Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL GENERAL (Sala Sexta ampliada)

de 8 de enero de 2025 *

[Texto rectificado mediante auto de 3 de junio de 2025]

«Tratamiento de datos personales — Protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión — Reglamento (UE) 2018/1725 — Concepto de "transferencia de datos personales a terceros países" — Transferencia de datos con ocasión de la consulta de un sitio de Internet — EU Login — Recurso de anulación — Acto no recurrible — Inadmisibilidad — Recurso por omisión — Definición de posición que pone fin a la omisión — Sobreseimiento — Recurso de indemnización — Violación suficientemente caracterizada de una norma jurídica que confiere derechos a los particulares — Relación de causalidad — Daños y perjuicios inmateriales»

En el asunto T-354/22,

Thomas Bindl, con domicilio en Múnich (Alemania), representado por el Sr. T. Herbrich, abogado,

parte demandante,

contra

Comisión Europea, representada por los Sres. A. Bouchagiar, B. Hofstötter y H. Kranenborg, en calidad de agentes,

parte demandada,

EL TRIBUNAL GENERAL (Sala Sexta ampliada),

integrado por la Sra. M. J. Costeira (Ponente), Presidenta, y la Sra. M. Kancheva, los Sres. U. Öberg y P. Zilgalvis y la Sra. E. Tichy-Fisslberger, Jueces;

Secretaria: Sra. S. Jund, administradora;

habiendo considerado los escritos obrantes en autos;

habiendo considerado la diligencia de ordenación del procedimiento de 21 de julio de 2023 y las respuestas de la Comisión y del demandante presentadas en la Secretaría del Tribunal General el 7 y el 8 de septiembre de 2023, respectivamente;

* Lengua de procedimiento: alemán.

celebrada la vista el 17 de octubre de 2023;

habiendo considerado la diligencia de ordenación del procedimiento de 9 de febrero de 2024 y las respuestas de la Comisión y del demandante presentadas en la Secretaría del Tribunal General el 12 y el 13 de marzo de 2024, respectivamente;

dicta la siguiente

Sentencia

1 Mediante su recurso, basado en los artículos 263 TFUE, 265 TFUE y 268 TFUE, el demandante, el Sr. Thomas Bindl, solicita al Tribunal General, en primer término, que anule aquellas transferencias de sus datos personales a terceros países que no dispongan de un nivel de protección adecuado, en segundo término, que declare que la Comisión Europea, contrariamente a Derecho, no se pronunció sobre su solicitud de información de 1 de abril de 2022 y, en tercer término, que le indemnice por los daños y perjuicios inmateriales que alega haber sufrido a raíz, por una parte, de la vulneración de su derecho de acceso a la información y, por otra parte, de las transferencias de sus datos personales.

Antecedentes del litigio y hechos posteriores a la interposición del recurso

2 El demandante es un ciudadano alemán que se interesa por determinados temas en los ámbitos de la informática y de la protección de datos personales.

3 La Dirección General de Comunicación de la Comisión es la responsable del tratamiento de datos personales a efectos del sitio de Internet de la Conferencia sobre el Futuro de Europa ubicado en la dirección «https://futureu.europa.eu» (en lo sucesivo, «sitio de Internet de la CFE»).

4 El demandante consultó el sitio de Internet de la CFE en varias ocasiones en 2021 y 2022. En particular, consultó este sitio de Internet el 30 de marzo de 2022 y se registró en el evento «GoGreen» que allí figuraba sirviéndose de su cuenta de Facebook y, el 8 de junio de 2022, volvió a consultar el citado sitio de Internet.

5 Mediante correo electrónico de 9 de noviembre de 2021 (en lo sucesivo, «solicitud de información de 9 de noviembre de 2021»), el demandante solicitó al delegado de la protección de datos de la Comisión que le facilitara cierta información en virtud del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO 2018, L 295, p. 39).

6 En dicho correo electrónico, el demandante, en primer lugar, indicó haber observado que, cuando se había conectado al sitio de Internet de la CFE, se había activado una conexión con proveedores terceros, como la empresa estadounidense Amazon Web Services; en segundo lugar, solicitó que se le indicara qué datos personales suyos habían sido tratados o almacenados y cuáles habían sido transferidos, en su caso, a terceros y, en tercer lugar, solicitó información sobre la base jurídica de esa transferencia y sobre la existencia de posibles garantías en cuanto a la transferencia a terceros países que no dispongan de un nivel de protección adecuado.

7 Mediante correo electrónico de 3 de diciembre de 2021, la Dirección General de Comunicación de la Comisión transmitió al demandante un enlace electrónico y lo informó de que ese enlace le permitía generar directamente una relación de los datos personales que habían sido tratados con ocasión de la consulta del sitio de Internet de la CFE. Además, indicó al demandante, por una parte, que sus datos personales no habían sido transferidos a destinatarios situados fuera de la Unión Europea y, por otra parte, que los almacenaba y trataba el sitio de Internet de la CFE, que utilizaba una red de distribución de contenidos gestionada por Amazon Web Services EMEA SARL (en lo sucesivo, «AWS EMEA»), con domicilio social en Luxemburgo (Luxemburgo). Precisó asimismo que, en el marco de los contratos celebrados entre la Comisión y AWS EMEA, el responsable del tratamiento de los datos no recurre a servicios que precisen transferir datos a los socios de AWS EMEA situados en los Estados Unidos y que, en principio, la transferencia de datos fuera del territorio de la Unión no está autorizada.

8 [En su versión rectificada mediante auto de 3 de junio de 2025] Mediante correo electrónico de 1 de abril de 2022, el demandante solicitó a la Comisión, con arreglo al Reglamento 2018/1725, determinada información sobre el tratamiento de sus datos (en lo sucesivo, «solicitud de información de 1 de abril de 2022»). En primer término, indicó haber observado que, cuando se había conectado al sitio de Internet de la CFE, se había establecido una conexión con proveedores terceros, como AWS EMEA, y que consideraba que se había establecido una conexión con la empresa Meta Platforms cuando hizo uso de sus datos de conexión de Facebook para registrarse en dicho sitio de Internet. En segundo término, solicitó que se le indicara qué datos personales suyos habían sido tratados o almacenados y cuáles habían sido transferidos, en su caso, a terceros. En tercer término, solicitó información sobre la base jurídica de esa transferencia y sobre la existencia de posibles garantías en cuanto a la transferencia a terceros países que no dispongan de un nivel de protección adecuado. Por último, solicitó una copia de sus datos, incluidos los almacenados o tratados por terceros, como Facebook.

9 Mediante correos electrónicos de 22 de abril y de 2 de mayo de 2022, el demandante insistió ante la Comisión para que diera respuesta a su solicitud de información de 1 de abril de 2022.

10 Mediante demanda presentada en la Secretaría del Tribunal General el 9 de junio de 2022, el demandante interpuso el presente recurso.

11 Mediante correo electrónico de 30 de junio de 2022, la Comisión informó al demandante de que consideraba que la solicitud de información de 1 de abril de 2022 era casi idéntica a la solicitud de información de 9 de noviembre de 2021 y que ya había dado respuesta a esta última mediante su correo electrónico de 3 de diciembre de 2021.

12 Amazon Web Services es una empresa domiciliada en los Estados Unidos y AWS EMEA es una empresa con domicilio social en Luxemburgo. Ambas empresas son filiales de la empresa estadounidense Amazon.com, Inc.

Pretensiones de las partes

13 El demandante solicita al Tribunal General que:

– Anule las transferencias de sus datos personales a terceros países que no dispongan de un nivel de protección adecuado que tuvieron lugar el 30 de marzo y el 8 de junio de 2022.

– Declare que la Comisión, contrariamente a Derecho, no se ha pronunciado sobre la solicitud de información de 1 de abril de 2022.

– Condene a la Comisión a abonarle la cuantía de 1 200 euros, más intereses, que corresponden, por una parte, al importe de 800 euros, como indemnización de los daños y perjuicios inmateriales sufridos a raíz de la vulneración de su derecho de acceso a la información, y, por otra parte, al importe de 400 euros, como indemnización por los daños y perjuicios inmateriales sufridos a raíz de las referidas transferencias de sus datos.

– Condene en costas a la Comisión.

14 La Comisión solicita al Tribunal General que:

– Inadmita las pretensiones de anulación y las pretensiones por omisión.

– Con carácter subsidiario, declare el sobreseimiento de las pretensiones por omisión.

– Desestime por infundadas las pretensiones de indemnización.

– Condene en costas al demandante.

Fundamentos de Derecho

Consideraciones preliminares sobre la protección de datos personales por las instituciones, órganos y organismos de la Unión

15 El artículo 16 TFUE, apartado 1, y el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta») disponen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

16 El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO 2016, L 119, p. 1), define las normas generales destinadas a proteger a las personas físicas en lo que respecta al tratamiento de los datos personales y a garantizar la libre circulación de tales datos (artículo 1, apartado 1, del Reglamento 2016/679).

17 El Reglamento 2018/1725 establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por las instituciones y organismos de la Unión y las normas relativas a la libre circulación de dichos datos entre ellos o entre ellos y destinatarios establecidos en la Unión (artículo 1, apartado 1, del Reglamento 2018/1725). Este Reglamento protege los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales (artículo 1, apartado 2, del Reglamento 2018/1725). Se aplica al tratamiento de datos personales por parte de todas las instituciones y organismos de la Unión (artículo 2, apartado 1, del Reglamento 2018/1725).

18 El considerando 5 del Reglamento 2018/1725 recuerda que, según la jurisprudencia del Tribunal de Justicia, cuando las disposiciones del Reglamento 2018/1725 apliquen los mismos principios que las disposiciones del Reglamento 2016/679, ambas deben interpretarse de manera homogénea, en particular porque debe entenderse que la estructura del Reglamento 2018/1725 es equivalente a la del Reglamento 2016/679. A este respecto, de la lectura conjunta de lo dispuesto en el artículo 2, apartado 3, del Reglamento 2016/679 y en el artículo 99 del Reglamento 2018/1725 también resulta que este último Reglamento se adapta a los principios y normas del Reglamento 2016/679.

Sobre la admisibilidad

Admisibilidad de las pretensiones de anulación

19 Mediante su primera pretensión, el demandante solicita la anulación de las transferencias de sus datos personales a terceros países que no dispongan de un nivel de protección adecuado que presuntamente tuvieron lugar el 30 de marzo y el 8 de junio de 2022 (en lo sucesivo, «transferencias controvertidas»).

20 En su escrito de contestación, la Comisión alega la inadmisibilidad de esta pretensión de anulación, debido a que no se dirige contra un acto impugnable, en el sentido del artículo 263 TFUE, sino que pretende que se le dirija un requerimiento.

21 El demandante sostiene la admisibilidad de la pretensión de anulación alegando que las transferencias controvertidas son actos que producen efectos jurídicos obligatorios y que afectan a su situación jurídica, menoscabando su derecho fundamental a la protección de los datos de carácter personal, garantizado por el artículo 8 de la Carta. Estima que cualquier otra interpretación es incompatible con el derecho fundamental a la tutela judicial efectiva, derecho que reconoce expresamente el artículo 64, apartado 1, del Reglamento 2018/1725.

22 Como recuerdan el artículo 64, apartado 1, y el considerando 79 del Reglamento 2018/1725, toda persona tiene derecho a la tutela judicial efectiva ante el Tribunal de Justicia de la Unión Europea, de conformidad con los Tratados, si considera que se vulneran los derechos que le confiere el citado Reglamento.

23 De ello se deduce que, en el marco del Reglamento 2018/1725, todo interesado tiene derecho, en particular, a interponer un recurso de anulación en las condiciones establecidas en el artículo 263 TFUE.

24 Según reiterada jurisprudencia, es posible formular el recurso de anulación establecido en el artículo 263 TFUE con respecto a cualquier acto de las instituciones, cualquiera que sea su forma, que tienda a producir efectos jurídicos obligatorios que puedan afectar a los intereses de la parte demandante, modificando sustancialmente su situación jurídica (véanse las sentencias de 19 de enero de 2017, Comisión/Total y Elf Aquitaine, C-351/15 P, EU:C:2017:27, apartados 35 y 36 y jurisprudencia citada, y de 16 de julio de 2020, Inclusion Alliance for Europe/Comisión, C-378/16 P, EU:C:2020:575, apartado 71 y jurisprudencia citada).

25 Para determinar si un acto produce efectos jurídicos obligatorios, hay que atenerse, según reiterada jurisprudencia del Tribunal de Justicia, al contenido esencial de dicho acto y apreciar sus efectos en función de criterios objetivos, como el contenido de tal acto, tomando en

consideración, en su caso, el contexto en el que se adoptó y las facultades de la institución, el órgano o el organismo de la Unión que lo haya adoptado (véase la sentencia de 15 de julio de 2021, FBF, C-911/19, EU:C:2021:599, apartado 38 y jurisprudencia citada).

26 En el caso de autos, el demandante solicita la anulación de las transferencias controvertidas, que, según él, tuvieron lugar en tres ocasiones. En primer lugar, sostiene que, con ocasión de su consulta del sitio de Internet de la CFE de 30 de marzo de 2022 (en lo sucesivo, «transferencia controvertida con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022»), se transfirieron ciertos datos personales suyos, en particular su dirección IP e información sobre su navegador y su terminal, a la empresa estadounidense Amazon Web Services, en su condición de operador de la red de distribución de contenidos denominada «Amazon CloudFront», que supuestamente utiliza dicho sitio de Internet.

27 En segundo lugar, el demandante estima que, cuando se conectó, el 30 de marzo de 2022, al servicio de autenticación de usuario de la Comisión EU Login, sirviéndose de su cuenta de Facebook, con la finalidad de registrarse en el evento «GoGreen» en el sitio de Internet de la CFE (en lo sucesivo, «transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022»), se transfirieron ciertos datos personales suyos, en particular su dirección IP e información sobre su navegador y su terminal, a la empresa estadounidense Meta Platforms, Inc.

28 En tercer lugar, el demandante alega que, cuando consultó el sitio de Internet de la CFE el 8 de junio de 2022 (en lo sucesivo, «transferencia controvertida con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022»), se transfirieron ciertos datos personales suyos a un servidor de Amazon CloudFront situado en Newark (Nueva Jersey, Estados Unidos).

29 Por otro lado, el demandante menciona en su demanda que accedió al sitio de Internet de la CFE el 9 de noviembre de 2021 y que se registró ese día en el sitio de Internet de la CFE sirviéndose de su cuenta de Facebook. Sin embargo, no invoca ningún dato concreto que permita concluir que su pretensión de anulación de las transferencias controvertidas contemple tales circunstancias. Por tanto, procede tener únicamente en cuenta las transferencias controvertidas mencionadas en los apartados 26 a 28 de la presente sentencia.

30 Hay que indicar que las transferencias controvertidas cuya anulación solicita el demandante, mencionadas en los apartados 26 a 28 de la presente sentencia, se corresponden, según el propio demandante, con operaciones informáticas de migración de datos iniciadas por los sistemas o servicios informáticos de la Comisión, en particular el sitio de Internet de la CFE, hacia servidores pertenecientes a empresas terceras domiciliadas fuera del territorio de la Unión.

31 Es cierto que la operación consistente en transferir datos personales desde una institución u órgano de la Unión a un tercer país constituye por sí misma un tratamiento de datos personales, en el sentido del artículo 3, punto 3, del Reglamento 2018/1725, realizado en el territorio de la Unión, tratamiento al que dicho Reglamento se aplica en virtud de su artículo 2, apartado 5 (véase, por analogía, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, en lo sucesivo, «sentencia Schrems II», EU:C:2020:559, apartado 83).

32 No obstante, no todas las operaciones que pueden dar lugar a una transferencia de datos personales, con arreglo al artículo 3, punto 3, del Reglamento 2018/1725, son actos impugnables, en el sentido del artículo 263 TFUE, tal como lo ha interpretado la jurisprudencia recordada en el anterior apartado 24.

33 En el caso de autos, aun suponiendo que se hayan demostrado las transferencias controvertidas, es preciso declarar que son actos materiales y no actos jurídicos. En efecto, las transferencias controvertidas, en los términos en que se describen en la demanda, son operaciones informáticas de migración de datos entre terminales o servidores, resultantes de las interacciones entre el demandante y los sistemas o servicios informáticos de la Comisión, cuando aquel consulta el sitio de Internet de la CFE o el servicio EU Login. En cambio, las transferencias controvertidas no son actos de la Comisión que produzcan efectos jurídicos vinculantes, es decir, no regulan una situación jurídica y, como resulta de su propia naturaleza, la Comisión en modo alguno tuvo la intención de conferirles tales efectos.

34 Por tanto, las transferencias controvertidas no son capaces de producir efectos jurídicos obligatorios que puedan afectar a los intereses del demandante, modificando sustancialmente su situación jurídica, de conformidad con la jurisprudencia recordada en el anterior apartado 24. Por consiguiente, no pueden considerarse actos impugnables en el sentido del artículo 263 TFUE.

35 De ello se deduce que hay que declarar inadmisibles las pretensiones de anulación del demandante.

Admisibilidad de las pretensiones por omisión

36 Mediante su segunda pretensión, el demandante solicita al Tribunal General que declare que la Comisión, contrariamente a Derecho, no se pronunció sobre la solicitud de información de 1 de abril de 2022.

37 En su escrito de contestación, la Comisión aduce la inadmisibilidad de esta pretensión por omisión, al no haber sido requerida para actuar con arreglo al artículo 265 TFUE, párrafo segundo. Con carácter subsidiario, la Comisión alega que no procede pronunciarse sobre la pretensión por omisión, habida cuenta de la respuesta que dio al demandante mediante correo electrónico de 30 de junio de 2022.

38 El demandante sostiene, en esencia, que la Comisión sigue estando obligada a responder a la solicitud de información de 1 de abril de 2022, puesto que la información que facilitó mediante su correo electrónico de 30 de junio de 2022 es insuficiente e inexacta.

39 Según reiterada jurisprudencia, el recurso previsto por el artículo 265 TFUE está basado en la idea de que la inacción ilegal de la una institución permite recurrir ante el juez de la Unión a fin de que este declare que la abstención de actuar es contraria al Tratado, cuando la institución de que se trate no haya subsanado dicha abstención (sentencia de 12 de julio de 1988, Parlamento/Consejo, 377/87, EU:C:1988:387, apartado 9; véase también la sentencia de 16 de diciembre de 2015, Suecia/Comisión, T-521/14, no publicada, EU:T:2015:976, apartado 33 y jurisprudencia citada).

40 En el caso de que el acto cuya omisión constituye el objeto del litigio haya sido adoptado después de la interposición del recurso, pero antes de pronunciarse la sentencia, la declaración por un tribunal de la Unión de la ilegalidad de la abstención inicial ya no puede producir las consecuencias previstas por el artículo 266 TFUE. De ello se deriva que, en tal caso, el objeto del recurso ha desaparecido, por lo que ya no procede resolver (sentencia de 12 de julio de 1988, Parlamento/Consejo, 377/87, EU:C:1988:387, apartados 10 y 11; véase también el auto de 13 de diciembre de 2000, Sodima/Comisión, C-44/00 P, EU:C:2000:686, apartado 83 y jurisprudencia citada).

41 En el caso de autos, hay que declarar que la Comisión respondió a la solicitud de información de 1 de abril de 2022 mediante su correo electrónico de 30 de junio de 2022 (véase el anterior apartado 11). Por consiguiente, la Comisión puso fin a la omisión alegada por el demandante en el presente recurso después de la interposición de dicho recurso. Por tanto, la segunda pretensión, que tiene por objeto que se declare, sobre la base del artículo 265 TFUE, la omisión de la Comisión por no haber respondido a la solicitud de información de 1 de abril de 2022, ha quedado sin objeto.

42 El hecho de que el contenido del correo electrónico de la Comisión de 30 de junio de 2022 no coincida con la respuesta deseada por el demandante es irrelevante a este respecto. En efecto, es indiferente la circunstancia de que la postura adoptada por la institución no satisfaga a la parte demandante, ya que el artículo 265 TFUE se refiere a la omisión por haberse abstenido de adoptar una decisión o una posición y no a la adopción de un acto diferente del que dicha parte habría deseado o considerado necesario (véase el auto de 6 de abril de 2017, Brancheforeningen for Regulerkraft i Danmark/Comisión, T-203/16, no publicado, EU:T:2017:279, apartado 22 y jurisprudencia citada).

43 De ello se deduce que no procede resolver en cuanto a las pretensiones por omisión del demandante y que no es necesario pronunciarse sobre la inadmisibilidad de tales pretensiones formulada por la Comisión.

Sobre las pretensiones de indemnización

44 Mediante su tercera pretensión, el demandante formula dos peticiones de indemnización. En primer lugar, solicita el abono de 800 euros como indemnización de los daños y perjuicios inmateriales que alega haber sufrido debido a que la Comisión no respetó su derecho de acceso a la información, con infracción de los artículos 14, apartados 3 y 4, y 17, apartados 1 y 2, del Reglamento 2018/1725, así como con violación del principio de transparencia establecido en el artículo 4, apartado 1, letra a), de dicho Reglamento. En segundo lugar, solicita el abono de 400 euros como indemnización de los daños y perjuicios inmateriales que supuestamente sufrió por las transferencias controvertidas, realizadas infringiendo los artículos 46 y 48, apartados 1 y 2, letra b), del Reglamento 2018/1725.

45 La Comisión solicita la desestimación de las pretensiones de indemnización.

Consideraciones preliminares sobre los requisitos para generar la responsabilidad extracontractual de la Unión en el marco del Reglamento 2018/1725

46 El artículo 65 del Reglamento 2018/1725 establece que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del citado Reglamento tiene derecho a recibir de la institución u organismo de la Unión responsable una indemnización por los daños y perjuicios sufridos, «con arreglo a las condiciones previstas en los Tratados».

47 Procede interpretar este artículo 65 del Reglamento 2018/1725 en el sentido de que establece que el derecho a recibir de la institución o del organismo de la Unión una indemnización por los daños y perjuicios sufridos como consecuencia de una infracción de dicho Reglamento está supeditado a los requisitos del artículo 340 TFUE, párrafo segundo, en virtud del cual la Unión debe reparar los daños causados por sus instituciones o sus agentes en el ejercicio de sus funciones, de conformidad con los principios generales comunes a los Derechos de los Estados miembros.

48 Según reiterada jurisprudencia, la generación de la responsabilidad extracontractual de la Unión exige que concurran tres requisitos acumulativos, a saber, la ilicitud de la actuación imputada a las instituciones, la realidad del daño y la existencia de una relación de causalidad entre esa actuación y el perjuicio invocado (véanse, en este sentido, las sentencias de 4 de julio de 2000, Bergaderm y Goupil/Comisión, C-352/98 P, EU:C:2000:361, apartados 39 a 42, y de 28 de octubre de 2021, Vialto Consulting/Comisión, C-650/19 P, EU:C:2021:879, apartado 138).

49 El carácter acumulativo de tales requisitos implica que, en el supuesto de que no se cumpla uno de ellos, deberá desestimarse el recurso de indemnización en su totalidad, sin que sea necesario examinar los demás requisitos (sentencia de 9 de septiembre de 1999, Lucaccioni/Comisión, C-257/98 P, EU:C:1999:402, apartados 14 y 63; véase también la sentencia de 25 de febrero de 2021, Dalli/Comisión, C-615/19 P, EU:C:2021:133, apartado 42 y jurisprudencia citada).

50 Por lo que se refiere al primer requisito, la jurisprudencia exige que se demuestre una violación suficientemente caracterizada de una norma jurídica cuyo objeto sea conferir derechos a los particulares (véase la sentencia de 4 de julio de 2000, Bergaderm y Goupil/Comisión, C-352/98 P, EU:C:2000:361, apartado 42 y jurisprudencia citada).

51 Este requisito relativo a la existencia de una infracción suficientemente caracterizada del Derecho de la Unión pretende, cualquiera que sea la naturaleza del acto ilícito de que se trate, evitar que el riesgo de tener que cargar con las indemnizaciones de los daños alegados por las personas interesadas menoscabe la capacidad de la institución de que se trate de ejercer plenamente sus competencias en aras del interés general, tanto en el marco de su actividad normativa o que implique decisiones de política económica como en la esfera de su competencia administrativa, sin que recaigan sobre terceros, no obstante, las consecuencias de incumplimientos flagrantes e inexcusables (véase, en este sentido, la sentencia de 14 de diciembre de 2018, East West Consulting/Comisión, T-298/16, EU:T:2018:967, apartado 124 y jurisprudencia citada).

52 El criterio decisivo que permite considerar que una violación es suficientemente caracterizada consiste en la inobservancia manifiesta y grave, por parte de la institución u órgano de la Unión de que se trate, de los límites impuestos a su facultad de apreciación. Cuando dicha institución u órgano solo dispone de un margen de apreciación considerablemente reducido, o incluso inexistente, la mera infracción del Derecho de la Unión puede bastar para demostrar la existencia de una violación suficientemente caracterizada (véase la sentencia de 10 de diciembre de 2002, Comisión/Camar y Tico, C-312/00 P, EU:C:2002:736, apartado 54 y jurisprudencia citada). No obstante, dicha jurisprudencia no establece ninguna relación automática entre, por una parte, la inexistencia de facultad de apreciación de la institución de que se trate y, por otra parte, la calificación de la infracción como violación suficientemente caracterizada del Derecho de la Unión (sentencia de 3 de marzo de 2010, Artegodan/Comisión, T-429/05, EU:T:2010:60, apartado 59). En efecto, aun cuando tiene carácter determinante, la extensión de la facultad de apreciación de la institución de que se trate no constituye un criterio exclusivo. A este respecto, el Tribunal de Justicia ha recordado de manera continuada que el régimen que ha establecido con arreglo al artículo 340 TFUE, párrafo segundo, tiene en cuenta, además, especialmente la complejidad de las situaciones que deben ser reguladas y las dificultades de aplicación o de interpretación de los textos (véase la sentencia de 23 de noviembre de 2011, Sison/Consejo, T-341/07, EU:T:2011:687, apartados 36 y 37 y jurisprudencia citada) o, más genéricamente, el ámbito, las circunstancias y el contexto en que la norma infringida se impone a la institución o al órgano de la Unión sujeto a tal norma (véase la sentencia de 4 de abril de 2017, Defensor del Pueblo/Staelen, C-337/15 P, EU:C:2017:256 apartado 40 y jurisprudencia citada).

53 De ello se deduce que únicamente la comprobación de una irregularidad que, en circunstancias análogas, no habría cometido una Administración normalmente prudente y diligente permite que se genere la responsabilidad de la Unión. Por tanto, corresponde al juez de la Unión, tras haber determinado si la institución de que se trate disponía de un margen de apreciación, tomar en consideración la complejidad de la situación que debe ser regulada, las dificultades de aplicación o de interpretación de los textos legales, el grado de claridad y de precisión de la norma vulnerada y el carácter intencional o inexcusable del error cometido (sentencia de 3 de marzo de 2010, Artegodan/Comisión, T-429/05, EU:T:2010:60, apartado 62).

54 En cuanto al requisito relativo a la realidad del daño, este debe ser real y cierto, cuestión que incumbe demostrar a la parte demandante (véase la sentencia de 9 de noviembre de 2006, Agraz y otros/Comisión, C-243/05 P, EU:C:2006:708, apartado 27 y jurisprudencia citada). En cambio, un daño puramente hipotético e indeterminado no origina derecho a reparación (véase la sentencia de 26 de octubre de 2011, Dufour/BCE, T-436/09, EU:T:2011:634, apartado 192 y jurisprudencia citada).

55 Por lo que respecta al requisito relativo a la relación de causalidad, esta entraña la existencia de una relación suficientemente directa de causa a efecto entre el comportamiento reprochado a la institución y el daño, relación que corresponde probar a la parte demandante, de modo que el comportamiento reprochado debe ser la causa determinante del perjuicio (véase la sentencia de 13 de diciembre de 2018, Unión Europea/ASPLA y Armando Álvarez, C-174/17 P y C-222/17 P, EU:C:2018:1015, apartado 23 y jurisprudencia citada).

56 Por otro lado, es preciso recordar que la acción de indemnización, basada en el artículo 340 TFUE, párrafo segundo, fue establecida como una vía autónoma, que tiene su función particular en el marco del sistema de recursos y está supeditada a condiciones de ejercicio concebidas pensando en su objeto específico, de modo que la declaración de inadmisibilidad del recurso de anulación no ocasiona automáticamente la inadmisibilidad del recurso de indemnización (véase la sentencia de 5 de septiembre de 2019, Unión Europea/Guardian Europe y Guardian Europe/Unión Europea, C-447/17 P y C-479/17 P, EU:C:2019:672, apartado 49 y jurisprudencia citada).

57 De ello se deduce que la inadmisión de la pretensión de anulación y el sobreseimiento de la pretensión por omisión, de conformidad con los apartados 35 y 43 de la presente sentencia, no implican consecuentemente la inadmisión de las peticiones de indemnización mencionadas en el anterior apartado 44.

58 Procede examinar las alegaciones formuladas por el demandante en sus peticiones de indemnización a la luz de estas consideraciones.

Sobre la primera petición de indemnización, que tiene como objetivo que se indemnicen los daños y perjuicios inmateriales resultantes de la vulneración del derecho de acceso a la información

59 Mediante su primera petición de indemnización, el demandante solicita que se condene a la Comisión a abonarle la cuantía de 800 euros como indemnización de los daños y perjuicios inmateriales sufridos a raíz de la vulneración de su derecho de acceso a la información.

60 El demandante empieza reprochando a la Comisión no haber respondido a la solicitud de información de 1 de abril de 2022 en el plazo fijado y no haberle comunicado las razones de su no actuación, infringiendo los artículos 14, apartados 3 y 4, y 17, apartados 1 y 2, del Reglamento

2018/1725 y violando el principio de transparencia, establecido en el artículo 4, apartado 1, letra a), del mismo Reglamento. Además, reprocha a la Comisión no haber respetado el artículo 17, apartados 1, letra c), y 2, del Reglamento 2018/1725, pues estima que la declaración relativa a la protección de la vida privada, que figura en el sitio de Internet de la CFE, no contiene información relativa a la transferencia de datos personales a terceros países ni a eventuales garantías adecuadas a efectos de dicha transferencia, como exige el artículo 48 del referido Reglamento. Añade que, en el correo electrónico de 3 de diciembre de 2021, la Comisión facilitó información errónea, ya que negó la transferencia de datos personales del demandante a destinatarios situados en los Estados Unidos.

61 El demandante sostiene a continuación que la inacción culposa de la Comisión le impidió controlar el tratamiento de sus datos personales, lo que da lugar a daños y perjuicios inmateriales en el sentido del considerando 46 del Reglamento 2018/1725. Por último, alega que esos daños y perjuicios inmateriales, que evalúa en 800 euros, están causados directamente por el comportamiento ilícito de la Comisión.

62 La Comisión rebate tal argumentación alegando, en esencia, que en el caso de autos no concurre ninguno de los requisitos para generar la responsabilidad extracontractual.

63 En primer lugar, por lo que respecta al requisito relativo a la ilicitud de la actuación imputada, hay que comprobar si el demandante adujo la violación de normas jurídicas cuyo objeto sea conferir derechos a los particulares.

64 A este respecto, procede observar que el artículo 17, apartado 1, letra c), del Reglamento 2018/1725 establece un derecho de acceso del interesado a información relativa a los destinatarios a los que se comunicaron sus datos personales, en particular a los destinatarios en terceros países. Así pues, esta disposición concreta el principio, consagrado en el artículo 4, apartado 1, letra a), del Reglamento 2018/1725, según el cual toda información y comunicación relativa al tratamiento de datos personales debe ser fácilmente accesible.

65 Además, el artículo 14, apartado 3, del Reglamento 2018/1725 fija el plazo de un mes para que el responsable del tratamiento de datos personales responda a las solicitudes de información. El artículo 14, apartado 4, de dicho Reglamento obliga asimismo al responsable del tratamiento de datos personales, en caso de que decida no atender a la solicitud, a informar al solicitante, en el plazo de un mes, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante el Supervisor Europeo de Protección de Datos (SEPD) y de interponer un recurso judicial. Así pues, estas disposiciones son normas de procedimiento administrativo que contribuyen a la aplicación del derecho de acceso a la información relativa a los datos personales del interesado y que precisan y modulan ese derecho. Además, estas disposiciones contribuyen a concretar el derecho conferido a toda persona, en virtud del artículo 41 de la Carta, a que las instituciones y órganos de la Unión traten su asunto dentro de un plazo razonable.

66 Por consiguiente, las disposiciones de los artículos 4, apartado 1, letra a), 14, apartados 3 y 4, y 17, apartado 1, letra c), del Reglamento 2018/1725, interpretadas conjuntamente, son normas jurídicas que tienen por objeto conferir derechos a los particulares, en el sentido de la jurisprudencia mencionada en el anterior apartado 50.

67 En segundo lugar, procede examinar si en el caso de autos ha quedado acreditada la vulneración de estas disposiciones por la Comisión.

68 Por una parte, el demandante sostiene que la Comisión infringió el artículo 17, apartados 1, letra c), y 2, del Reglamento 2018/1725, pues estima que la declaración relativa a la protección de la vida privada que figura en el sitio de Internet de la CFE no incluye información sobre la transferencia de datos personales a destinatarios establecidos en terceros países, sobre eventuales garantías adecuadas relativas a dicha transferencia o sobre la identificación de los contratantes como destinatarios de tales datos.

69 Como se ha mencionado en el anterior apartado 64, el artículo 17, apartados 1, letra c), y 2, del Reglamento 2018/1725 establece que el interesado tiene derecho, en particular, a obtener información sobre los destinatarios establecidos en terceros países a los que se comunicaron los datos personales y sobre las garantías adecuadas referidas a las transferencias de datos a esos destinatarios.

70 De ello se deduce que estas disposiciones establecen un derecho de acceso del interesado a determinada información, pero no obligan a que dicha información figure en un documento determinado, ni siquiera en una declaración relativa a la protección de la vida privada, como la que figura en el sitio de Internet de la CFE. En otras palabras, de estas disposiciones no resulta que la información de que se trata deba ser divulgada mediante la citada declaración. Dicho esto, el demandante, como cualquier interesado, conserva el derecho a obtener tal información ejercitando su derecho de acceso a la información, previsto en el artículo 17, apartados 1, letra c), y 2, del Reglamento 2018/1725, cuestión que va más allá del alcance de la ilegalidad que el demandante imputa a la Comisión, que se limita al contenido de la declaración relativa a la protección de la vida privada (véase el anterior apartado 68).

71 En cualquier caso, en el presente asunto, del tenor de dicha declaración relativa a la protección de la vida privada, que acompaña a la demanda, se desprende que esa declaración incluye información relativa a los destinatarios o a las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales. Así, en el apartado 7 de dicha declaración se menciona, en particular, que el acceso a los datos se «concede […] al personal autorizado de la Comisión […] y a sus contratistas encargados de realizar esta operación de tratamiento, con arreglo al principio de la “necesidad de conocer”». Además, la alegación del demandante basada en que dicha declaración no incluye información sobre la transferencia de datos personales a destinatarios establecidos en terceros países se fundamenta en la hipótesis de que la consulta del sitio de Internet de la CFE implica la transferencia de datos personales de los usuarios a un tercer país. Sin embargo, la presente petición de indemnización tiene como fundamento la vulneración del derecho de acceso a la información y no la vulneración de las disposiciones relativas a la transferencia de datos personales a terceros países, en la que, por otro lado, se sustenta la segunda petición de indemnización.

72 Por tanto, no se ha demostrado en el presente asunto que la Comisión haya infringido el artículo 17, apartados 1, letra c), y 2, del Reglamento 2018/1725 en lo que respecta a la declaración relativa a la protección de la vida privada que figura en el sitio de Internet de la CFE.

73 Por otra parte, el demandante reprocha a la Comisión no haber respondido a la solicitud de información de 1 de abril de 2022 en el plazo fijado y no haberlo informado de las razones de su no actuación, infringiendo los artículos 14, apartados 3 y 4, y 17, apartados 1 y 2, del Reglamento 2018/1725 y violando el principio de transparencia. Imputa asimismo a la Comisión haberle comunicado información errónea en el correo electrónico de 3 de diciembre de 2021.

74 Procede comenzar señalando que el demandante no formula ninguna alegación concreta en apoyo de la violación del principio de transparencia. Por consiguiente, esta alegación no tiene un contenido autónomo en relación con la imputación basada en el incumplimiento del plazo de respuesta a la solicitud de información y de la obligación de comunicar las razones por las que se superó dicho plazo.

75 Además, las alegaciones del demandante basadas en la vulneración del artículo 17, apartados 1 y 2, del Reglamento 2018/1725, así como en que la Comisión le comunicó información errónea en el correo electrónico de 3 de diciembre de 2021, se sustentan en la hipótesis de que la consulta del sitio de Internet de la CFE implica la transferencia de datos personales de los usuarios a un tercer país. Pues bien, como se ha mencionado en el anterior apartado 71, la presente petición de indemnización se fundamenta en la vulneración del derecho de acceso a la información y no en la vulneración de las disposiciones relativas a la transferencia de datos personales a terceros países, de la que parte la segunda petición de indemnización.

76 Por tanto, en el presente asunto no se ha demostrado que la Comisión haya infringido el artículo 17, apartados 1 y 2, del Reglamento 2018/1725.

77 Por lo que respecta a la imputación del demandante basada en la infracción del artículo 14, apartados 3 y 4, del Reglamento 2018/1725, de los autos se desprende que la Comisión respondió a la solicitud de información de 9 de noviembre de 2021 en el plazo de un mes establecido en el artículo 14, apartado 3, del Reglamento 2018/1725 (véanse los apartados 5 y 7 de la presente sentencia). En lo relativo a la solicitud de información de 1 de abril de 2022, la Comisión informó al demandante, mediante correo electrónico de 30 de junio de 2022, de que consideraba que la solicitud de información de 1 de abril de 2022 era casi idéntica a la solicitud de información de 9 de noviembre de 2021, a la que ya había respondido mediante su correo electrónico de 3 de diciembre de 2021 (véase el anterior apartado 11).

78 De ello se deduce que, por lo que respecta a la solicitud de información de 1 de abril de 2022, la Comisión incumplió el plazo de un mes, establecido en el artículo 14, apartado 4, del Reglamento 2018/1725 (véase el anterior apartado 65).

79 De los apartados 68 a 78 de la presente sentencia se desprende que la única ilegalidad imputada a la Comisión que queda acreditada en el caso de autos es la del incumplimiento del plazo previsto en el artículo 14, apartado 4, del Reglamento 2018/1725.

80 En estas circunstancias, y con independencia de si el incumplimiento de dicho plazo por parte de la Comisión constituye una violación suficientemente caracterizada de una norma jurídica, hay que comenzar examinando si el incumplimiento del citado plazo ocasionó al demandante un daño moral real y cierto, en el sentido de la jurisprudencia recordada en el anterior apartado 54.

81 En lo que atañe a la realidad de los daños y perjuicios inmateriales supuestamente sufridos, cabe recordar que, aunque la presentación de pruebas no se considera necesariamente como un requisito para el reconocimiento de tales daños y perjuicios, incumbe a la parte demandante demostrar, al menos, que el comportamiento reprochado a la institución de que se trata podía causarle tal perjuicio (sentencia de 16 de julio de 2009, SELEX Sistemi Integrati/Comisión, C-481/07 P, no publicada, EU:C:2009:461, apartado 38; véase también la sentencia de 2 de julio de 2019, Fulmen/Consejo, T-405/15, EU:T:2019:469, apartado 188 y jurisprudencia citada).

82 En el caso de autos, el demandante solicita la indemnización de unos daños y perjuicios inmateriales por importe de 800 euros alegando que el comportamiento reprochado a la Comisión le impidió controlar el tratamiento de sus datos personales.

83 No obstante, hay que señalar que tales daños y perjuicios inmateriales no han sido demostrados en el caso de autos. En efecto, la única ilegalidad acreditada en el presente asunto es la del incumplimiento, por parte de la Comisión, del plazo de un mes previsto en el artículo 14, apartado 4, del Reglamento 2018/1725 (véase el anterior apartado 79). Pues bien, este plazo no fue superado en más de dos meses (véase el anterior apartado 77). Además, las solicitudes de información de 9 de noviembre de 2021 y de 1 de abril de 2022 eran fundamentalmente las mismas (véanse los apartados 5 y 8 de la presente sentencia), de modo que el demandante ya había recibido una respuesta a parte, al menos, de su solicitud de información el 3 de diciembre de 2021, día en que la Comisión respondió a la solicitud de información de 9 de noviembre de 2021 (véase el anterior apartado 7).

84 Por otro lado, la alegación del demandante basada en la comunicación de información errónea (véase el anterior apartado 75) se refiere a la procedencia de la información y no a la observancia de la norma procedimental cuya infracción ha quedado demostrada en el anterior apartado 78, por lo que no es pertinente para demostrar los daños y perjuicios inmateriales alegados.

85 De ello se deduce que no se ha demostrado que el incumplimiento, por parte de la Comisión, del plazo previsto en el artículo 14, apartado 4, del Reglamento 2018/1725 pudiera causar al demandante los daños y perjuicios inmateriales alegados.

86 Por consiguiente, dado que no concurre uno de los requisitos acumulativos para que se genere la responsabilidad extracontractual de la Unión, establecidos en el artículo 340 TFUE, párrafo segundo, se debe desestimar la primera petición de indemnización del demandante.

Sobre la segunda petición de indemnización, que tiene por objeto la indemnización de los daños y perjuicios inmateriales derivados de las transferencias controvertidas

87 Mediante su segunda petición de indemnización, el demandante solicita el abono de 400 euros como indemnización de los daños y perjuicios inmateriales que alega haber sufrido por las transferencias controvertidas mencionadas en los apartados 26 a 28 de la presente sentencia, concretamente la transferencia controvertida con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, la transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022 y la transferencia controvertida con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022.

88 El demandante sostiene, en esencia, que las transferencias controvertidas se efectuaron a destinatarios domiciliados en los Estados Unidos, país que no tiene un nivel de protección adecuado. Aduce que la Comisión no puso de manifiesto ninguna de las garantías adecuadas que pueden justificar tales transferencias, establecidas en el capítulo V del Reglamento 2018/1725, por lo que infringió los artículos 46 y 48, apartados 1 y 2, letra b), de dicho Reglamento, así como los artículos 7, 8 y 47 de la Carta. El demandante estima que las transferencias controvertidas implicaron que se corriera el riesgo de que los servicios de seguridad e inteligencia de ese país hubiesen podido acceder a sus datos, por lo que tales transferencias le causaron daños y perjuicios inmateriales, en el sentido del considerando 46 del Reglamento 2018/1725, al haberse visto privado de sus derechos y libertades e impedido para ejercer el control sobre sus datos.

89 La Comisión rebate esta argumentación alegando, en esencia, que en el caso de autos no concurren los requisitos para que se genere la responsabilidad extracontractual.

– Consideraciones preliminares sobre las disposiciones relativas a la transferencia de datos personales a un tercer país

90 En primer lugar, procede observar que, a tenor de su artículo 2, apartado 5, el Reglamento 2018/1725 se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

91 En segundo lugar, el concepto de «datos personales» debe interpretarse como referido a toda información sobre una persona física identificada o identificable, de conformidad con el artículo 3, punto 1, del Reglamento 2018/1725.

92 En tercer lugar, es preciso observar que la transferencia de datos constituye una operación de «tratamiento» de datos en el sentido del artículo 3, punto 3, del Reglamento 2018/1725.

93 En cuarto lugar, hay que indicar que las «transferencias de datos personales a terceros países u organizaciones internacionales» se rigen por el capítulo V del Reglamento 2018/1725, que, no obstante, no las define.

94 Sin embargo, del considerando 63 del Reglamento 2018/1725 se desprende que las transferencias contempladas en las disposiciones del capítulo V de dicho Reglamento se refieren a los datos personales transferidos desde las instituciones y organismos de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales.

95 Además, de una interpretación sistemática del Reglamento 2018/1725 resulta que la transferencia de datos personales a terceros países, con arreglo a su artículo 46, exige, en primer lugar, que el responsable del tratamiento de los datos de que se trate pertenezca a una institución u organismo de la Unión y esté sometido, por tanto, al citado Reglamento (artículo 1 del Reglamento 2018/1725); en segundo lugar, que el responsable del tratamiento ponga, por transmisión o de otro modo, datos personales a disposición de un destinatario, en particular de otra persona física o jurídica (artículo 3, puntos 3 y 13, del Reglamento 2018/1725), y, en tercer lugar, que ese destinatario esté domiciliado en un tercer país (artículo 46 del Reglamento 2018/1725), es decir, un país que no sea miembro ni de la Unión ni del Espacio Económico Europeo (EEE).

96 En quinto lugar, es preciso declarar que las disposiciones del capítulo V del Reglamento 2018/1725 pretenden respetar, con ocasión de las transferencias de datos personales a terceros países o a organizaciones internacionales, el nivel de protección de las personas físicas garantizado en la Unión, de conformidad con el objetivo precisado en su considerando 63.

97 En sexto lugar, el artículo 46 del Reglamento 2018/1725 establece un principio general según el cual solo se realizarán transferencias de datos personales a un tercer país u organización internacional si, a reserva de las demás disposiciones de dicho Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en su capítulo V.

98 En séptimo lugar, por lo que respecta a las condiciones que se definen en el capítulo V del Reglamento 2018/1725, procede observar que el artículo 47, apartado 1, de este Reglamento establece que puede realizarse una transferencia de datos personales a un tercer país o una

organización internacional cuando la Comisión haya decidido, mediante una decisión de adecuación adoptada, en particular, en virtud del artículo 45, apartado 3, del Reglamento 2016/679, que el país o la organización internacional de que se trate garantiza un nivel de protección adecuado y cuando los datos se transfieran exclusivamente para permitir el ejercicio de funciones que sean competencia del responsable del tratamiento.

99 Es preciso recordar al respecto que las dos decisiones de adecuación de la Comisión relativas a los Estados Unidos fueron invalidadas. Por una parte, mediante la sentencia de 6 de octubre de 2015, Schrems (C-362/14, EU:C:2015:650), el Tribunal de Justicia invalidó la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO 2000, L 215, p. 7). Por otra parte, mediante la sentencia Schrems II, el Tribunal de Justicia invalidó la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU (DO 2016, L 207, p. 1).

100 De ello se deduce que, el día en que se produjeron las transferencias controvertidas, no existía ninguna decisión de adecuación, en el sentido del artículo 47 del Reglamento 2018/1725, con respecto a los Estados Unidos.

101 A falta de una decisión de adecuación de la Comisión con respecto a los Estados Unidos, se aplica el artículo 48, apartado 1, del Reglamento 2018/1725, según el cual solo pueden transferirse datos personales a un tercer país o a una organización internacional si el responsable del tratamiento o el encargado del tratamiento hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

102 Las garantías adecuadas con arreglo al apartado 1 del artículo 48 del Reglamento 2018/1725, que se enumeran en sus apartados 2 y 3, pueden ser aportadas, en particular, por cláusulas tipo de protección de datos, adoptadas por la Comisión, de conformidad con el artículo 48, apartado 2, letra b), de dicho Reglamento.

103 No obstante, las cláusulas tipo de protección de datos previstas en el artículo 48, apartado 2, letra b), del Reglamento 2018/1725 pueden necesitar la adopción de medidas adicionales, con el fin de garantizar el respeto del nivel de protección adecuado, conforme al Derecho de la Unión (véase, por analogía, la sentencia Schrems II, apartados 133 y 134).

104 Además, las garantías adecuadas con arreglo al artículo 48, apartado 1, del Reglamento 2018/1725 pueden ser aportadas, en particular, mediante cláusulas contractuales, previstas en el artículo 48, apartado 3, letra a), de dicho Reglamento, celebradas entre, por una parte, el responsable o el encargado y, por otra parte, el responsable, el encargado o el destinatario de los datos personales en el tercer país, previa autorización del SEPD.

105 Por otro lado, es preciso recordar que los artículos 7, 8 y 47 de la Carta establecen, respectivamente, el derecho al respeto de la vida privada, el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva y a un juez imparcial.

106 En el caso de autos, procede comenzar señalando que la segunda petición de indemnización del demandante se basa en la vulneración, por parte de la Comisión, de las disposiciones de los artículos 46 y 48, apartados 1 y 2, letra b), del Reglamento 2018/1725 y de los artículos 7, 8 y 47 de la Carta. Pues bien, de los apartados 91 a 105 de la presente sentencia resulta que dichas disposiciones del Reglamento 2018/1725 concretan derechos fundamentales como los establecidos en los artículos 7 y 8 de la Carta y persiguen garantizar conjuntamente la continuidad del elevado nivel de protección de los datos personales en caso de transferencia de esos datos a terceros países u organizaciones internacionales.

107 De ello se deduce que las disposiciones cuya infracción alega el demandante en apoyo de su segunda petición de indemnización tienen por objeto proteger el interés individual de los interesados, por lo que son normas jurídicas cuyo objeto es conferir derechos a los particulares, en el sentido de la jurisprudencia recordada en el apartado 50 anterior.

108 Procede comprobar ahora si concurren los requisitos para que se genere la responsabilidad extracontractual de la Comisión por las tres transferencias controvertidas mencionadas en el apartado 87 anterior.

109 Dado que las transferencias controvertidas mencionadas en los apartados 26 y 28 de la presente sentencia se llevaron a cabo por utilizar el sitio de Internet de la CFE la red de distribución de contenidos o «RDC» (en inglés, «content delivery network» o «CDN») denominada «Amazon CloudFront» (en lo sucesivo, «servicio Amazon CloudFront»), hay que comenzar determinando las condiciones de funcionamiento de este servicio en el marco del sitio de Internet.

– Sobre el funcionamiento del servicio Amazon CloudFront en el marco del sitio de Internet de la CFE

110 En el caso de autos, consta que el sitio de Internet de la CFE utiliza la red de distribución de contenidos Amazon CloudFront y que esta red se activa cada vez que un usuario consulta el referido sitio de Internet.

111 De los autos, en particular de las respuestas de las partes a la diligencia de ordenación del procedimiento de 21 de julio de 2023 y de sus informes orales y respuestas en la vista de 17 de octubre de 2023, se desprende que, en primer lugar, el servicio Amazon CloudFront es un servicio de Internet que acelera la distribución de los contenidos de Internet —en el caso de autos, del contenido del sitio de Internet de la CFE— a los usuarios. El servicio Amazon CloudFront distribuye el contenido a través de una red mundial de servidores o de centros de datos denominados «ubicaciones periféricas» o «servidores periféricos».

112 En segundo lugar, el servicio Amazon CloudFront se basa en un mecanismo de enrutamiento que dirige la solicitud de un usuario del sitio de Internet de la CFE hacia el servidor periférico que proporciona el menor tiempo de latencia, con arreglo a un principio de proximidad con la terminal del usuario, con la finalidad de que el contenido se transmita al usuario en las mejores condiciones posibles. Si, como consecuencia, en particular, de dificultades técnicas, no está disponible el servidor periférico que presente la menor latencia, la conexión se establece con el que tenga la segunda menor latencia y así sucesivamente.

113 En tercer lugar, el sitio de Internet de la CFE utiliza el servicio Amazon CloudFront en virtud del contrato n.º 2020-1742, firmado entre la Comisión y AWS EMEA, filial propiedad de la empresa estadounidense Amazon.com, con sede social en Luxemburgo (véase el anterior apartado 12).

114 En cuarto lugar, en ese contrato, la Comisión optó, por lo que respecta al sitio de Internet de la CFE, por la zona geográfica denominada «América del Norte (Estados Unidos, México, Canadá), Europa e Israel». Esto significa que la distribución de contenidos de este sitio de Internet no se realiza a través de la red mundial de ubicaciones periféricas de Amazon CloudFront, sino únicamente a través de aquellas situadas en las zonas geográficas antes citadas, es decir, los Estados Unidos, México, Canadá, Europa e Israel.

115 En quinto lugar, por el principio de proximidad mencionado en el anterior apartado 112, las solicitudes de consulta del sitio de Internet de la CFE que cursan los usuarios de la Unión suelen dirigirse a servidores periféricos de la red Amazon CloudFront situados en ese territorio, siendo, en cambio, raros los supuestos en que tales solicitudes se dirigen a servidores situados fuera de la Unión.

116 En sexto lugar, de los autos se desprende que la infraestructura de la red de ubicaciones periféricas de Amazon CloudFront la suministra un conjunto de empresas, algunas de las cuales pertenecen al grupo Amazon y otras son empresas terceras cuya relación puede consultarse en el sitio de Internet de Amazon Web Services, en función de la zona geográfica de que se trate. Por lo que se refiere a la zona geográfica denominada «América del Norte (Estados Unidos, México, Canadá), Europa e Israel», las empresas en cuestión están domiciliadas tanto en Estados miembros de la Unión como fuera de la Unión, en particular en los Estados Unidos, Israel, México, Suiza o el Reino Unido. Todas las empresas explotan servidores en el país en el que están domiciliadas, por lo que la ubicación geográfica de los servidores que intervienen en la prestación del servicio Amazon CloudFront también depende de la ubicación de las empresas en cuestión.

117 En séptimo lugar, las cláusulas del contrato entre la Comisión y AWS EMEA establecen, en particular, lo siguiente:

– AWS EMEA debe poder garantizar que los datos permanezcan en reposo y en tránsito en el territorio del EEE (sección 11.2 del contrato);

– no se autoriza a AWS EMEA a cambiar la ubicación del tratamiento de datos sin previa autorización de la Comisión [sección 12.2.3, letra a), del contrato];

– toda transferencia de datos personales en virtud del contrato a terceros países u organizaciones internacionales debe cumplir íntegramente las exigencias expuestas en el capítulo V del Reglamento 2018/1725 [sección 12.2.3, letra b), del contrato];

– AWS EMEA no puede transferir ningún dato personal a un país situado fuera del EEE, a menos que la Comisión haya dado su autorización previa por escrito a esa transferencia y que la transferencia tenga lugar respetando las condiciones de dicho capítulo V (sección 1.8.9 del contrato);

– AWS EMEA debe transmitir a la Comisión cualquier solicitud de acceso a los datos personales y debe utilizar todos los recursos disponibles contra tales solicitudes (secciones 1.8.3, 1.8.4 y 1.8.5 del contrato);

– AWS EMEA debe asegurarse de que estas medidas también se aplican en caso de recurso a subcontratistas (sección 1.8.8 del contrato).

118 En octavo lugar, la Comisión consultó al SEPD acerca de las cláusulas contractuales antes mencionadas, pero este no las autorizó formalmente, con arreglo al artículo 48, apartado 3, letra a), del Reglamento 2018/1725.

– Transferencia controvertida con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022

119 [En su versión rectificada mediante auto de 3 de junio de 2025] El demandante sostiene, en esencia, que, con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, apreció que determinados datos personales suyos, en particular su dirección IP e información sobre su navegador y su terminal, habían sido transferidos a los Estados Unidos. En efecto, en primer término, estima que dicho sitio de Internet utiliza una red de distribución de contenidos denominada «Amazon CloudFront», cuyo operador es Amazon Web Services, una empresa estadounidense filial de la empresa norteamericana Amazon.com. En segundo término, el demandante aduce que, con ocasión de esa consulta, ciertos datos personales suyos fueron enviados al servicio Amazon CloudFront, más concretamente al servidor de Amazon.com, domiciliada en Seattle (Washington, Estados Unidos), cuya dirección IP es 18.66.192.74. En tercer término, alega que Amazon facilitó la clave de seguridad utilizada por el sitio de Internet de la CFE (denominada «certificado SSL»), motivo por el cual considera que hay que presumir que Amazon podía descodificar todos los datos personales del demandante transferidos a sus servidores, incluidas las opiniones de este sobre el futuro de Europa. En cuarto término, sostiene que la empresa que presta el servicio Amazon CloudFront está sometida a las leyes estadounidenses, por lo que está obligada a transmitir información a los servicios de seguridad y vigilancia de los Estados Unidos, incluso en el caso de que los servidores estén ubicados fuera de ese país. Además, reprocha a la Comisión que no haya adoptado «medidas adicionales», en el sentido de la sentencia Schrems II, para garantizar un nivel de protección adecuado de los datos transferidos a los Estados Unidos.

120 La Comisión rebate estas alegaciones.

121 Por lo que respecta a la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, de los autos se desprende que el demandante consultó ese día el citado sitio de Internet (véase el anterior apartado 3) y que, con ocasión de esa consulta, se produjo la transferencia de su dirección IP y de información sobre su navegador y su terminal.

122 A este respecto, es preciso señalar que la dirección IP debe ser calificada de dato personal, en el sentido del artículo 3, punto 1, del Reglamento 2018/1725, puesto que cumple los dos requisitos que en él se establecen. Por un lado, es una información sobre una persona física y, por otro, se trata de una persona identificada o identificable, en este caso el demandante (sentencia de 26 de abril de 2023, JUR/SEPD, T-557/20, recurrida en casación, EU:T:2023:219, apartado 59; véanse también, en este sentido y por analogía, las sentencias de 24 de noviembre de 2011, Scarlet Extended, C-70/10, EU:C:2011:771, apartado 51, y de 19 de octubre de 2016, Breyer, C-582/14, EU:C:2016:779, apartado 49). En efecto, incluso las direcciones IP denominadas «dinámicas», que, por naturaleza, son cambiantes, se corresponden con una identidad precisa en un momento dado, que, en el presente asunto, coincide con el momento en que tuvo lugar la consulta del sitio de Internet de la CFE.

123 También se ha demostrado que la transferencia de datos mencionada en el anterior apartado 121 fue efectuada por el sitio de Internet de la CFE, a través del servicio Amazon CloudFront, con destino a un servidor cuya dirección IP es 18.66.192.74.

124 Se ha acreditado asimismo que, en el momento de los hechos, la dirección IP 18.66.192.74 estaba atribuida a un servidor ubicado en Múnich (Alemania) y que ese servidor pertenecía a la empresa A 100 ROW GmbH, que estaba domiciliada en Alemania y formaba parte de la relación de empresas citada en el anterior apartado 116.

125 De ello se deduce ciertamente que, con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, hubo una transferencia de datos personales —en el sentido del artículo 3, punto 1, del Reglamento 2018/1725— del demandante, especialmente de su dirección IP.

126 Sin embargo, en el presente asunto no se ha demostrado que, con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, haya habido una transferencia de datos personales del demandante a un tercer país y, en particular, a los Estados Unidos.

127 En cambio, de los apartados 121 a 124 de la presente sentencia se desprende que, con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, la transferencia de datos personales del demandante fue efectuada por el sitio de Internet de la CFE, a través del servicio Amazon CloudFront, con destino a un servidor ubicado en Múnich. Dicho servidor pertenecía a una empresa domiciliada en Alemania, que formaba parte de la red de prestadores de la infraestructura del servicio Amazon CloudFront, servicio que se presta a la Comisión sobre la base de un contrato con AWS EMEA, empresa domiciliada en Luxemburgo.

128 De ello se deduce que, con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, los datos personales del demandante fueron transferidos a un destinatario domiciliado en la Unión.

129 Por otro lado, incluso admitiendo que los datos personales del demandante no hubieran abandonado el territorio de la Unión, tales datos fueron, no obstante, transferidos a un servidor que pertenece a la red de ubicaciones periféricas del servicio Amazon CloudFront, que comprende, por lo que respecta a la distribución de contenidos del sitio de Internet de la CFE, una red de ubicaciones periféricas que no se circunscribe al territorio del EEE, sino que va más allá de él (véase el anterior apartado 116).

130 Sin embargo, las circunstancias concretas descritas en el anterior apartado 127 no demuestran la existencia de una transferencia de datos personales a destinatarios domiciliados fuera del territorio del EEE, en particular en los Estados Unidos.

131 Así pues, la transferencia controvertida con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022 no equivale a una transferencia de datos personales a un tercer país, en el sentido del artículo 46 del Reglamento 2018/1725, dado que el concepto de transferencia a un tercer país exige que los datos personales sean puestos a disposición de un destinatario domiciliado fuera del EEE (véase el apartado 93 de la presente sentencia).

132 La alegación del demandante basada en que AWS EMEA está obligada, como filial de una empresa estadounidense, a transferir los datos personales a las autoridades estadounidenses, aun cuando tales datos estén almacenados en el territorio de la Unión, no desvirtúa esta conclusión.

133 Si bien es cierto que el acceso a los datos personales tratados en el EEE por las autoridades de un tercer país en virtud de la normativa de ese país constituye una transferencia de datos personales a un tercer país, en el sentido del artículo 46 del Reglamento 2018/1725, no es menos cierto que, en el caso de autos, no se ha demostrado que ese acceso haya tenido lugar. En efecto, el demandante

no ha demostrado ni alegado que se transfiriera a las autoridades estadounidenses ninguno de sus datos personales ni ha demostrado o alegado la existencia de una solicitud de esas autoridades en cuanto a los datos transferidos a dicho servidor de Amazon CloudFront, ubicado en Múnich.

134 Por tanto, la alegación del demandante no versa sobre una infracción directa de lo dispuesto en el capítulo V del Reglamento 2018/1725, sino únicamente sobre la posibilidad de tal infracción, en el supuesto de que AWS EMEA, por su condición de filial de una empresa norteamericana, no pueda oponerse a una petición de las autoridades estadounidenses que tenga por objeto el acceso a datos almacenados en servidores ubicados en el territorio del EEE.

135 Pues bien, la mera posibilidad de que un tercer país acceda a datos personales no equivale a una transferencia de datos, en el sentido del artículo 46 del Reglamento 2018/1725, tal como se ha interpretado en el anterior apartado 93, puesto que no se ha demostrado que, por transmisión o de otro modo, se hayan puesto datos personales del demandante a disposición de un destinatario domiciliado en un tercer país. En otras palabras, la posible infracción del citado artículo 46 no puede asimilarse a una infracción directa de esta disposición.

136 Además, procede recordar que, en el marco de la presente petición de indemnización, el examen del Tribunal General versa sobre la comprobación de los requisitos para que se genere la responsabilidad extracontractual de la Comisión y, en particular, sobre el requisito relativo a la ilegalidad del comportamiento de la Comisión, que exige que se demuestre una violación suficientemente caracterizada de las disposiciones del Reglamento 2018/1725 y de la Carta invocadas por el demandante.

137 A este respecto, la mera posibilidad de que se infrinja lo dispuesto en el capítulo V del Reglamento 2018/1725 no basta, en todo caso, para demostrar una actuación ilícita de la Comisión que equivalga a una violación suficientemente caracterizada de dichas disposiciones.

138 No desvirtúa esta conclusión la alegación del demandante basada en la sentencia Schrems II. En efecto, es preciso señalar que, en esa sentencia, el Tribunal de Justicia se pronunció sobre algunas de las condiciones en las que pueden transferirse datos personales a los Estados Unidos y no sobre las condiciones en las que pueden tratar tales datos, en el territorio del EEE, filiales de sociedades estadounidenses, como AWS EMEA.

139 De todo lo anterior resulta que, por lo que respecta a la transferencia controvertida con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, el demandante no ha demostrado que la Comisión hubiera cometido una violación suficientemente caracterizada, en el sentido de la jurisprudencia recordada en el anterior apartado 50, de las disposiciones de los artículos 46 y 48, apartados 1 y 2, letra b), del Reglamento 2018/1725 y de los artículos 7, 8 y 47 de la Carta.

140 Por consiguiente, dado que no concurre uno de los requisitos acumulativos para que se genere la responsabilidad extracontractual de la Unión, previstos en el artículo 340 TFUE, párrafo segundo, hay que desestimar la segunda petición de indemnización en lo que respecta a la transferencia controvertida con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022, sin que sea necesario examinar las demás alegaciones del demandante.

– Transferencia controvertida con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022

141 El demandante sostiene que, con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022, se produjo una transferencia de sus datos personales, en particular de su dirección IP, a servidores de Amazon CloudFront situados en los Estados Unidos. Según el demandante, estas transferencias no se derivan de su actividad como usuario del sitio de Internet, sino que son el resultado del funcionamiento del servicio Amazon CloudFront, en cuyo contexto la posibilidad de que se transfieran datos a los Estados Unidos es inherente a la infraestructura mundial en la que se sustenta este servicio. El demandante aduce que su situación no difiere de la de un ciudadano de la Unión que consulta el sitio de Internet de la CFE con ocasión, por ejemplo, de un desplazamiento profesional a los Estados Unidos. Estima que la Comisión no da muestras de toda la diligencia necesaria para evitar las transferencias de datos a los Estados Unidos al haber optado por una red de distribución de contenidos basada en una estructura a escala mundial, en lugar de una solución de alojamiento únicamente europea.

142 Según el demandante, la citada transferencia de datos personales le causó daños y perjuicios inmateriales, en el sentido del considerando 46 del Reglamento 2018/1725, puesto que perdió el control de sus datos, que fueron transferidos a los Estados Unidos y sometidos a una vigilancia ilegal por parte de las autoridades estadounidenses, y se vio privado de sus derechos y libertades.

143 La Comisión rebate estas alegaciones.

144 Con carácter preliminar y habida cuenta de la argumentación del demandante, procede recordar que, en la presente petición de indemnización, el examen del Tribunal General no versa directamente sobre la legalidad de la decisión de la Comisión de utilizar el servicio Amazon CloudFront para distribuir contenidos del sitio de Internet de la CFE, sino sobre la verificación de los requisitos para que se genere la responsabilidad extracontractual de la Comisión en lo que respecta a la transferencia controvertida con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022.

145 En el caso de autos, el Tribunal General considera oportuno comenzar examinando el requisito relativo a la existencia de una relación de causalidad entre el supuesto comportamiento ilícito de la Comisión y los daños y perjuicios inmateriales alegados.

146 De la jurisprudencia recordada en el anterior apartado 55 resulta que el requisito relativo a la relación de causalidad entraña la existencia de una relación suficientemente directa de causa a efecto entre el comportamiento reprochado a la institución y el daño, relación que corresponde probar al demandante, de modo que el comportamiento reprochado debe ser la causa determinante del perjuicio.

147 Además, de la jurisprudencia resulta que el nexo causal exigido para generar la responsabilidad extracontractual de la Unión en el sentido del artículo 340 TFUE, párrafo segundo, existe desde el momento en que el perjuicio es la consecuencia directa de la falta de que se trate (sentencia de 28 de junio de 2007, Internationaler Hilfsfonds/Comisión, C-331/05 P, EU:C:2007:390, apartado 23).

148 En lo relativo al carácter directo de la relación de causalidad, el Tribunal General ya ha declarado que el perjuicio debe resultar directamente de la ilegalidad reprochada y no de una elección del demandante respecto del modo de reaccionar ante el acto supuestamente ilegal. De ese modo, se

ha considerado que el mero hecho de que el comportamiento ilegal haya constituido una condición necesaria (*conditio sine qua non*) para que se produjera el perjuicio, en el sentido de que este no hubiera tenido lugar sin dicho comportamiento, no basta para demostrar una relación de causalidad suficientemente directa con arreglo a la jurisprudencia de la Unión (véanse, en este sentido y por analogía, las sentencias de 30 de noviembre de 2011, Transnational Company «Kazchrome» y ENRC Marketing/Consejo y Comisión, T-107/08, EU:T:2011:704, apartado 80 y jurisprudencia citada, y de 23 de mayo de 2019, Remag Metallhandel y Jaschinsky/Comisión, T-631/16, no publicada, EU:T:2019:352, apartado 52 y jurisprudencia citada).

149 Así pues, de la jurisprudencia se desprende que esa relación de causalidad no se demuestra cuando el perjuicio alegado es consecuencia directa de la propia decisión o de la libre elección del demandante y, por consiguiente, no puede imputarse a la institución o al órgano de que se trate (véanse, en este sentido y por analogía, las sentencias de 28 de junio de 2007, Internationaler Hilfsfonds/Comisión, C-331/05 P, EU:C:2007:390, apartados 22 a 29; de 17 de febrero de 2017, Novar/EUIPO, T-726/14, EU:T:2017:99, apartados 31 y 32, y de 28 de febrero de 2018, Vakakis kai Synergates/Comisión, T-292/15, EU:T:2018:103, apartado 173 y jurisprudencia citada).

150 Por tanto, en el caso de autos, es preciso determinar si el comportamiento reprochado a la Comisión, es decir, la utilización del servicio Amazon CloudFront como red de distribución de contenidos del sitio de Internet de la CFE, es la causa directa de los daños y perjuicios inmateriales alegados, consistentes en la pérdida del control sobre los datos personales del demandante que supuestamente fueron transferidos a los Estados Unidos cuando consultó dicho sitio de Internet el 8 de junio de 2022.

151 A este respecto, en primer término, de los autos y de las respuestas de las partes a las preguntas formuladas en la vista resulta que, el 8 de junio de 2022, el demandante se encontraba en Múnich y consultó varias veces el sitio de Internet de la CFE. En esas consultas, la dirección IP del demandante estableció conexiones sucesivas con diferentes servidores del servicio Amazon CloudFront, geográficamente muy distantes entre sí. De este modo, se conectó a las 7.13 h a un servidor situado en Múnich, a las 11.13 h a un servidor ubicado en Londres (Reino Unido), a las 12.56 h a un servidor situado en Hillsboro (Oregón, Estados Unidos), a las 13.05 h a un servidor ubicado en Newark y a las 19.12 h a un servidor que se encontraba en Fráncfort del Meno (Alemania).

152 En segundo término, de los autos se desprende que la dirección IP del demandante fue transferida a los diferentes servidores del servicio Amazon CloudFront mencionados en el anterior apartado 151, incluidos los ubicados en los Estados Unidos.

153 En tercer término, procede recordar que la dirección IP del demandante constituye un dato personal.

154 En cuarto término, es preciso indicar que el 8 de junio de 2022 el sitio de Internet de la CFE contabilizó 4 548 accesos y dieciocho direcciones IP diferentes. Entre ellas, una única dirección IP, a saber, la del demandante, estableció una conexión con servidores situados fuera de la Unión, concretamente en los Estados Unidos y en el Reino Unido. A este respecto, hay que observar que no se ha demostrado, ni siquiera alegado, que, el 8 de junio de 2022, el servicio Amazon CloudFront correspondiente al sitio de Internet de la CFE hubiese tenido problemas técnicos o de otra naturaleza que impidieran el funcionamiento normal de su mecanismo de enrutamiento con arre-

glo al principio de proximidad, el cual dirige las solicitudes de los usuarios del sitio de Internet de la CFE hacia el servidor periférico que proporciona la menor latencia en función de la ubicación geográfica del usuario (véase el anterior apartado 112).

155 En quinto término, por lo que respecta a las circunstancias relativas a las conexiones de la dirección IP del demandante a servidores situados en los Estados Unidos, por una parte, de los autos y de las respuestas de las partes en la vista se desprende que el demandante sostiene que tales conexiones eran el resultado del funcionamiento de Amazon CloudFront y no de ninguna otra manipulación que pudiera imputársele. Por otra parte, la Comisión observa que esas conexiones eran atípicas y solo pueden explicarse mediante una manipulación técnica del demandante.

156 A este respecto, procede señalar que las circunstancias descritas en el anterior apartado 151 demuestran que las diferentes ubicaciones de los servidores a los que se conectó la dirección IP del demandante no pueden ser el resultado de unos desplazamientos físicos realizados por el demandante en el mismo día, los cuales no son posibles, habida cuenta de las distancias y de los intervalos de tiempo de que se trata. Tampoco se han demostrado, ni siquiera alegado, fallos en el servicio Amazon CloudFront, lo que permite concluir que, el 8 de junio de 2022, este servicio funcionaba con arreglo al principio de proximidad con la terminal del usuario y que su mecanismo de enrutamiento dirigía las solicitudes de los usuarios del sitio de Internet de la CFE hacia el servidor periférico que proporcionaba el menor tiempo de latencia (véase el anterior apartado 154).

157 En estas circunstancias, las conexiones de la dirección IP del demandante a servidores ubicados en los Estados Unidos mientras se encontraba en Alemania no son el resultado del funcionamiento normal del servicio Amazon CloudFront, sino más bien de un ajuste técnico llevado a cabo por el demandante, con el objetivo de modificar su ubicación aparente y de presentarse en el ámbito digital como si, en el mismo día, se encontrara sucesivamente en lugares próximos a Múnich, Londres, Hillsboro, Newark y Fráncfort del Meno.

158 De ello se deduce que, ciertamente, el funcionamiento del servicio Amazon CloudFront, junto con su mecanismo de enrutamiento que funciona con arreglo al principio de proximidad y cubre una zona geográfica mayor que el territorio del EEE, que incluye, en particular, los Estados Unidos (véanse los apartados 112 y 114 de la presente sentencia), permitió que, al consultar el sitio de Internet de la CFE, la dirección IP del demandante se conectara a servidores de Amazon CloudFront ubicados en los Estados Unidos.

159 No obstante, aunque la utilización por la Comisión del servicio Amazon CloudFront sea una condición necesaria para que se produzcan las transferencias de datos personales a los Estados Unidos mencionadas en el anterior apartado 152, esta circunstancia no basta, en caso de autos, para establecer una relación de causalidad suficientemente directa entre los daños y perjuicios inmateriales alegados por el demandante y el comportamiento supuestamente ilícito de la Comisión, consistente en utilizar ese servicio infringiendo lo dispuesto en el capítulo V del Reglamento 2018/1725.

160 En efecto, debe considerarse que la conducta del demandante constituye la causa directa e inmediata de los daños y perjuicios inmateriales alegados y no la ilegalidad supuestamente cometida por la Comisión utilizando el servicio Amazon CloudFront.

161 Así pues, fue el demandante quien estableció las condiciones necesarias para conectarse a servidores situados en los Estados Unidos mediante el funcionamiento del servicio Amazon CloudFront. Fue la conducta del demandante lo que hizo que el mecanismo de enrutamiento del servicio Amazon CloudFront enviara sus solicitudes de consulta del sitio de Internet de la CFE hacia servidores ubicados en los Estados Unidos, puesto que estos tenían la menor latencia en relación con la ubicación aparente del demandante en el ámbito digital, que no coincidía con su ubicación real.

162 Por otro lado, el demandante no puede adoptar una conducta que pretende provocar un determinado resultado (concretamente la transferencia de sus datos personales a un tercer país) y solicitar, posteriormente, la indemnización de los perjuicios supuestamente causados por ese resultado, cuya causa directa es su propia conducta. Así pues, a diferencia de lo que alega el demandante, en un recurso de indemnización como el del caso de autos, su situación no puede apreciarse de manera similar a la de un usuario que se haya desplazado efectivamente a los Estados Unidos y que, consecuentemente, haya accedido al sitio de Internet de la CFE desde ese país.

163 De todo lo anterior resulta que, por lo que respecta a la transferencia controvertida con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022, no se ha demostrado una relación de causalidad suficientemente directa entre el comportamiento supuestamente ilegal de la Comisión y los daños y perjuicios alegados.

164 Dado que no concurre uno de los requisitos acumulativos para generar la responsabilidad extracontractual de la Unión, hay que desestimar la petición de indemnización en lo que respecta a la transferencia controvertida con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022, sin que sea necesario examinar los demás requisitos para generar dicha responsabilidad.

– *Transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022*

165 El demandante sostiene que, el 30 de marzo de 2022, cuando se registró en el evento «GoGreen» disponible en el sitio de Internet de la CFE, su dirección IP e información sobre su navegador y su terminal fueron transferidas a la empresa Meta Platforms, domiciliada en los Estados Unidos y propietaria de la red social Facebook. En efecto, con ocasión de ese registro, el demandante alega haber sido dirigido al servicio de autenticación de la Unión EU Login, que ofrece, en particular, conectarse a través de diferentes redes sociales. El demandante aduce haber optado por la conexión a través de su cuenta de Facebook y que, cuando seleccionó el hipervínculo que le redirigía hacia Facebook, ese enlace condujo a la transferencia de su dirección IP a Facebook. El demandante sostiene haber aceptado únicamente las «*cookies* esenciales» de Facebook. El demandante imputa a Facebook haber recabado y transferido a los servidores de Meta Platforms otros datos personales suyos, en concreto su dirección de correo electrónico, su nombre y apellido y su foto de perfil, sirviéndose de *cookies*, en particular de la denominada «sb». Estima que de la jurisprudencia se desprende que los gestores de sitios de Internet que utilizan Facebook en sus sitios de Internet, como es el caso de la Comisión, son responsables, junto con Facebook, de que se respete el Derecho de la Unión en materia de protección de datos. Así pues, concluye que la Comisión es corresponsable de la instalación de las *cookies* que almacena Facebook. El demandante alega haber perdido el control sobre sus datos personales transferidos a Facebook y haberse visto privado de sus derechos y libertades, lo que, en su opinión, da lugar a daños y perjuicios inmateriales en el sentido del considerando 46 del Reglamento 2018/1725.

166 La Comisión rebate tal argumentación. Alega, en esencia, que no transfirió datos a Meta Platforms. Estima que no es obligatorio registrarse a través de EU Login para participar en el evento «GoGreen» y aduce que, aunque utilizara EU Login, el demandante tuvo diferentes posibilidades de autenticación, incluidas algunas que no exigen la utilización de una cuenta en redes sociales. Por tanto, estima que fue elección del demandante conectarse al servicio EU Login con su cuenta de Facebook, por lo que fue él y no la Comisión quien inició el acceso al sitio de Internet de Facebook. Además, la Comisión sostiene que, desde un punto de vista técnico, la opción de autenticación a través de Facebook se lleva a cabo mediante el hipervínculo que se muestra en el sitio de Internet EU Login, que no incluye datos personales del usuario. A diferencia de lo que sostiene el demandante, la Comisión aduce que los datos recabados mediante las *cookies* utilizadas por Facebook no se transfieren a la Comisión al conectarse a EU Login ni son responsabilidad suya. En opinión de la Comisión, esas *cookies* son el resultado de intercambios entre Facebook y el demandante, en virtud del consentimiento prestado por este, sin que ella intervenga en esos intercambios. La Comisión sostiene asimismo que la jurisprudencia aducida por el demandante no es aplicable en el presente asunto y que, en cualquier caso, la alegación del demandante basada en una supuesta responsabilidad conjunta de la Comisión y de Meta Platforms es un motivo nuevo formulado por vez primera en la fase de réplica, que, por consiguiente, es inadmisible.

167 En el caso de autos, procede comenzar examinando el marco fáctico en el que se inscribe la transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022, teniendo en cuenta los datos que resultan de los autos y las respuestas de las partes a las preguntas formuladas por el Tribunal General en la vista y mediante la diligencia de ordenación del procedimiento de 9 de febrero de 2024.

168 A este respecto, procede señalar que el evento «GoGreen», organizado por un organismo establecido en los Países Bajos, fue anunciado en el sitio de Internet de la CFE. El registro para dicho evento podía efectuarse, en particular, en el sitio de Internet de la CFE, a través del servicio EU Login.

169 El demandante optó por registrarse en el sitio de Internet de la CFE utilizando EU Login.

170 EU Login es el servicio de autenticación de usuario de la Comisión, que protege varios centenares de sitios Internet y aplicaciones vinculados a la Unión. En el caso de autos, la conexión a EU Login, con vistas a registrarse en el evento «GoGreen», tenía como objetivo garantizar que dicho registro se realizara a través de una dirección electrónica verificada, reduciendo los riesgos ligados al registro de falsos usuarios o a la usurpación de identidad.

171 EU Login presenta varias opciones de conexión en su página web. La primera opción es conectarse directamente a EU Login, bien rellenando los datos de conexión referidos a una cuenta de EU Login preexistente, bien creando una cuenta para tal servicio. La segunda opción es utilizar un documento de identidad electrónico «eID», disponible para los ciudadanos de determinados Estados miembros. La tercera opción, posible para un número limitado de servicios, consiste en utilizar una cuenta que el usuario ya posea en Facebook, Twitter o Google, seleccionando el hipervínculo correspondiente, que se muestra en el sitio de Internet de EU Login.

172 La posibilidad de conectarse a EU Login a través de una cuenta de Facebook deriva del hecho de que la Comisión consideró que ha de darse a los usuarios la posibilidad de conectarse a EU Login a través de cuentas preexistentes en plataformas —con el fin de ofrecerles un acceso más fácil y rápido— y la posibilidad de autenticarse sin necesidad de crear una cuenta EU Login, con lo que,

de este modo, se evita multiplicar el número de cuentas y de entidades con las que los usuarios deben compartir sus datos personales. Por otro lado, la Comisión consideró que Facebook era fiable a los efectos de comprobar las direcciones electrónicas de los usuarios, habida cuenta de las medidas que adopta. No obstante, el hipervínculo que permite conectarse a través de una cuenta Facebook preexistente solo está disponible en EU Login para aquellos sitios de Internet o aplicaciones que no requieren más que un nivel de seguridad básico.

173 El demandante optó por conectarse a EU Login a través de su cuenta de Facebook, utilizando el hipervínculo «Sign in with Facebook» que se muestra en el sitio de Internet de EU Login (en lo sucesivo, «hipervínculo “conectarse con Facebook”»).

174 El hipervínculo «conectarse con Facebook» contiene un enlace a un sitio de Internet externo a la Comisión. Cuando se activa este hipervínculo seleccionándolo, da acceso a una dirección URL del sitio de Internet de Facebook, es decir, a una dirección individual de ese sitio de Internet.

175 El acceso a la dirección URL del sitio de Internet de Facebook da lugar a una comunicación entre el navegador del usuario y el citado sitio de Internet, en cuyo marco el navegador transfiere la dirección IP del usuario al sitio de Internet de que se trata. Esa transferencia es similar a la que se produce cuando el usuario utiliza directamente la dirección URL de cualquier sitio de Internet en su navegador, puesto que cualquier internauta que desee acceder a un sitio de Internet debe comunicar forzosamente la dirección IP.

176 A través del hipervínculo «conectarse con Facebook», EU Login envía determinada información a Facebook, que es necesaria para el proceso de autenticación y que adopta la forma del siguiente ejemplo:

https://www.facebook.com/v3.0/dialog/oauth?response_type=code&
client_id=1200572836629487&
redirect_uri=https%3A%2F%2Fecas.ec.europa.eu%2Fcas%2FoAuthCallback&scope=email&
state=useFacebook%7CECAS_LR-5249395-
yQYIt4muQF7PyfSbvEk42Lt0Zm6AmYrUlJfVU5FfsrkYNTaFX552FQShXP9oggHF9jlEUohJx6I4ACrQJ0zPJ4-rS0vSrmBGYCzOpBivVtNak-
93Am7vhlDrqH4FT9cBOzViGrSdq4b2TrFkbOxzHB4zyingpuKF16KQfMnmu5izfXzUIIDHx1HqNS9QGEFVWzoeq0

177 Más concretamente, la información contenida en el hipervínculo «conectarse con Facebook» es la siguiente:

– en primer lugar, la parte «client_id=1200572836629487» contiene un «código de identificación único» que identifica a EU Login como aplicación. Este número identificativo es el mismo para todos los usuarios que deseen autenticarse en EU Login utilizando Facebook;

– en segundo lugar, la parte «redirect_uri=https%3A%2F%2Fecas.ec.europa.eu%2Fcas%2FoAuthsback» contiene la dirección URL genérica de EU Login, que es la dirección a la que Facebook debe enviar al usuario una vez que este haya prestado su consentimiento a que Facebook transfiera sus datos personales a EU Login;

– en tercer lugar, la parte «scope=email» contiene los datos que Facebook debe transferir a EU Login para garantizar que el usuario es debidamente autenticado, en particular su dirección electrónica y el nombre y los apellidos que se indicaron en el sitio de Facebook cuando se creó la cuenta de Facebook;

– en cuarto lugar, la parte «state=useFacebook» indica que la larga cadena de caracteres que sigue es un valor aleatorio de seguridad que se utiliza para evitar los ataques de seguridad y que tiene una validez limitada en el tiempo. EU Login genera este valor aleatorio de seguridad aleatoriamente y cumple la función de frase secreta que Facebook debe repetir cuando se transfieren datos a EU Login, a fin de que EU Login pueda saber que la dirección electrónica, el nombre y los apellidos comunicados se refieren al usuario que ha puesto en marcha el método de autenticación. Expirado el plazo o autenticado el usuario, ya no es posible utilizar el valor de seguridad; y

– en quinto lugar, la parte «response_type=code» indica que la transferencia de datos de Facebook a EU Login sigue yendo acompañada de un código único. Este código único incluye el valor aleatorio de seguridad anteriormente mencionado. El código único equivale a un número de registro único o a un número de serie que autentifica los datos transferidos por Facebook a EU Login.

178 Una vez que el usuario accede a la dirección URL de Facebook, se halla en ese sitio de Internet, en el que, en primer lugar, se muestra una ventana que pide al usuario que acepte el uso, por parte de Facebook, de testimonios de conexión o *cookies*. A continuación, si se aceptan las *cookies*, se abre otra ventana, lo que permite rellenar el nombre de usuario y la contraseña de la cuenta del usuario en Facebook. Por último, una vez conectado a su cuenta de Facebook, el usuario puede autorizar a Facebook a que utilice *cookies* en otras aplicaciones y sitios de Internet respondiendo a la pregunta «Allow Facebook to use cookies and similar technologies placed on other apps and websites?». Si el usuario da su consentimiento a este uso, se le requerirá posteriormente para que preste su consentimiento a que Facebook facilite a EU Login los nombres, apellidos, foto de perfil y dirección electrónica vinculados a su cuenta de Facebook. Por otro lado, a lo largo de este proceso, el usuario puede interrumpir la autenticación a través de su cuenta de Facebook eligiendo la opción «Cancel». En este supuesto, es redirigido al sitio de Internet de EU Login, en el que se vuelve a mostrarse la página con las opciones de conexión.

179 En el caso de autos, cuando el demandante seleccionó el hipervínculo «conectarse con Facebook», su navegador de Internet accedió a la dirección URL del sitio de Internet de Facebook y, consecuentemente, comunicó a dicho sitio su dirección IP. A continuación, cuando se encontraba en el sitio de Internet de Facebook, el demandante seleccionó las opciones que permitían a Facebook utilizar únicamente las *cookies* esenciales, se conectó, posteriormente, a su cuenta de Facebook y, por último, autorizó a Facebook a que comunicara a EU Login su nombre, apellido, foto de perfil y dirección electrónica, tal como los había cumplimentado en su cuenta de Facebook.

180 A raíz de estas autorizaciones, Facebook remitió al demandante al sitio de Internet de EU Login, de conformidad con lo indicado en el hipervínculo «conectarse con Facebook» (véase el anterior apartado 177, guiones primero y segundo).

181 Al mismo tiempo, Facebook comunicó a EU Login el valor aleatorio de seguridad y el código único mencionados en el anterior apartado 177, guiones cuarto y quinto. Por una parte, esta comunicación de Facebook permitió a EU Login saber que los datos personales que Facebook

ponía a su disposición correspondían al usuario que había puesto en marcha el proceso de autenticación, esto es, en el caso de autos, el demandante. Por otra parte, permitió a EU Login acceder, durante un período de tiempo limitado, a los datos personales mencionados en el anterior apartado 177, tercer guion, esto es, en particular, el nombre, el apellido y la dirección de correo electrónico del demandante, tal como los cumplimentó en su cuenta de Facebook. La transferencia de esos datos por Facebook a EU Login se hizo a través de una conexión encriptada entre ellos. EU Login autenticó la dirección electrónica del demandante sobre la base de los datos puestos a disposición por Facebook.

182 Por otro lado, es preciso indicar que la red social Facebook es propiedad de Meta Platforms, empresa domiciliada en los Estados Unidos.

183 Además, procede señalar que la visualización de este hipervínculo en el sitio de Internet de EU Login se rige por las condiciones generales de la plataforma Facebook, divulgadas en la dirección de Internet «https://developers.facebook.com/terms».

184 A la luz de estas consideraciones, procede examinar si concurren los requisitos para generar la responsabilidad extracontractual de la Comisión.

185 El demandante alega, en esencia, que, con ocasión de su conexión a EU Login de 30 de marzo de 2022, tuvo lugar una transferencia de datos personales suyos, en particular de su dirección IP, a servidores de la red social Facebook, cuya empresa propietaria está domiciliada en los Estados Unidos. El demandante sostiene que esa transferencia se realizó infringiendo el artículo 46 del Reglamento 2018/1725 y le causó daños y perjuicios inmateriales consistentes en la pérdida del control de sus datos y en la privación de sus derechos y libertades.

186 Con carácter preliminar, procede recordar que, como resulta del anterior apartado 95, una transferencia de datos personales a un tercer país, con arreglo a su artículo 46, exige que una institución, organismo u órgano de la Unión ponga, por transmisión o de otro modo, datos personales a disposición de un destinatario domiciliado en un tercer país, es decir, un país que no sea miembro ni de la Unión ni del EEE.

187 En el caso de autos, ha quedado demostrado que, en primer término, entre las opciones de conexión a EU Login, el demandante optó por conectarse con su cuenta de Facebook. En segundo término, el hipervínculo «conectarse con Facebook» contiene un enlace a una dirección URL del sitio de Internet de Facebook. En tercer término, cuando el demandante activó ese hipervínculo seleccionándolo, su navegador accedió a la dirección URL del sitio de Internet de Facebook y, posteriormente, transfirió su dirección IP a Facebook (véanse los apartados 173 a 175 de la presente sentencia).

188 De ello se deduce que la Comisión, a través del hipervínculo «conectarse con Facebook», que se muestra en la página web de EU Login, creó las condiciones que permiten que se transfiera la dirección IP del demandante a Facebook. Pues bien, esta dirección IP constituye un dato personal del demandante (véase el anterior apartado 122), que fue transferido, a través de dicho hipervínculo, a Meta Platforms, empresa domiciliada en los Estados Unidos. Por tanto, esa transferencia equivale a una transferencia de datos personales a un tercer país, con arreglo al artículo 46 del Reglamento 2018/1725.

189 Además, ha quedado demostrado en el caso de autos que, cuando se realizó esa transferencia de datos, esto es, el 30 de marzo de 2022, no existía ninguna decisión de adecuación, en el sentido del artículo 47 del Reglamento 2018/1725, con respecto a los Estados Unidos (véase el anterior apartado 100).

190 A falta de una decisión de adecuación de la Comisión con respecto a los Estados Unidos, la transferencia de datos personales a un tercer país o a una organización internacional solo puede hacerse si el responsable del tratamiento o el encargado del tratamiento hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas, de conformidad con el artículo 48, apartado 1, del Reglamento 2018/1725 (véase el anterior apartado 101).

191 En el presente asunto, la Comisión no ha demostrado, ni siquiera alegado, la existencia de una garantía adecuada, en particular de una cláusula tipo de protección de datos o de una cláusula contractual adoptadas en las condiciones establecidas en el artículo 48, apartados 2 y 3, del Reglamento 2018/1725 (véanse los apartados 102 a 104 de la presente sentencia). En cambio, ha quedado demostrado que la visualización del hipervínculo «conectarse con Facebook» en el sitio de Internet de EU Login se rige únicamente por las condiciones generales de la plataforma Facebook (véase el anterior apartado 183).

192 Por consiguiente, la Comisión creó las condiciones para que se produjera la transferencia de datos personales del demandante a un tercer país, sin cumplir, no obstante, las condiciones establecidas en el artículo 46 del Reglamento 2018/1725.

193 Se ha de concluir, por tanto, sin que sea necesario examinar las demás alegaciones del demandante, que la Comisión incurrió en una violación suficientemente caracterizada, en el sentido de la jurisprudencia recordada en el anterior apartado 50, del artículo 46 del Reglamento 2018/1725, por lo que respecta a la transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022.

194 Por consiguiente, es preciso examinar si concurren en el caso de autos los demás requisitos para que se genere la responsabilidad extracontractual de la Comisión, relativas al daño y a la relación de causalidad.

195 El demandante alega que la transferencia ilícita de su dirección IP a una empresa domiciliada en los Estados Unidos le causó daños y perjuicios inmateriales consistentes en la pérdida del control de sus datos y en la privación de sus derechos y libertades.

196 A este respecto, hay que considerar que el artículo 65 del Reglamento 2018/1725 no solo da derecho a una indemnización de los daños y perjuicios materiales, sino también de los daños y perjuicios inmateriales sufridos como consecuencia de la infracción de dicho Reglamento, sin que sea necesario demostrar cierto grado de gravedad [véase, en este sentido y por analogía, la sentencia de 4 de mayo de 2023, Österreichische Post (Daños y perjuicios inmateriales relacionados con el tratamiento de datos personales), C-300/21, EU:C:2023:370, apartados 45 y 51].

197 En el caso de autos, los daños y perjuicios inmateriales alegados por el demandante deben considerarse reales y ciertos, en el sentido de la jurisprudencia recordada en el anterior apartado 54, ya que la transferencia mencionada en el apartado 188 de la presente sentencia,

realizada infringiendo el artículo 46 del Reglamento 2018/1725, colocó al demandante en una situación de inseguridad en cuanto al tratamiento de sus datos personales, en particular de su dirección IP.

198 Además, existe una relación de causalidad suficientemente directa, con arreglo a la jurisprudencia recordada en el anterior apartado 55, entre la infracción por la Comisión del artículo 46 del Reglamento 2018/1725 y los daños y perjuicios inmateriales sufridos por el demandante.

199 En las circunstancias del caso de autos, procede valorar en equidad el importe de los daños y perjuicios inmateriales causados por la Comisión en la cuantía de 400 euros.

200 En consecuencia, se debe condenar a la Comisión a abonar al demandante la cuantía de 400 euros por los daños y perjuicios inmateriales sufridos derivados de la transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022.

Costas

201 A tenor del artículo 134, apartado 3, del Reglamento de Procedimiento del Tribunal General, cuando se estimen parcialmente las pretensiones de una y otra parte, cada parte cargará con sus propias costas. Sin embargo, si se estimase que las circunstancias del caso lo justifican, el Tribunal General podrá decidir que una de las partes cargue, además de con sus propias costas, con una porción de las costas de la otra parte.

202 En el caso de autos, se han desestimado las pretensiones primera y segunda del demandante y una parte de su tercera pretensión. No obstante, se ha estimado parcialmente la tercera pretensión y se condena a la Comisión a pagar la indemnización que el demandante ha solicitado en concepto de indemnización de los daños y perjuicios inmateriales que sufrió como consecuencia de la transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022. En estas circunstancias, procede resolver que la Comisión cargue con sus propias costas y con la mitad de las costas del demandante. El demandante cargará con la mitad de sus propias costas.

En virtud de todo lo expuesto,

EL TRIBUNAL GENERAL (Sala Sexta ampliada)

decide:

1) Declarar el recurso inadmisible en lo que respecta a las pretensiones de anulación.

2) Sobreseer las pretensiones de que declare que la Comisión Europea, contrariamente a Derecho, no se pronunció sobre la solicitud de información del Sr. Thomas Bindl de 1 de abril de 2022.

3) Condenar a la Comisión a abonar al Sr. Bindl la cuantía de 400 euros en concepto de indemnización de los daños y perjuicios inmateriales sufridos.

4) Desestimar las pretensiones de indemnización en todo lo demás.

5) La Comisión cargará con sus propias costas y con la mitad de las costas del Sr. Bindl.

6) El Sr. Bindl cargará con la mitad de sus propias costas.

Costeira Kancheva Öberg

Zilgalvis Tichy-Fisslberger

Pronunciada en audiencia pública en Luxemburgo, a 8 de enero de 2025.

Firmas

Índice

Antecedentes del litigio y hechos posteriores a la interposición del recurso . . . 2

Pretensiones de las partes . . . 3

Fundamentos de Derecho . . . 4

Consideraciones preliminares sobre la protección de datos personales por las instituciones, órganos y organismos de la Unión . . . 4

Sobre la admisibilidad . . . 5

Admisibilidad de las pretensiones de anulación . . . 5

Admisibilidad de las pretensiones por omisión . . . 7

Sobre las pretensiones de indemnización . . . 8

Consideraciones preliminares sobre los requisitos para generar la responsabilidad extracontractual de la Unión en el marco del Reglamento 2018/1725 . . . 8

Sobre la primera petición de indemnización, que tiene como objetivo que se indemnicen los daños y perjuicios inmateriales resultantes de la vulneración del derecho de acceso a la información . . . 10

Sobre la segunda petición de indemnización, que tiene por objeto la indemnización de los daños y perjuicios inmateriales derivados de las transferencias controvertidas . . . 14

– Consideraciones preliminares sobre las disposiciones relativas a la transferencia de datos personales a un tercer país . . . 15

– Sobre el funcionamiento del servicio Amazon CloudFront en el marco del sitio de Internet de la CFE . . . 17

– Transferencia controvertida con ocasión de la consulta del sitio de Internet de la CFE de 30 de marzo de 2022 . . . 19

– Transferencia controvertida con ocasión de las consultas del sitio de Internet de la CFE de 8 de junio de 2022 . . . 22

– Transferencia controvertida con ocasión de la conexión a EU Login de 30 de marzo de 2022 . . . 25

Costas . . . 31