnada deben interpretarse a la luz de los elementos que figuran en el considerando 23 de dicha Decisión, que, al igual que el artículo 32 del RGPD, dispone lo siguiente:

Los datos personales también deben tratarse de forma que se garantice su seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daños accidentales. Para ello, los responsables y encargados del tratamiento deben adoptar las medidas técnicas u organizativas adecuadas para proteger los datos personales frente a posibles amenazas. Estas medidas deben evaluarse teniendo en cuenta el estado de la técnica, los costes pertinentes, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos de las personas.

- 202 En tercer lugar, procede señalar que los términos «crear», «gestionar», «utilizar» y «difundir» del punto II.4, letra a), del anexo 1 de la Decisión impugnada y los términos «almacenar», «utilizar» y «divulgar» del punto III.6, letra f), del mismo anexo constituyen manifestaciones específicas de la operación consistente en el «tratamiento» de datos personales, en el sentido del artículo 32 del RGPD, y que, al igual que dicho artículo, pretenden abarcar una amplia gama de operaciones relativas a datos personales.

- 203 En cuarto lugar, el término «utilización», que figura tanto en el punto II.4, letra a), del anexo 1 de la Decisión impugnada como en el punto III.6, letra f), del mismo anexo, se define como el acto de usar algo para un fin o uso específico. Desde esta perspectiva, la utilización de datos personales incluye su consulta, ya que, por definición, para poder utilizar los datos, es necesario primero tener acceso a ellos y, por lo tanto, consultarlos. De ello se desprende que el argumento de la demandante de que no se exigen medidas de seguridad en la Decisión impugnada cuando las organizaciones de DPC consultan datos personales procedentes de la Unión carece de fundamento.

- 204 En vista de todos estos elementos, procede desestimar el quinto motivo y, por tanto, el recurso en su totalidad.

IV. Costas

- 205 A tenor del artículo 134(1) del Reglamento de Procedimiento, la parte que pierda el proceso será condenada en costas, si así lo hubiera solicitado la otra parte.

206 Dado que la Comisión concluyó que el demandante debía ser condenado y que éste no ha prosperado, debe condenarse a éste a soportar, además de sus propias costas, las de la Comisión, incluso en el marco del procedimiento provisional.

207 Además, de conformidad con el artículo 138, apartado 1, del Reglamento de Procedimiento, los Estados miembros y las instituciones coadyuvantes en el procedimiento soportarán sus propias costas. Por consiguiente, Irlanda soportará las suyas.

208 Además, de conformidad con el artículo 138(3) del Reglamento de Procedimiento, la Corte podrá ordenar que una parte interviniente distinta de las mencionadas en los párrafos 1 y 2 de dicho artículo cargue con sus propias costas. En el presente caso, procede ordenar que Estados Unidos de América cargue con sus propias costas.

Por estas razones,

EL TRIBUNAL (Sala Décima, Ampliada)

declara y ordena:

- 1) Se desestima el recurso.*
- 2) El Sr. Philippe Latombe cargará con sus propias costas y con las de la Comisión Europea, incluso en el marco del procedimiento provisional.*
- 3) Irlanda soportará sus propias costas.*
- 4) Los Estados Unidos de América soportarán sus propios costos.*

Porchia

Jaeger

Madise

Nihoul

Verschuur

Así pronunciado en audiencia pública en Luxemburgo el 3 de septiembre de 2025.

El empleado

El Presidente

V. Di Bucci

O. Porchia