Recopilación de la Jurisprudencia

CONCLUSIONES DEL ABOGADO GENERAL
SR. YVES BOT
presentadas el 23 de septiembre de 2015[1]

Asunto C-362/14

Maximillian Schrems
contra
Data Protection Commissioner

[Petición de decisión prejudicial planteada por la High Court (Irlanda)]

«Procedimiento prejudicial — Datos personales — Protección de las personas físicas en lo que respecta al tratamiento de dichos datos — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8 y 47 — Directiva 95/46/CE — Artículo 25 — Decisión 2000/520/CE — Transferencia de datos personales a Estados Unidos — Evaluación del carácter adecuado o no del nivel de protección — Denuncia de una persona física cuyos datos personales han sido transferidos a un país tercero — Autoridad de control nacional — Facultades»

I. **Introducción**

1. Tal como constató la Comisión Europea en su Comunicación de 27 de noviembre de 2013,[2] «las transferencias de datos personales son un elemento importante y necesario de la relación transatlántica. Forman parte integrante de los intercambios comerciales entre ambos lados del Atlántico, incluidos los relacionados con los nuevos sectores digitales en crecimiento, tales como las redes sociales o la computación en nube, que implican la transferencia de grandes cantidades de datos de la UE a Estados Unidos».[3]

2. Los intercambios comerciales son objeto de 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.[4] Dicha Decisión proporciona una base jurídica para la transferencia de datos personales desde la Unión a empresas establecidas en Estados Unidos que operan conforme al régimen de puerto seguro.

3. La citada Decisión se enfrenta actualmente al reto de facilitar los flujos de datos entre la Unión y Estados Unidos, garantizando al tiempo un alto nivel de protección de dichos datos, conforme exige el Derecho de la Unión.

1 — Lengua original: francés.

2 — Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.» [COM(2013) 846 final].

3 — Página 2.

4 — DO L 215, p. 7, y corrección de errores en DO 2001, L 115, p. 14.

4. En efecto, recientemente determinadas revelaciones han puesto de manifiesto la existencia de programas estadounidenses de recogida de información a gran escala. Dichas revelaciones han creado confusión en relación con el respeto de las normas del Derecho de la Unión en las transferencias de datos personales a empresas ubicadas en Estados Unidos y en relación con las deficiencias del régimen de puerto seguro.

5. Mediante la presente petición de decisión prejudicial se solicita al Tribunal de Justicia que aclare qué postura deben adoptar las autoridades de control nacionales y la Comisión cuando se enfrentan a disfunciones en el marco de la aplicación de la Decisión 2000/520.

6. La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos [5] prevé, en su capítulo IV, normas relativas a la transferencia de datos personales a países terceros.

7. En dicho capítulo, el artículo 25, apartado 1, de la citada Directiva establece el principio según el cual la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente puede efectuarse cuando el país tercero de que se trate garantice un nivel de protección adecuado.

8. A sensu contrario, tal como señala el legislador de la Unión en el considerando 57 de dicha Directiva, cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales.

9. En virtud del artículo 25, apartado 2, de la Directiva 95/46, «el carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países».

10. Con arreglo al artículo 25, apartado 6, de esta misma Directiva, la Comisión podrá hacer constar que un país tercero garantiza un nivel de protección adecuado de los datos personales a la vista de su legislación interna o de sus compromisos internacionales. Desde el momento en que la Comisión adopte una Decisión en este sentido, podrá efectuarse la transferencia de datos personales al país tercero de que se trate.

11. En aplicación de dicha disposición, la Comisión adoptó la Decisión 2000/520. Del artículo 1, apartado 1, de dicha Decisión, resulta que se considerará que «los principios de puerto seguro», aplicados de conformidad con la orientación que proporcionan las «preguntas más frecuentes», [6] garantizan un nivel de protección adecuado de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos.

12. En consecuencia, la Decisión 2000/520 autoriza la transferencia de datos personales desde los Estados miembros a empresas establecidas en Estados Unidos que se han comprometido a respetar los principios de puerto seguro.

5 — DO L 281, p. 31. Directiva en su versión modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y el Consejo, de 29 de septiembre de 2003 (DO L 284, p. 1) (en lo sucesivo, «Directiva 95/46»).

6 — Frequently asked questions; en lo sucesivo, «FAQ».

13. La Decisión 2000/520 establece, en su anexo I, determinados principios a los que se pueden adherir voluntariamente las empresas, acompañados de ciertos límites y de un sistema de control específico. En 2013 eran más de 3 200 las empresas que se habían adherido a lo que puede calificarse como «código de conducta».

14. El régimen del puerto seguro se basa en una solución que combina la autocertificación y autoevaluación de las empresas privadas con la intervención del poder público.

15. Los principios de puerto seguro se formularon «en consulta con la industria y la opinión pública para facilitar el comercio y las transacciones entre Estados Unidos [...] y la Unión [...]. Son de utilización exclusiva de las entidades estadounidenses que reciben datos personales de la Unión Europea, al efecto de reunir los requisitos de "puerto seguro" y obtener la correspondiente presunción de "adecuación"». [7]

16. Los principios de puerto seguro, que figuran en el anexo I de la Decisión 2000/520, prevén, en especial:

— La obligación de notificación, según la cual las «entidades informarán a los particulares de los fines con los que cuales recogen y utilizan información sobre ellos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales se revelará la información; las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación. La notificación se hará [...] la primera vez que se invite a los particulares a proporcionar a la entidad información personal o, posteriormente, tan pronto como sea posible, pero en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que la transfiere o la divulga por primera vez a un tercero». [8]

— La obligación de las entidades de ofrecer a los particulares la posibilidad de decidir si su información personal puede divulgarse a un tercero o bien puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o que no haya sido autorizado posteriormente por el particular. Si se trata de información delicada, «la opción de participar será afirmativa o explícita (aceptación) si la información va a revelarse a un tercero o a utilizarse para un fin distinto del que inicialmente motivó la recogida de información o de una manera distinta a la autorizada con posterioridad por éste al optar por la "aceptación"». [9]

— Normas relativas a la transferencia ulterior de los datos. Así, para revelar información a terceros, las entidades deberán aplicar los principios de notificación y opción. [10]

— En cuanto a la seguridad de los datos, la obligación de que «las entidades que creen, mantengan, utilicen o difundan información personal tom[en] precauciones razonables para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, su modificación y su destrucción». [11]

— En lo que atañe a la integridad de la información, la obligación de que las entidades, «[...] adopt[en] medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales». [12]

7 — Párrafo segundo del anexo I de la Decisión 2000/520.

8 — Véase el anexo I, bajo el título «Notificación».

9 — Véase el anexo I, bajo el título «Opción».

10 — Véase el anexo I, bajo el título «Transferencia ulterior».

11 — Véase el anexo I, bajo el título «Seguridad».

12 — Véase el anexo I, bajo el título «Integridad de los datos».

— Que las entidades que tengan información privada de personas físicas deberán dar en principio a dichas personas «acceso a la información personal [y permitirles] corregir, modificar o suprimir dicha información si resultase inexacta»; [13]

— La obligación de prever «mecanismos para garantizar la conformidad con los principios [de puerto seguro], una vía de recurso para las personas a que se refieran los datos y se vean afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora». [14]

17. Toda entidad estadounidense que desee adherirse a los principios de puerto seguro estará obligada a indicar, en su política de protección de la vida privada, que manifiesta públicamente que se adhiere a dichos principios y que los cumple, y a autocertificar su adhesión a los principios mediante la notificación al Departamento de Comercio de Estados Unidos del compromiso de cumplirlos. [15]

18. Las entidades disponen de diversos medios para cumplir los principios de puerto seguro. En este sentido, pueden, por ejemplo, «[integrarse] en un programa autorregulado de protección de la vida privada que siga los principios mencionados» o reunir las condiciones de puerto seguro «elaborando sus propias medidas autorreguladoras de protección de la vida privada siempre que se adecuen a dichos principios». «Además, las entidades sujetas a disposiciones de naturaleza legal, reglamentaria, administrativa u otra (o a reglamentaciones), que protejan con eficacia el secreto de los datos personales, podrán acogerse también a los beneficios del puerto seguro». [16]

19. Existen diversos mecanismos, que combinan el arbitraje privado y la supervisión de las autoridades públicas, para comprobar que se respetan los principios de puerto seguro. En este sentido, puede llevar a cabo el control de dicho cumplimiento un tercero independiente a través de un sistema de resolución extrajudicial de controversias. Además, las entidades pueden comprometerse a cooperar con el grupo de expertos de la Unión Europea en protección de datos. Por último, la Federal Trade Commission (Comisión Federal del Comercio; en lo sucesivo, «FTC»), en virtud de la competencia que le confiere el artículo 5 de la Ley relativa a la Comisión Federal del Comercio Federal (Trade Commission Act), y el Department of Transportation (Departamento de Transporte), en virtud de la competencia que le confiere el artículo 41712 del Código de Estados Unidos de América (United States Code) que figura en su título 49, son competentes para tramitar denuncias.

20. Con arreglo al párrafo cuarto del anexo I de la Decisión 2000/520, la adhesión a los principios de puerto seguro puede, no obstante, limitarse, en particular, «cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley» y por «disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones». [17]

21. Por otro lado, la facultad de las autoridades competentes de los Estados miembros de suspender los flujos de datos está sujeta a varios requisitos previstos en el artículo 3, apartado 1, de la Decisión 2000/520.

22. La presente petición de decisión prejudicial lleva a plantearse cuál es el alcance de la Decisión 2005/520 a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), y de los artículos 25, apartado 6, y 28 de la Directiva 95/46. La presente petición se plantea en el marco de un litigio entre el Sr. Schrems y el Data Protection

13 — Véase el anexo I, bajo el título «Acceso».

14 — Véase el anexo I, bajo el título «Aplicación».

15 — Artículo 1, apartados 2 y 3, de la Decisión 2000/520. Véase, asimismo, el anexo II, FAQ 6.

16 — Párrafo tercero del anexo I.

17 — Véase, asimismo, el anexo IV B.

Commissioner (comisario para la protección de datos; en lo sucesivo, «comisario») que tiene por objeto la negativa de este último a abrir la instrucción de una denuncia interpuesta por el Sr. Schrems basada en que Facebook Ireland Ltd. (en lo sucesivo, «Facebook Ireland») almacena los datos personales de sus usuarios en servidores situados en Estados Unidos.

23. El Sr. Schrems es ciudadano austriaco y reside en Austria. Es usuario de la red social Facebook desde 2008.

24. A todos los usuarios de Facebook que residen en el territorio de la Unión se les solicita que firmen un contrato con Facebook Ireland, filial de la sociedad matriz Facebook Inc., establecida en Estados Unidos (en lo sucesivo, «Facebook USA»). La totalidad o parte de los datos de los usuarios de Facebook Ireland residentes en la Unión son transferidos a los servidores de Facebook USA, ubicados físicamente en Estados Unidos, en los que se almacenan.

25. El 25 de junio de 2013, el Sr. Schrems presentó una denuncia ante el comisario en la que alegaba, en esencia, que la legislación y la práctica estadounidenses no ofrecen protección real alguna a los datos almacenados en el territorio de Estados Unidos en cuanto atañe a la supervisión estatal. Ello resulta de las revelaciones efectuadas a partir de mayo de 2013 por Edward Snowden sobre las actividades de los servicios de inteligencia estadounidenses y, en particular, de la National Security Agency (Agencia de Seguridad Nacional estadounidense; en lo sucesivo, «NSA»).

26. En particular, de dichas revelaciones se desprende que la NSA creó un programa denominado «PRISM» en el marco del cual dicha agencia obtuvo libre acceso a los datos almacenados en masa en servidores situados en Estados Unidos, de titularidad o sujetos al control de una serie de empresas que operan en el ámbito de Internet y de la tecnología, como Facebook USA.

27. El comisario estimó que no estaba obligado a abrir la instrucción de la denuncia, ya que ésta carecía de fundamento jurídico. Consideró que no había pruebas de que la NSA hubiera accedido a los datos personales del Sr. Schrems. Además, en su opinión, procedía archivar la denuncia a raíz de la Decisión 2000/520 mediante la cual la Comisión hizo constar que Estados Unidos garantiza, en el marco del régimen de puerto seguro, un nivel de protección adecuado a los datos personales transmitidos. Toda cuestión de la adecuación de la protección de datos en Estados Unidos debe determinarse de conformidad con dicha Decisión, que le impide examinar el problema que plantea la denuncia.

28. La legislación nacional que llevó al comisario a desestimar la reclamación es la siguiente.

29. El artículo 10, apartado 1, de la Ley de protección de datos (Data Protection Act) de 1988, en su versión modificada por la Data Protection (Amendment) Act de 2003 (en lo sucesivo, «Ley de protección de datos») confiere a dicho comisario competencias para examinar las denuncias y establece:

«a) El comisario podrá examinar o disponer que se examine si se han vulnerado, siguen vulnerándose o eventualmente podrían vulnerarse las disposiciones de la presente ley en nombre de cualquier persona, bien mediando denuncia del interesado ante el comisario relativa a la vulneración de una de sus disposiciones, bien cuando el comisario estime de oficio que tal infracción se está produciendo.

b) Cuando una persona presente una denuncia ante el comisario en virtud de la letra a) del presente apartado, el comisario:

i) instruirá o solicitará que se instruya la denuncia, a no ser que ésta sea insustancial o temeraria, y

ii) si, transcurrido un plazo razonable, no logra que las partes afectadas alcancen un acuerdo amistoso en relación con el objeto de la denuncia, notificará por escrito al denunciante la resolución que haya adoptado, informándole de que, de resultarle perjudicial, puede interponer recurso contra ella en virtud del artículo 26 de la presente Ley, en el plazo de 21 días a contar desde la recepción de la notificación».

30. En el caso de autos, el comisario concluyó que la denuncia del Sr. Schrems era «insustancial o temeraria» en el sentido de que estaba abocada al fracaso por cuanto carecía de fundamento jurídico. En tal motivo basó su negativa a investigar la denuncia.

31. El artículo 11 de la Ley de protección de datos regula la transferencia de datos personales fuera del territorio nacional. El artículo 11, apartado 2, letra a), de dicha Ley, dispone:

«Siempre que, en el marco de cualquier procedimiento regulado por la presente Ley:

i) deba determinarse si un país o territorio situado fuera del Espacio Económico Europeo [(EEE)] al que vayan a transferirse datos personales garantiza el nivel de protección adecuado indicado en el apartado 1 del presente artículo, y

ii) la Unión haya formulado una constatación con respecto al tipo de transmisión de que se trate,

la cuestión se resolverá de conformidad con dicha constatación».

32. El artículo 11, apartado 2, letra b), de la Ley de protección de datos define el concepto de constatación de la Unión de la siguiente manera:

«En la letra a) del presente apartado, se entenderá por "constatación de la Unión" toda constatación formulada por la Comisión [...] a efectos de los apartados 4 o 6 del artículo 25 de la Directiva [95/46], en el marco del procedimiento previsto en el artículo 31, apartado 2, de [dicha Directiva] con el fin de determinar si un país o territorio situado fuera del [EEE] garantiza el nivel de protección adecuado indicado en el apartado 1 del presente artículo».

33. El comisario señaló que la Decisión 2000/520 constituye una «constatación de la Unión» en el sentido del artículo 11, apartado 2, letra a), de la Ley de 1988, de modo que toda cuestión relativa a la adecuación de la protección de datos en el tercer país al que se transfieran los datos debe resolverse de conformidad con dicha constatación. Dado que dicha circunstancia constituía el fundamento de la reclamación del Sr. Schrems, a saber, que se estaban transfiriendo datos personales a un tercer país que no ofrecía en la práctica un nivel de protección adecuado, el comisario consideró que tanto la naturaleza como la propia existencia de la Decisión 2000/520 le impedían examinar dicha cuestión.

34. El Sr. Schrems interpuso un recurso ante la High Court contra la decisión del comisario de archivar su denuncia. Tras haber examinado las pruebas aportadas en el procedimiento principal, dicho órgano jurisdiccional constató que la vigilancia electrónica y la interceptación de datos personales responden a finalidades necesarias e indispensables para el interés público, a saber, el mantenimiento de la seguridad nacional y la prevención de delitos graves. La High Court observó, a este respecto, que la vigilancia e interceptación de los datos personales transferidos desde la Unión a Estados Unidos sirven a objetivos legítimos relacionados con la lucha contra el terrorismo.

35. Según dicho órgano jurisdiccional, las revelaciones efectuadas por el Sr. Snowden demostraron, sin embargo, que la NSA y otros organismos similares habían cometido excesos considerables. Si bien la Foreign Intelligence Surveillance Court (en lo sucesivo, «FISC»), que interviene en el marco de la Ley relativa a la vigilancia de los servicios de inteligencia extranjeros de 1978 (Foreign Intelligence

Surveillance Act),[18] lleva a cabo tareas de supervisión, el procedimiento que se sustancia ante dicho órgano es secreto y no contradictorio. Por otro lado, al margen de que las decisiones relativas al acceso a los datos personales deberían adoptarse sobre la base del Derecho estadounidense, los ciudadanos de la Unión no tendrían ningún derecho a ser oídos en relación con la cuestión de la supervisión y la interceptación de sus datos.

36. De los voluminosos documentos que acompañan a las declaraciones juradas efectuadas en el procedimiento principal se desprende que no se ha cuestionado la exactitud de buena parte de las revelaciones del Sr. Snowden. Por consiguiente, la High Court concluyó que una vez que se transfieren datos personales a Estados Unidos, la NSA y otras agencias de seguridad estadounidenses, tales como el Federal Bureau of Investigation (FBI), pueden acceder a dichos datos en el marco de una vigilancia e interceptación masivas indiscriminadas.

37. La High Court observa que, en Derecho irlandés, la importancia de los derechos constitucionales a la vida privada y a la inviolabilidad del domicilio exige que toda injerencia en dichos derechos sea proporcionada y se lleve a cabo conforme a los requisitos establecidos por la ley. El acceso masivo e indiscriminado a datos personales no se ajusta en modo alguno al principio de proporcionalidad y, por tanto, debe ser considerado contrario a la Constitución irlandesa.[19]

38. La High Court señala que, para que las interceptaciones de comunicaciones electrónicas sean consideradas constitucionalmente válidas, es necesario demostrar que determinadas interceptaciones de las comunicaciones y la vigilancia de determinadas personas o grupos de personas están objetivamente justificadas en aras de la seguridad nacional y de la eliminación de la delincuencia y que tales interceptaciones se efectúan con garantías adecuadas y comprobables.

39. Por consiguiente, la High Court indica que, si el caso de autos debiera analizarse exclusivamente a la luz del Derecho irlandés, se plantearía un problema de considerable envergadura en lo que concierne a la cuestión de si Estados Unidos «ofrece un nivel de protección adecuado de la intimidad y de los derechos y libertades fundamentales de las personas», en el sentido del artículo 11, apartado 1, de la Ley de protección de datos. De ello se desprende que, con arreglo al Derecho irlandés y, en particular, a sus criterios constitucionales, el comisario no habría podido archivar la denuncia del Sr. Schrems, sino que tendría que haberla examinado.

40. Sin embargo, la High Court constata que el asunto de que conoce versa sobre la aplicación del Derecho de la Unión en el sentido del artículo 51, apartado 1, de la Carta, de manera que la legalidad de la decisión del comisario debe apreciarse con arreglo al Derecho de la Unión.

41. La High Court explica el problema al que se enfrentó el comisario de la manera que se expone a continuación. En virtud del artículo 11, apartado 2, letra a), de la Ley de protección de datos, el comisario debe zanjar la cuestión de la adecuación de la protección en el tercer país «de conformidad» con una constatación de la Unión efectuada por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46. De ello se desprende que el comisario no puede hacer caso omiso de dicha constatación. Dado que la Comisión, en su Decisión 2000/520, constató que Estados Unidos ofrece un nivel de protección adecuado en lo que respecta al tratamiento de datos por las empresas adheridas a los principios de puerto seguro, el comisario debía necesariamente archivar una denuncia en la que se alega que el nivel de protección es inadecuado.

18 — Véase el artículo 702 de dicha Ley, en su versión modificada por la Ley de 2008 (Foreign Intelligence Surveillance Act of 2008). En virtud de dicho artículo la NSA posee una base de datos conocida con el nombre de «PRISM» (véase el «Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection», de 27 de noviembre de 2013).

19 — La High Court hace referencia, en particular, al respeto de la dignidad humana y de la libertad de la persona (Preámbulo de la Constitución); a la autonomía personal (artículo 40, apartado 3, puntos 1 y 2); a la inviolabilidad del domicilio (artículo 40, apartado 5) y a la protección de la vida familiar (artículo 41).

42. Si bien la High Court constata que el comisario se atuvo escrupulosamente al tenor de la Directiva 95/46 y la Decisión 2000/520, señala que, en realidad, el Sr. Schrems censura más los términos del propio régimen de puerto seguro que el modo en que el comisario lo aplicó, al tiempo que recalca que el demandante no impugnó directamente la validez de la Directiva 95/46 ni de la Decisión 2000/520.

43. Según la High Court, la cuestión esencial radica por tanto en si, desde el punto de vista del Derecho de la Unión y habida cuenta, en particular, de la posterior entrada en vigor de los artículos 7 y 8 de la Carta, el comisario está vinculado en términos absolutos por la constatación de la Comisión contenida en la Decisión 2000/520 en relación al carácter adecuado de la normativa y prácticas estadounidenses en materia de protección de datos.

44. La High Court precisa, además, que en el recurso de que conoce, no se formula imputación alguna en relación con las actuaciones de Facebook Ireland ni de Facebook USA en cuanto tales. Pues bien, dicho órgano jurisdiccional considera que el artículo 3, apartado 1, letra b), de la Decisión 2000/520, que permite a las autoridades nacionales competentes ordenar a cualquier entidad que suspenda el flujo de datos hacia el país tercero, sólo es aplicable en caso de que la denuncia se dirija contra la conducta de la empresa de que se trate, lo que no ocurre en el caso de autos.

45. La High Court recalca, por tanto, que no se censura realmente la conducta de Facebook USA en sí, sino más bien que la Comisión haya considerado que la legislación y la práctica estadounidenses en materia de protección de datos ofrecen una protección adecuada, pese a que las revelaciones del Sr. Snowden ponen claramente de manifiesto que las autoridades estadounidenses pueden acceder de un modo masivo e indiferenciado a datos personales de la población residente en territorio de la Unión. [20]

46. En este sentido, la High Court estima que es dudoso que la Decisión 2000/520 cumpla, en la práctica, los requisitos previstos en los artículos 7 y 8 de la Carta, sobre todo a la luz de los principios formulados por el Tribunal de Justicia en su sentencia Digital Rights Ireland y otros. [21] En particular, la garantía consagrada en el artículo 7 de la Carta y que emana de los valores fundamentales presentes en las tradiciones constitucionales comunes a los Estados miembros se vería comprometida si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada sin necesidad de aportar una motivación objetiva basada en razones de seguridad nacional o de prevención del delito vinculadas específicamente a las personas afectadas y sin ninguna garantía adecuada y comprobable. Así, como el recurso del Sr. Schrems sugiere que la Decisión 2000/520 puede *in abstracto* ser incompatible con los artículos 7 y 8 de la Carta, el Tribunal de Justicia podría considerar que cabe interpretar la Directiva 95/46, y en particular su artículo 25, apartado 6, así como la Decisión 2000/520, en el sentido de que permiten a las autoridades nacionales llevar a cabo sus propias investigaciones con el fin de determinar si la transmisión de datos personales a un tercer país cumple los requisitos que se derivan de los artículos 7 y 8 de la Carta.

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

«1) En el marco de la resolución de una reclamación presentada ante el comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, Estados Unidos) cuya legislación y práctica no prevén una protección adecuada de la persona sobre la que versan los datos, ¿está vinculado dicho comisario en términos absolutos por la declaración

20 — La High Court indica, a este respecto, que el principal motivo de recurso invocado por el Sr. Schrems consiste en que, a la luz de las recientes revelaciones del Sr. Snowden y del hecho de que se han suministrado datos personales a los servicios de inteligencia estadounidenses a gran escala, el comisario no podía concluir que en Estados Unidos existe un nivel adecuado de protección.

21 — C-293/12 y C-594/12, EU:C:2014:238, apartados 65 a 69.

comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?

2) En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520?»

II. **Análisis**

48. Mediante las dos cuestiones prejudiciales planteadas, la High Court solicita al Tribunal de Justicia que precise cuáles son las facultades que tienen atribuidas las autoridades de control nacionales en el marco de la resolución de una denuncia relativa a una transferencia de datos de carácter personal a una empresa establecida en un tercer país en la que se alega como fundamento que dicho tercer país no ofrece una protección adecuada a los datos transmitidos, aun cuando la Comisión haya adoptado, sobre la base del artículo 25, apartado 6, de la Directiva 95/46, una decisión en la que reconoce que dicho tercer país garantiza un nivel de protección adecuado.

49. Cabe observar que la denuncia del Sr. Schrems ante el comisario encierra una doble dimensión. Por un lado, censura la transferencia de datos de carácter personal efectuada de Facebook Ireland a Facebook USA. El Sr. Schrems solicita que se ponga fin a dicha transferencia en la medida en que, en su opinión, Estados Unidos no ofrece un nivel de protección adecuado de los datos de carácter personal que se transfieren en el marco del régimen de puerto seguro. Más concretamente, reprocha a dicho país tercero que haya creado el programa PRISM que permite a la NSA acceder libremente a los datos almacenados en masa en servidores situados en Estados Unidos. En este sentido, la denuncia versa específicamente sobre las transferencias de datos personales de Facebook Ireland a Facebook USA, al tiempo que cuestiona en términos más generales el nivel de protección garantizado con respecto a tales datos en el marco del régimen de puerto seguro.

50. El comisario consideró que la misma existencia de una decisión de la Comisión por la que se declara que Estados Unidos ofrece, en el marco del régimen de puerto seguro, un nivel de protección adecuado, le impedía investigar dicha denuncia.

51. Por consiguiente, conviene examinar conjuntamente las dos cuestiones mediante las que se pretende, en sustancia, determinar si el artículo 28 de la Directiva 95/46, a la luz de los artículos 7 y 8 de la Carta, debe interpretarse en el sentido de que la existencia de una decisión adoptada por la Comisión en virtud del artículo 25, apartado 6, de dicha Directiva, tiene por efecto impedir que una autoridad de control nacional investigue una denuncia en la que se alega que un país tercero no ofrece un nivel de protección adecuado para los datos de carácter personal transferidos y, en su caso, suspenda la transmisión de dichos datos.

52. El artículo 7 de la Carta garantiza el derecho al respeto de la vida privada, mientras que su artículo 8 proclama expresamente el derecho a la protección de los datos personales. Los apartados 2 y 3 de este último artículo precisan que dichos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley, que toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación, y que el respeto de estas normas estará sujeto al control de una autoridad independiente.

A. *Sobre las facultades de las autoridades de control nacionales en caso de existencia de una decisión de adecuación de la Comisión*

53. Como indica el Sr. Schrems en sus observaciones, a efectos de la denuncia objeto del litigio principal, la cuestión fundamental es la transferencia de datos personales de Facebook Ireland a Facebook USA a la luz del acceso generalizado por parte de la NSA y otras agencias de seguridad estadounidenses a los datos almacenados en Facebook USA en virtud de las facultades que les confiere la legislación estadounidense.

54. Según el Sr. Schrems, la autoridad de control nacional que conozca de una denuncia en la que se cuestione la constatación de que un país tercero ofrece un nivel de protección adecuado de los datos transferidos, y que disponga de elementos probatorios del carácter fundado de las alegaciones formuladas en dicha denuncia, tiene la facultad de ordenar la suspensión de la transferencia de datos llevada a cabo por la empresa designada en la referida denuncia.

55. Habida cuenta de la obligación del comisario de proteger los derechos fundamentales del Sr. Schrems, este último sostiene que el comisario no sólo tiene la obligación de iniciar una investigación, sino que, en caso de admitirse una denuncia, también debe ejercitar sus facultades para suspender el flujo de datos entre Facebook Ireland y Facebook USA.

56. Pues bien, el comisario archivó la denuncia sobre la base de las disposiciones contenidas en la Ley de protección de datos que enumeran sus facultades. Dicha conclusión se basa en la opinión del comisario de que está vinculado por la Decisión 2000/520.

57. De ello se desprende que el núcleo principal del presente asunto consiste en determinar si la apreciación de la Comisión sobre la adecuación del nivel de protección manifestada en la Decisión 2000/520 es vinculante en términos absolutos para la autoridad nacional de protección de datos y le impide investigar las alegaciones que pongan en duda dicha apreciación. Por consiguiente, mediante las cuestiones prejudiciales se pretende que se dilucide el alcance de las facultades de investigación de las autoridades nacionales de protección de datos en caso de existir una decisión de adecuación de la Comisión.

58. Según la Comisión, es importante tener en cuenta la articulación entre las facultades respectivas de ésta y de las autoridades nacionales de protección de datos. Las competencias de estas últimas se centran en la aplicación de la legislación en esta materia a casos concretos, mientras que la Comisión es competente para revisar con carácter general la aplicación de la Decisión 2000/520, incluida toda decisión que implique su suspensión o derogación.

59. La Comisión alega que el Sr. Schrems no ha formulado ninguna alegación concreta que sugiera que corría el riesgo inminente de sufrir daños graves a raíz de la transferencia de datos entre Facebook Ireland y Facebook USA. Al contrario, por su naturaleza abstracta y general, la preocupación manifestada por el Sr. Schrems sobre los programas de vigilancia establecidos por las agencias de seguridad estadounidenses es idéntica a las que llevó a la Comisión a iniciar la revisión de la Decisión 2000/520.

60. Según la Comisión, las autoridades de control nacionales interferirían en las competencias que le han sido conferidas para renegociar las condiciones de dicha Decisión con Estados Unidos o, en su caso, suspender sus efectos, si adoptasen medidas sobre la base de denuncias en las que sólo se manifiestan preocupaciones estructurales y abstractas.

61. No comparto la opinión de la Comisión. A mi parecer, la existencia de una decisión adoptada por la Comisión sobre la base del artículo 25, apartado 6, de la Directiva 95/46 no puede anular, ni siquiera mermar, las facultades de que disponen las autoridades de control nacionales en virtud del artículo 28 de dicha Directiva. A diferencia de lo que afirma la Comisión, considero que nada obsta a que las

autoridades de control nacionales que conozcan de denuncias individuales, en virtud de sus facultades en materia de investigación y de su independencia, lleguen a sus propias conclusiones sobre el nivel de protección general ofrecido por un tercer país y extraigan las consecuencias que se derivan de dichas conclusiones en sus decisiones sobre casos individuales.

62. Según reiterada jurisprudencia del Tribunal de Justicia, para interpretar una disposición de Derecho de la Unión procede tener en cuenta, no sólo su tenor literal, sino también su contexto y los objetivos perseguidos por la normativa de la que forma parte. [22]

63. Del considerando 62 de la Directiva 95/46 se desprende que «la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales».

64. Con arreglo al artículo 28, apartado 1, párrafo primero, de dicha Directiva, «los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva». Dicha Directiva, en su artículo 28, apartado 1, párrafo segundo, establece que «estas autoridades ejercerán las funciones que les son atribuidas con total independencia».

65. El artículo 28, apartado 3, de la Directiva 95/46 enumera las facultades de cada autoridad de control, a saber, poderes de investigación, poderes efectivos de intervención que les permiten, en especial, prohibir provisional o definitivamente un tratamiento, y capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de dicha Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

66. Además, en virtud del artículo 28, apartado 4, párrafo primero, de la Directiva 95/46, «toda autoridad de control entenderá de las solicitudes que cualquier persona [...] le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales». El artículo 28, apartado 4, párrafo segundo, de dicha Directiva precisa que «toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de [la citada] Directiva». Cabe precisar que esta última disposición permite a los Estados miembros adoptar medidas legales para limitar el alcance de diversas obligaciones y derechos previstos en la Directiva 95/46, siempre que dicha limitación constituya una medida necesaria, especialmente por motivos de seguridad del Estado, defensa, seguridad pública y prevención, investigación, detección y represión de infracciones penales.

67. Como ya ha señalado el Tribunal de Justicia, el requisito de someter el respeto de las disposiciones del Derecho de la Unión relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales al control de una autoridad independiente, resulta asimismo del Derecho primario de la Unión, en particular, del artículo 8, apartado 3, de la Carta, y del artículo 16 TFUE, apartado 2. [23] Asimismo, el Tribunal de Justicia ha recordado que «la creación en los Estados miembros de autoridades de control independientes constituye [...] un elemento esencial del respeto a la protección de las personas en lo que respecta al tratamiento de datos personales». [24]

22 — Véase, en especial, la sentencia Koushkaki (C-84/12, EU:C:2013:862), apartado 34 y jurisprudencia citada.

23 — Véanse las sentencias Comisión/Austria (C-614/10, EU:C:2012:631), apartado 36 y Comisión/Hungría (C-288/12, EU:C:2014:237), apartado 47.

24 — Véase, en especial, la sentencia Comisión/Hungría (C-282/12, EU:C:2014:237), apartado 48 y jurisprudencia citada. Véase también, en el mismo sentido, la sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), apartado 68 y jurisprudencia citada.

68. Por otro lado, el Tribunal de Justicia ha estimado que «el artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46 debe interpretarse en el sentido de que las autoridades de control competentes para vigilar el tratamiento de datos personales han de disfrutar de la independencia que les permita ejercer sus funciones sin influencia externa. Esta independencia en particular excluye toda orden o influencia externa con independencia de la forma que revista, directa o indirecta, que pudiera orientar sus decisiones y, en consecuencia, poner en peligro el cumplimiento de la tarea que corresponde a dichas autoridades de establecer un justo equilibrio entre la protección del derecho a la intimidad y la libre circulación de datos personales». [25]

69. El Tribunal de Justicia ha precisado asimismo que «la garantía de independencia de las autoridades de control nacionales trata de asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales». [26] Dicha garantía de independencia se ha establecido «para reforzar la protección de las personas y de los organismos afectados por [las] decisiones [de dichas autoridades de control nacionales]». [27]

70. Conforme se desprende, en particular, del considerando 10 y del artículo 1 de la Directiva 95/46, ésta tiene por objeto asegurar en el seno de la Unión «un alto nivel de protección de las libertades y derechos fundamentales en lo que respecta al tratamiento de datos personales». [28] Según el Tribunal de Justicia, «las autoridades de control previstas en el artículo 28 de la Directiva 95/46 son las guardianas de los mencionados derechos y libertades fundamentales». [29]

71. Habida cuenta de la importancia del papel que desempeñan las autoridades de control nacionales en materia de protección de las personas físicas en lo que respecta al tratamiento de datos personales, sus facultades de intervención deben permanecer íntegras aun cuando la Comisión haya adoptado una decisión sobre la base del artículo 25, apartado 6, de la Directiva 95/46.

72. A este respecto, cabe señalar que nada indica que los regímenes de transferencia de datos personales a terceros países estén excluidos del ámbito de aplicación material del artículo 8, apartado 3, de la Carta, que consagra al más alto nivel de la jerarquía normativa en Derecho de la Unión la importancia del control ejercido por una autoridad independiente del respeto de la normativa relativa a la protección de datos personales.

73. Si las autoridades de control nacionales estuvieran vinculadas en términos absolutos por las decisiones adoptadas por la Comisión, su total independencia se vería inevitablemente cercenada. Por su papel de guardianas de los derechos fundamentales, las autoridades de control nacionales deben poder investigar, con total independencia, las reclamaciones que se les presenten, en aras del interés superior de la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

74. Además, como señalaron acertadamente el Gobierno belga y el Parlamento Europeo en la vista, no existe ningún vínculo jerárquico entre el capítulo IV de la Directiva 95/46, relativo a la transferencia de datos personales a países terceros, y el capítulo VI de dicha Directiva, consagrado, en particular, a la función que desempeñan las autoridades de control nacionales. En dicho capítulo VI no hay nada que sugiera que las disposiciones relativas a las autoridades de control nacionales estén de alguna manera subordinadas a las disposiciones de otro tipo relativas a las transferencias de datos recogidas en el capítulo IV de la Directiva 95/46.

25 — Véase, en especial, la sentencia Comisión/Hungría (C-288/12, EU:C:2014:237), apartado 51 y jurisprudencia citada.

26 — Sentencia Comisión/Alemania (C-518/07, EU:C:2010:125), apartado 25.

27 — *Ibídem.*

28 — *Ibídem*, apartado 22 y jurisprudencia citada.

29 — *Ibídem*, apartado 23. Véanse también, en este sentido, las sentencias Comisión/Austria (C-614/10, EU:C:2012:631), apartado 52, y Comisión/Hungría (C-288/12, EU:C:2014:237), apartado 53.

75. Al contrario, se desprende expresamente del artículo 25, apartado 1, de dicha Directiva, contenido en su capítulo IV, que la autorización de la transferencia de datos personales a un país tercero que garantice un nivel de protección adecuado únicamente podrá efectuarse en cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás normas de dicha Directiva.

76. A este respecto, procede recordar que, en virtud de dicha disposición, los Estados miembros deben prever en su legislación nacional que la transferencia a un tercer país de datos personales objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente puede efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la Directiva 95/46, el país tercero de que se trate garantice un nivel de protección adecuado.

77. De conformidad con el artículo 28, apartado 1, de dicha Directiva, las autoridades de control nacionales se encargan de vigilar la aplicación en el territorio de los Estados miembros de las disposiciones adoptadas por ellos en aplicación de la citada Directiva.

78. La proximidad de estas dos disposiciones permite considerar que la regla enunciada en el artículo 25, apartado 1, de la Directiva 95/46, según la cual la transferencia de datos personales únicamente puede efectuarse si el país tercero destinatario garantiza un nivel de protección adecuado, forma parte de las normas cuyo cumplimiento deben supervisar las autoridades de control nacionales.

79. Resulta conveniente interpretar en sentido amplio, de conformidad con el artículo 8, apartado 3, de la Carta, los poderes de las autoridades de control nacionales para investigar, con total independencia, las reclamaciones de que conozcan en virtud del artículo 28 de la Directiva 95/46. Por consiguiente, dichos poderes no pueden verse mermados por los poderes conferidos por el legislador de la Unión a la Comisión, en virtud del artículo 25, apartado 6, de la citada Directiva, para hacer constar el carácter adecuado del nivel de protección ofrecido por un país tercero.

80. Habida cuenta de su papel fundamental en materia de protección de datos personales, las autoridades de control nacionales deben poder abrir una investigación cuando se les presenten reclamaciones en las que se aporten elementos que permitan poner en duda el nivel de protección garantizado por un país tercero, incluso cuando la Comisión haya declarado, en una decisión adoptada sobre la base del artículo 25, apartado 6, de la Directiva 95/46, que el país tercero de que se trate garantiza un nivel de protección adecuado.

81. Si, tras finalizar sus investigaciones, la autoridad de control nacional considera que la transferencia de datos impugnada socava la protección que debe garantizarse a los ciudadanos de la Unión en relación con el tratamiento de sus datos personales, podrá suspender la transferencia de datos controvertida, con independencia de la evaluación general que haya realizado la Comisión en su decisión.

82. En efecto, no se discute que, en virtud del artículo 25, apartado 2, de la Directiva 95/46, el carácter adecuado del nivel de protección que ofrece un país tercero se evalúa atendiendo a todas las circunstancias concurrentes, tanto de hecho como de Derecho. Si una de dichas circunstancias cambia, de manera que pueda quedar en entredicho el carácter adecuado del nivel de protección que ofrece un país tercero, la autoridad de control nacional que conozca de una denuncia debe poder extraer las consecuencias que proceda en relación con la transferencia impugnada.

83. Ciertamente, como señaló Irlanda, el comisario, al igual que las demás autoridades estatales, está vinculado por la Decisión 2000/520. En efecto, resulta del artículo 288 TFUE, párrafo cuarto, que toda decisión adoptada por una institución de la Unión será obligatoria en todos sus elementos. Por consiguiente, la Decisión 2000/520 es vinculante para los Estados miembros, destinatarios de la misma.

84. A este respecto, cabe señalar que la propia Decisión 2000/520 dispone, en su artículo 5, que «los Estados miembros adoptarán todas las medidas necesarias para cumplir[la], a más tardar en un plazo de noventa días a partir de la fecha de su notificación a los Estados miembros». Además, el artículo 6 de dicha Decisión confirma que «los destinatarios de [ésta] serán los Estados miembros».

85. Sin embargo, considero que, habida cuenta de las disposiciones anteriormente referidas de la Directiva 95/46 y de la Carta, el efecto imperativo de la Decisión 2000/520 no impide que el comisario pueda investigar denuncias en las que se alegue que determinadas transferencias de datos de carácter personal efectuadas a Estados Unidos en el marco de dicha Decisión no presentan las garantías necesarias de protección exigidas por el Derecho de la Unión. En otras palabras, dicho efecto vinculante no exige que deban archivarse de forma sumaria todas las denuncias de ese tipo, es decir, inmediatamente y sin apreciar su fundamento.

86. Cabe añadir que se desprende, asimismo, de la sistemática del artículo 25 de la Directiva 95/46 que la declaración según la cual un país tercero garantiza o no un nivel de protección adecuado puede efectuarse o bien por los Estados miembros, o bien por la Comisión. Por consiguiente, se trata de una facultad compartida.

87. Del artículo 25, apartado 6, de dicha Directiva resulta que desde el momento en que la Comisión hace constar que un país tercero garantiza un nivel de protección adecuado, en el sentido del artículo 25, apartado 2, de dicha Directiva, los Estados miembros deben adoptar las medidas necesarias para ajustarse a la decisión de la Comisión.

88. Dado que dicha decisión tiene por efecto permitir las transferencias de datos personales a un país tercero que, según la Comisión, garantiza un nivel de protección adecuado, los Estados miembros deben, en principio, permitir que las empresas establecidas en su territorio transfieran datos a dicho país.

89. No obstante, el artículo 25 de la Directiva 95/46 no confiere en exclusiva a la Comisión la facultad de constatar la adecuación o no del nivel de protección de los datos de carácter personal transferidos. La estructura de dicho artículo pone de manifiesto que los Estados miembros también desempeñan su función en esta materia. Es evidente que las decisiones de la Comisión cumplen una función importante en aras de la uniformidad de los requisitos de transferencia válidos dentro de los Estados miembros. Sin embargo, dicha uniformidad sólo existe en tanto no se cuestione dicha constatación.

90. En mi opinión, el argumento de la necesidad de uniformar los requisitos de transferencia de datos personales a un país tercero halla su límite en una situación como la controvertida en el procedimiento principal, en la que no sólo la Comisión tiene conocimiento de que su constatación es objeto de críticas, sino que además ella misma formula críticas y entabla negociaciones para subsanarlas.

91. La evaluación del carácter adecuado o no del nivel de protección que ofrece un país tercero puede dar lugar también a una relación de cooperación entre los Estados miembros y la Comisión. El artículo 25, apartado 3, de la Directiva 95/46 prevé, a este respecto, que «los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2». Como observa el Parlamento, ello es sin duda indicativo de que los Estados miembros y la Comisión desempeñan una función equivalente a la hora de detectar los casos en los que un país tercero no garantiza un nivel de protección adecuado.

92. La decisión de adecuación tiene por objeto autorizar la transferencia de datos personales al país tercero de que se trata. Ello no entraña que los ciudadanos de la Unión ya no puedan presentar ante las autoridades de control solicitudes de protección de sus datos personales. A este respecto, cabe señalar que el artículo 28, apartado 4, párrafo primero, de la Directiva 95/46, según el cual «toda

autoridad de control entenderá de las solicitudes que cualquier persona [...] le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales», no prevé ninguna excepción a este principio para el caso de que la Comisión haya adoptado una decisión al amparo del artículo 25, apartado 6, de dicha Directiva.

93. En este sentido, si bien una decisión adoptada por la Comisión en virtud de los poderes de ejecución que le confiere dicha disposición tiene por efecto permitir la transferencia de datos personales a un país tercero, dicha decisión no puede, en cambio, tener por efecto arrebatar todo poder a los Estados miembros y en particular a sus autoridades de control nacionales, o incluso limitar sus competencias, cuando se invoquen ante ellas supuestas violaciones de derechos fundamentales.

94. Toda autoridad de control nacional debe poder ejercitar las facultades previstas en el artículo 28, apartado 3, de la Directiva 95/46, entre ellas, la de prohibir provisional o definitivamente un tratamiento de datos personales. Aunque la enumeración de los poderes, recogida en dicha disposición, no prevé expresamente facultades en relación con transferencias de datos de un Estado miembro a un país tercero, en mi opinión, dicha transferencia está incluida en el concepto de tratamiento de datos. [30] Además, como resulta de la redacción de dicha disposición, la enumeración no es exhaustiva. En todo caso, habida cuenta del papel fundamental que desempeñan las autoridades nacionales de control en el sistema creado por la Directiva 95/46, éstas deben tener la facultad de suspender toda transferencia de datos en caso de que se demuestre que se ha producido una violación de los derechos fundamentales o se sospeche que pueda producirse.

95. Cabe añadir que privar a las autoridades nacionales de control de sus poderes de investigación en circunstancias como las controvertidas en el caso de autos no sólo sería contrario al principio de independencia, sino también al objetivo de la Directiva 95/46 que resulta del artículo 1, apartado 1, de ésta.

96. Como ha observado el Tribunal de Justicia, «de los considerandos 3, 8 y 10 de la Directiva 95/46 resulta que el legislador de la Unión pretendió facilitar la libre circulación de los datos personales mediante la aproximación de las legislaciones de los Estados miembros, protegiendo al mismo tiempo los derechos fundamentales de las personas, particularmente el derecho al respeto de la vida privada, y asegurando un alto nivel de protección dentro de la Unión. El artículo 1 de dicha Directiva establece, por ello, que los Estados miembros deben garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales». [31]

97. Las disposiciones de la Directiva 95/46 deben, por tanto, interpretarse de conformidad con el objetivo de ésta de asegurar un alto nivel de protección de las libertades y los derechos fundamentales de las personas físicas, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales dentro de la Unión.

98. Habida cuenta de la importancia de dicho objetivo y del papel que deben desempeñar los Estados miembros para alcanzarlo, cuando concurren circunstancias particulares que ponen seriamente en entredicho el respeto de los derechos fundamentales garantizados por la Carta en el marco de una transferencia de datos personales a un país tercero, los Estados miembros y, por ende, sus autoridades de control nacionales, no pueden estar vinculados en términos absolutos por una decisión de adecuación de la Comisión.

30 — Véanse las conclusiones del Abogado General Léger presentadas en el asunto Parlamento/Consejo y Comisión (C-317/04, EU:C:2005:710), puntos 92 a 95. Véase, asimismo, la sentencia Parlamento/Consejo y Comisión (C-317/04 y C-318/04, EU:C:2006:346), apartado 56.

31 — Véase, en especial, la sentencia IPI (C-473/12, EU:C:2013:715), apartado 28 y jurisprudencia citada.

99. El Tribunal de Justicia ya ha declarado que «las disposiciones de la Directiva 95/46, en la medida en que regulan el tratamiento de datos personales que pueden atentar contra las libertades fundamentales y, en particular, contra el derecho a la intimidad, deben ser interpretadas a la luz de los derechos fundamentales que, según reiterada jurisprudencia, forman parte de los principios generales del Derecho cuyo respeto garantiza el Tribunal de Justicia y que están actualmente recogidos en la Carta». [32]

100. Asimismo, procede citar la jurisprudencia según la cual «corresponde a los Estados miembros no sólo interpretar su Derecho nacional de conformidad con el Derecho de la Unión, sino también procurar que la interpretación de un texto de Derecho derivado que tomen como base no entre en conflicto con los derechos fundamentales tutelados por el ordenamiento jurídico de la Unión o con los demás principios generales del Derecho de la Unión». [33]

101. En este sentido, el Tribunal de Justicia consideró, en su sentencia N. S. y otros, [34] que «una aplicación del Reglamento [(CE)] nº 343/2003 [[35]] basada en la presunción irrefutable de que se respetarán los derechos fundamentales de los solicitantes de asilo en el Estado miembro en principio responsable para el examen de su solicitud es incompatible con la obligación de los Estados miembros de interpretar y aplicar el Reglamento nº 343/2003 conforme a los derechos fundamentales». [36]

102. A este respecto, el Tribunal de Justicia admitió, en el contexto de la calificación recíproca de los Estados miembros como países de origen seguros para cuestiones jurídicas y prácticas relacionadas con el derecho de asilo, que debe presumirse que el trato dispensado a los solicitantes de asilo en cada Estado miembro es conforme con las exigencias de la Carta, de la Convención sobre el Estatuto de los Refugiados, firmada en Ginebra el 28 de julio de 1951, [37] y del Convenio para la protección de los derechos humanos y de las libertades fundamentales, firmado en Roma el 4 de noviembre de 1950. [38] Sin embargo, el Tribunal de Justicia consideró que «no cabe excluir que este sistema se enfrente, en la práctica, a graves dificultades de funcionamiento en un Estado miembro determinado, de manera que exista un riesgo importante de que los solicitantes de asilo, en caso de ser trasladados a ese Estado miembro, reciban un trato incompatible con sus derechos fundamentales». [39]

103. Por consiguiente, el Tribunal de Justicia consideró que «incumbe a los Estados miembros, incluidos los órganos jurisdiccionales nacionales, no trasladar a un solicitante de asilo al "Estado miembro responsable" en el sentido del Reglamento nº 343/2003 cuando no puedan ignorar que las deficiencias sistemáticas del procedimiento de asilo y de las condiciones de acogida de los solicitantes de asilo en ese Estado miembro constituyen motivos serios y acreditados para creer que el solicitante correrá un riesgo real de ser sometido a tratos inhumanos o degradantes en el sentido del artículo 4 de la Carta». [40]

104. En mi opinión, la jurisprudencia derivada de la sentencia N.S. y otros, [41] puede aplicarse a una situación como la existente en el procedimiento principal. En este sentido, una interpretación del Derecho derivado de la Unión basada en la presunción irrefutable de que se respetarán los derechos fundamentales —ya sea por un Estado miembro, por la Comisión, o por un país tercero— debe

32 — Véase, en particular, la sentencia Google Spain y Google (C-131/12, EU:C:2014:317), apartado 68 y jurisprudencia citada.

33 — Véase, en especial, la sentencia N.S. y otros (C-411/10 y C-493/10, EU:C:2011:865), apartado 77 y jurisprudencia citada.

34 — C-411/10 y C-493/10, EU:C:2011:865.

35 — Reglamento del Consejo de 18 de febrero de 2003 por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país (DO L 50, p. 1).

36 — Apartado 99 de dicha sentencia.

37 — Recopilación de Tratados de las Naciones Unidas, vol. 189, p. 150, nº 2545 (1954).

38 — Véase la sentencia N.S. y otros (C-411/10 y C-493/10, EU:C:2011:865), apartado 80.

39 — *Ibídem*, apartado 81.

40 — *Ibídem*, apartado 94.

41 — C-411/10 y C-493/10, EU:C:2011:865.

considerarse incompatible con la obligación de los Estados miembros de interpretar y aplicar el Derecho derivado de la Unión conforme a los derechos fundamentales. El artículo 25, apartado 6, de la Directiva 95/46 no establece, por tanto, esa presunción irrefutable de respeto de los derechos fundamentales en lo que concierne a la apreciación por la Comisión del carácter adecuado del nivel de protección ofrecido por un país tercero. Al contrario, debe considerarse refutable la presunción, en la que se basa dicha disposición, de que la transferencia de datos a un país tercero respetará los derechos fundamentales. [42] Por consiguiente, no cabe interpretar dicha disposición en el sentido de que pone en entredicho las garantías que figuran en particular en el artículo 28, apartado 3, de la Directiva 95/46 y en el artículo 8, apartado 3, de la Carta, que tienen por objeto la protección y el respeto del derecho a la protección de datos personales.

105. Por tanto, cabe deducir de la sentencia N. S. y otros que, en caso de que se constaten deficiencias sistemáticas en el país tercero al que se transfieren los datos personales, los Estados miembros deben poder adoptar las medidas necesarias para proteger los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta.

106. Por otro lado, como señaló el Gobierno italiano en sus observaciones, la adopción por la Comisión de una decisión de adecuación no puede tener por efecto reducir la protección de los ciudadanos de la Unión en lo que respecta al tratamiento de sus datos cuando éstos se transfieren a un país tercero, frente al nivel de protección del que disfrutarían en caso de que sus datos fueran objeto de tratamiento dentro de la Unión. Por consiguiente, las autoridades de control nacionales deben poder intervenir y ejercitar sus facultades en relación con las transferencias de datos a países terceros objeto de una decisión de adecuación. De lo contrario, los ciudadanos de la Unión estarán mucho menos protegidos que si sus datos se sometieran a tratamiento dentro de la Unión.

107. En este sentido, la adopción por la Comisión de una decisión al amparo del artículo 25, apartado 6, de la Directiva 95/46 únicamente tiene por efecto levantar la prohibición general de exportar datos personales a países terceros que garanticen un nivel de protección comparable al ofrecido por dicha Directiva. En otros términos, no se trata de crear un régimen especial de excepción y menos protector para los ciudadanos de la Unión que el régimen general previsto por dicha Directiva para los tratamientos de datos que se llevan a cabo dentro de la Unión.

108. Es cierto que el Tribunal de Justicia observó, en el apartado 63 de su sentencia Lindqvist, [43] que «el capítulo IV de la Directiva 95/46, en el que figura el artículo 25, establece un régimen especial». Sin embargo, a mi parecer, ello no significa que dicho régimen deba ser menos protector. Al contrario, para alcanzar el objetivo de protección de datos establecido en el artículo 1, apartado 1, de la Directiva 95/46, el artículo 25 de ésta impone una serie de obligaciones a los Estados miembros y a la Comisión [44] y plantea el principio según el cual si un país tercero no ofrece un nivel de protección adecuado, debe prohibirse la transferencia de datos personales a dicho país. [45]

109. En lo que atañe más concretamente al régimen de puerto seguro, la Comisión sólo contempla la intervención de las autoridades de control nacionales y la suspensión por su parte de los flujos de datos en el marco previsto en el artículo 3, apartado 1, letra b), de la Decisión 2000/520.

42 — Apartado 104 de dicha sentencia.

43 — C-101/01, EU:C:2003:596.

44 — Apartado 65.

45 — Apartado 64.

110. Según el considerando 8 de dicha Decisión, «aunque se compruebe el nivel adecuado de la protección, por motivos de transparencia y para proteger la capacidad de las autoridades correspondientes de los Estados miembros de garantizar la protección de las personas en lo que respecta al tratamiento de sus datos personales, resulta necesario especificar en la presente Decisión las circunstancias excepcionales que pudieran justificar la suspensión de flujos específicos de información».

111. En el presente asunto lo que se cuestiona, en particular, es la aplicación del artículo 3, apartado 1, letra b), de dicha Decisión. En este sentido, en virtud de dicha disposición, las autoridades de control nacionales pueden acordar la suspensión de flujos de datos cuando «existen grandes probabilidades de que se estén vulnerando los principios; existen razones para creer que el mecanismo de aplicación correspondiente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad y proporcionarle la oportunidad de alegar».

112. Dicha disposición establece diversos requisitos que las partes han interpretado de diferentes maneras en el presente procedimiento.[46] Sin entrar en los pormenores de dichas interpretaciones, de ellas se desprende que dichos requisitos delimitan de manera estricta el poder de las autoridades de control nacionales de suspender los flujos de datos.

113. Pues bien, a diferencia de lo que sostiene la Comisión, el artículo 3, apartado 1, letra b), de la Decisión 2000/520 debe interpretarse de conformidad con el objetivo de protección de datos personales que persigue la Directiva 95/46, así como a la luz del artículo 8 de la Carta. El hecho de que la interpretación deba hacerse imperativamente a la luz de los derechos fundamentales aboga por que dicha disposición sea interpretada de manera amplia.

114. De ello se desprende, en mi opinión, que los requisitos previstos en el artículo 3, apartado 1, letra b), de la Decisión 2000/520, no pueden impedir que una autoridad de control nacional ejerza, con total independencia, los poderes que se le confieren en virtud del artículo 28, apartado 3, de la Directiva 95/46.

115. Tal como indicaron, en esencia, los Gobiernos belga y austriaco en la vista, la salida de emergencia que constituye el artículo 3, apartado 1, letra b), de la Decisión 2000/520 es tan estrecha, que es complicado utilizarla. Exige que se cumplan requisitos acumulativos y pone el listón demasiado alto. Pues bien, a la luz del artículo 8, apartado 3, de la Carta, es imposible que el margen de discrecionalidad de las autoridades de control nacionales en lo que atañe a las facultades que les confiere el artículo 28, apartado 3, de la Directiva 95/46, se vea restringido de tal manera que no puedan ejercerse.

116. A este respecto, el Parlamento señaló acertadamente que fue el legislador de la Unión quien decidió los poderes que debían corresponder a las autoridades de control nacionales. Pues bien, el poder de ejecución conferido por el legislador de la Unión a la Comisión en el artículo 25, apartado 6, de la Directiva 95/46 no afecta a los poderes otorgados por este mismo legislador a las autoridades de control nacionales en el artículo 28, apartado 3, de dicha Directiva. En otros términos, la Comisión no dispone del poder de restringir las facultades de las autoridades de control nacionales.

46 — Según el Sr. Schrems, no se cumple el primer requisito, según el cual han de existir «grandes probabilidades de que se estén vulnerando los principios». Pues bien, no se alega que la propia Facebook USA, en su condición de entidad autocertificada a la que se transfieren datos, haya vulnerado los principios de puerto seguro a raíz de que las autoridades estadounidenses hayan accedido de manera masiva e indiscriminada a los datos que almacena. En efecto, los principios de puerto seguro se encuentran expresamente limitados por la legislación estadounidense definida en el anexo I, párrafo cuarto, de la Decisión 2000/520, mediante remisión a las disposiciones legales y reglamentarias y a la jurisprudencia.

117. Por consiguiente, para garantizar un nivel de protección adecuado de los derechos fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales, las autoridades de control nacionales deben tener la facultad de abrir una investigación cuando se invoquen ante ellas vulneraciones de tales derechos. Si, una vez finalizada la investigación, dichas autoridades consideran que existen serios indicios de que, en un país con respecto al cual se ha dictado una decisión de adecuación, se ha vulnerado el derecho de los ciudadanos de la Unión a la protección de sus datos personales, deben poder suspender la transferencia de datos al destinatario establecido en dicho país tercero.

118. En otras palabras, las autoridades de control nacionales deben poder llevar a cabo sus investigaciones y, en su caso, suspender una transferencia de datos, con independencia de los requisitos restrictivos establecidos en el artículo 3, apartado 1, letra b), de la Decisión 2000/520.

119. Por otra parte, en virtud de su capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46 o de poner dichas infracciones en conocimiento de la autoridad judicial, prevista en el artículo 28, apartado 3, de dicha Directiva, las autoridades de control nacionales, cuando tengan conocimiento de hechos que demuestren que un país tercero no garantiza un nivel de protección adecuado, deben poder acudir ante un órgano jurisdiccional nacional que, en su caso, podrá decidir plantear ante el Tribunal de Justicia una petición de decisión prejudicial para apreciar la validez de una decisión de adecuación de la Comisión.

120. De todas las consideraciones anteriores se desprende que el artículo 28 de la Directiva 95/46, leído a la luz de los artículos 7 y 8 de la Carta, debe interpretarse en el sentido de que la existencia de una decisión adoptada por la Comisión sobre la base del artículo 25, apartado 6, de dicha Directiva, no tiene por efecto impedir que una autoridad de control nacional investigue una denuncia en la que se afirme que un país tercero no garantiza un nivel de protección adecuado de los datos de carácter personal transferidos y, en su caso, suspenda la transmisión de datos impugnada.

121. Aun cuando la High Court insiste en su resolución de remisión en que el Sr. Schrems no ha impugnado formalmente en su recurso en el procedimiento principal la validez de la Directiva 95/46, ni la de la Decisión 2000/520, de dicha resolución de remisión resulta que la principal censura del Sr. Schrems consiste en cuestionar la constatación de que Estados Unidos garantiza un nivel de protección adecuado de los datos de carácter personal transferidos en el marco del régimen de puerto seguro.

122. Asimismo, se desprende de las observaciones del comisario que la denuncia del Sr. Schrems trata de impugnar directamente la Decisión 2000/520. Con su denuncia, este último ha pretendido impugnar los términos y el funcionamiento del régimen de puerto seguro, aduciendo que la vigilancia masiva de los datos personales transferidos a Estados Unidos demuestra que no existe una protección real de dichos datos ni de hecho, ni de Derecho, en dicho país tercero.

123. Además, el propio órgano jurisdiccional remitente observa que la garantía prevista en el artículo 7 de la Carta y que emana de los valores fundamentales presentes en las tradiciones constitucionales comunes a los Estados miembros se vería comprometida si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y general sin la obligación de aportar una motivación objetiva basada en razones de seguridad nacional o de prevención del delito vinculadas específicamente a las personas afectadas y sin ninguna garantía adecuada y comprobable.[47] Así pues, el órgano jurisdiccional remitente manifiesta indirectamente sus dudas en cuanto a la validez de la Decisión 2000/520.

47 — Apartado 24 de la resolución de remisión.

124. Por tanto, la apreciación de si Estados Unidos garantiza un nivel de protección adecuado de los datos de carácter personal transferidos en el marco del régimen de puerto seguro, conduce necesariamente a reflexionar sobre la validez de dicha Decisión.

125. A este respecto, conviene señalar que en el marco del mecanismo de cooperación entre el Tribunal de Justicia y los órganos jurisdiccionales nacionales creado por el artículo 267 TFUE, el Tribunal de Justicia, aun cuando se recurra a él exclusivamente con carácter prejudicial, podrá verse obligado, en circunstancias particulares, a examinar la validez de determinadas disposiciones de Derecho derivado.

126. Pues bien, en varias ocasiones, el Tribunal de Justicia ha anulado de oficio un acto del que únicamente se solicitaba su interpretación. [48] Asimismo, ha considerado que «cuando parece que el verdadero objeto de las cuestiones planteadas por un órgano jurisdiccional nacional consiste más bien en el examen de la validez que en la interpretación de actos [de la Unión], incumbe al Tribunal de Justicia proporcionar de inmediato la respuesta a dicho órgano jurisdiccional sin obligarle a un formalismo meramente dilatorio incompatible con la naturaleza propia de los mecanismos establecidos por el artículo [267 TFUE]». [49] Por otro lado, el Tribunal de Justicia ya ha afirmado que debe entenderse que las dudas manifestadas por un órgano jurisdiccional remitente sobre la compatibilidad de un acto de Derecho derivado con las normas relativas a la protección de los derechos fundamentales ponen asimismo en cuestión la validez de dicho acto en relación con el Derecho de la Unión. [50]

127. Cabe recordar asimismo que, conforme a la jurisprudencia del Tribunal de Justicia, los actos de las instituciones, de los órganos y de los organismos de la Unión gozan de una presunción de validez, lo cual implica que producen efectos jurídicos mientras no hayan sido revocados, anulados en el marco de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad. Sólo el Tribunal de Justicia es competente para declarar la invalidez de un acto de la Unión, competencia cuyo objeto es garantizar la seguridad jurídica preservando la aplicación uniforme del Derecho de la Unión. A falta de declaración de invalidez, de modificación o de derogación por la Comisión, la Decisión sigue siendo obligatoria en todos sus elementos y directamente aplicable en todo Estado miembro. [51]

128. Con objeto de proporcionar una respuesta completa al órgano jurisdiccional remitente y disipar todas las dudas planteadas durante el presente procedimiento sobre la validez de la Decisión 2000/520, opino, por consiguiente, que el Tribunal de Justicia debe analizar la validez de dicha Decisión.

129. Dicho esto, también es importante precisar que el análisis de la validez o nulidad de la Decisión 2000/520 debe circunscribirse a las alegaciones que han sido objeto de debate en el marco del presente procedimiento. En efecto, dado que en dicho contexto no se han debatido todos los aspectos relativos al funcionamiento del régimen de puerto seguro, no creo que sea posible efectuar en este asunto un examen exhaustivo de las deficiencias de dicho régimen.

130. En cambio, en el presente procedimiento, sí se ha debatido ante el Tribunal de Justicia si el acceso generalizado e indiscriminado de los servicios de inteligencia estadounidenses a los datos transferidos puede afectar a la legalidad de la Decisión 2000/520. Por tanto, puede examinarse la validez de dicha Decisión desde esa perspectiva.

48 — Véanse, en especial, las sentencias Strehl (62/76, EU:C:1977:18), apartados 10 a 17; Roquette Frères (145/79, EU:C:1980:234), apartado 6, y Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576), apartados 32 a 39.

49 — Sentencia Schwarze (16/65, EU:C:1965:117), p. 1094.

50 — Véase la sentencia Hauer (44/79, EU:C:1979:290), apartado 16.

51 — Véase, en especial, la sentencia CIVAD (C-533/10, EU:C:2012:347), apartados 39 a 41 y jurisprudencia citada.

B. *Sobre la validez de la Decisión 2000/520*

1. Sobre los elementos que deben tenerse en cuenta para evaluar la validez de la Decisión 2000/520

131. Conviene recordar la jurisprudencia según la cual «en el marco de un recurso de anulación, la legalidad de un acto debe apreciarse a la luz de los elementos de hecho y de Derecho existentes en la fecha en que se adoptó este acto, pudiendo únicamente ser censurada la valoración de la Comisión si se revela manifiestamente errónea a la vista de los elementos de que disponía al adoptar dicho acto». [52]

132. En su sentencia Gaz de France — Berliner Investissement, [53] el Tribunal de Justicia recordó el principio según el cual «la apreciación de la validez de un acto, apreciación que debe efectuar el Tribunal de Justicia en el marco de una remisión prejudicial, normalmente debe basarse en la situación que existe en el momento de la adopción de ese acto». [54] Sin embargo, pareció admitir que «la validez de un acto pueda, en ciertos casos, apreciarse en función de elementos nuevos que hayan tenido lugar con posterioridad a su adopción». [55]

133. La posibilidad enunciada por el Tribunal de Justicia me parece particularmente pertinente en el caso de autos.

134. En efecto, las decisiones adoptadas por la Comisión sobre la base del artículo 25, apartado 6, de la Directiva 95/46, presentan características particulares. Tienen por objeto evaluar si el nivel de protección de datos personales que ofrece un país tercero es o no adecuado. Se trata de una apreciación que está abocada a evolucionar en función del contexto circunstancial y jurídico vigente en el país tercero.

135. Habida cuenta de que la decisión de adecuación constituye un tipo de decisión particular, es preciso matizar en el caso de autos el principio de que la apreciación de su validez únicamente se puede efectuar en función de la situación existente en la fecha de su adopción. De lo contrario, tal norma tendría entrañaría que, varios años después de la adopción de una decisión de adecuación, el Tribunal de Justicia no podría tomar en consideración a la hora de valorar su validez acontecimientos acaecidos con posterioridad, y ello aun cuando tal remisión prejudicial para apreciar la validez no tenga límite temporal y se haya planteado precisamente a raíz del acaecimiento de hechos posteriores que ponen de manifiesto las deficiencias del acto impugnado.

136. En el caso de autos, el mantenimiento en vigor de la Decisión 2000/520 desde hace unos quince años atestigua que la Comisión confirma implícitamente la evaluación que llevó a cabo en el año 2000. Por tanto, cuando, en el marco de una cuestión prejudicial, el Tribunal de Justicia deba examinar la validez de una evaluación mantenida en el tiempo por la Comisión, no sólo es posible, sino también apropiado, que pueda confrontar dicha evaluación a los nuevos acontecimientos que se hayan producido tras la adopción de la decisión de adecuación.

52 — Véase, en especial, la sentencia BVGD/Comisión (T-104/07 y T 339/08, EU:T:2013:366), apartado 291, que se remite a la sentencia IECC/Comisión (C-449/98 P, EU:C:2001:275), apartado 87.

53 — C-247/08, EU:C:2009:600.

54 — Apartado 49 y jurisprudencia citada.

55 — Apartado 50 y jurisprudencia citada. Véase, en este sentido, Lenaerts, K., Maselis, I., y Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, que indican que, «in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court» (punto 10.16, p. 471).

137. Habida cuenta de la particular naturaleza de la decisión de adecuación, ésta debe ser objeto de una revisión periódica por parte de la Comisión. Si, tras el acaecimiento de nuevos acontecimientos que se hayan producido entretanto, la Comisión no modifica su decisión, se entenderá que confirma implícita, pero necesariamente, la apreciación efectuada inicialmente. De este modo, reitera su declaración según la cual el país tercero de que se trata garantiza un nivel de protección adecuado de los datos personales transferidos. Corresponde al Tribunal de Justicia examinar si dicha declaración sigue siendo válida a pesar de los acontecimientos acaecidos con posterioridad.

138. Por consiguiente, en mi opinión, para garantizar un control jurisdiccional efectivo de este tipo de decisiones, la apreciación de su validez debe realizarse teniendo en cuenta el contexto fáctico y jurídico vigente.

2. Sobre el concepto de nivel de protección adecuado

139. El artículo 25 de la Directiva 95/46 se basa íntegramente en el principio según el cual no pueden transferirse datos personales a un país tercero si éste no garantiza un nivel de protección adecuado de tales datos. El objetivo de dicho artículo es, por tanto, garantizar la continuidad de la protección conferida por dicha Directiva en caso de transferencia de datos personales a un país tercero. A este respecto, conviene recordar que dicha Directiva ofrece un alto nivel de protección de los ciudadanos de la Unión en lo que respecta al tratamiento de sus datos personales.

140. Atendiendo al importante papel que desempeña la protección de los datos personales en lo que atañe al derecho fundamental al respeto de la vida privada, debe garantizarse, por tanto, ese alto nivel de protección incluso en caso de transferencia de datos personales a un país tercero.

141. Por ello considero que la Comisión únicamente puede declarar, sobre la base del artículo 25, apartado 6, de la Directiva 95/46, que un país tercero garantiza un nivel de protección adecuado si, una vez realizada una evaluación de conjunto del Derecho y de las prácticas vigentes en el país tercero en cuestión, puede afirmar que dicho país tercero garantiza un nivel de protección sustancialmente equivalente al ofrecido por dicha Directiva, aun cuando las modalidades de dicha protección puedan diferir de las que generalmente se aplican en la Unión.

142. Si bien puede entenderse que el término inglés «adequate», desde un punto de vista lingüístico, designa un nivel de protección simplemente satisfactorio o suficiente, y que, en este sentido, pertenece a un campo semántico distinto del término español «adecuado», conviene observar que el único criterio que debe guiar la interpretación de dicho término es el objetivo de alcanzar un alto nivel de protección de los derechos fundamentales, como exige la Directiva 95/46.

143. El examen del nivel de protección ofrecido por un país tercero deben abordar dos elementos fundamentales, a saber, el contenido de las normas aplicables y los mecanismos para garantizar el respeto de dichas normas. [56]

144. A mi parecer, para alcanzar un nivel de protección sustancialmente equivalente al vigente dentro de la Unión, el régimen de puerto seguro, que se fundamenta en gran medida en la autocertificación y la autoevaluación de las empresas que se adhieren voluntariamente a dicho régimen, debe ir acompañado de garantías adecuadas y de un mecanismo de control válido. En este sentido, las transferencias de datos personales a países terceros no deben ser objeto de una protección inferior a la que se aplica a los tratamientos de datos realizados dentro de la Unión.

56 — Véase la página 5 del documento de trabajo WP 12 de la Comisión, titulado «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE», adoptado el 24 de julio de 1998 por el Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

145. A este respecto, cabe señalar, de entrada, que, en la Unión, rige la idea de que un mecanismo de control externo, que revista la forma de una autoridad independiente, constituye un elemento necesario de todo sistema que tenga por objeto garantizar el respeto de la legislación relativa a la protección de datos personales.

146. Además, para garantizar el efecto útil del artículo 25, apartados 1 a 3, de la Directiva 95/46, conviene tener en cuenta que el carácter adecuado del nivel de protección ofrecido por un país tercero es una situación cambiante que puede variar a lo largo del tiempo en función de diversos de factores. Los Estados miembros y la Comisión deben, por consiguiente, estar alerta ante cualquier cambio en las circunstancias que pueda exigir una reconsideración del carácter adecuado del nivel de protección ofrecido por un país tercero. La apreciación del carácter adecuado del nivel de dicha protección no puede circunscribirse en ningún caso a una fecha concreta y mantenerse posteriormente de forma indefinida, al margen de todo cambio de circunstancias que demuestre que, en realidad, el nivel de protección ofrecido ya no es adecuado.

147. La obligación que tiene el país tercero de garantizar un nivel de protección adecuado constituye, por tanto, una obligación permanente. Si la evaluación se lleva a cabo en una fecha concreta, el mantenimiento de la decisión de adecuación presupone que, desde entonces, no se ha producido ninguna circunstancia que ponga en duda la evaluación inicial efectuada por la Comisión.

148. En efecto, no hay que olvidar que el objetivo del artículo 25 de la Directiva 95/46 es en todo caso el de evitar que los datos de carácter personal sean transferidos a un país tercero que no garantiza un nivel de protección adecuado, en vulneración del derecho fundamental a la protección de datos personales garantizado por el artículo 8 de la Carta.

149. Es importante recalcar que la facultad que el legislador de la Unión atribuye a la Comisión, en virtud del artículo 25, apartado 6, de la Directiva 95/46, de hacer constar que un país tercero garantiza un nivel de protección adecuado está expresamente sujeta a la condición de que dicho país tercero garantice un nivel de protección adecuado, en el sentido del apartado 2 de dicho artículo. Si concurren nuevas circunstancias que puedan desvirtuar la evaluación inicial de la Comisión, ésta deberá adaptar su decisión en consecuencia.

3. Análisis

150. Procede recordar que, en virtud del artículo 25, apartado 6, de la Directiva 95/46, «la Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas». Leído en relación con el artículo 25, apartado 2, de dicha Directiva, el artículo 25, apartado 6, de ésta indica que, para hacer constar que un país tercero garantiza un nivel de protección adecuado, la Comisión debe llevar a cabo una evaluación de conjunto de las normas de Derecho vigentes en el país tercero y de su aplicación.

151. Anteriormente se ha indicado que el mantenimiento por la Comisión de su Decisión 2000/520, a pesar de la concurrencia de elementos fácticos y jurídicos nuevos, debe entenderse como una voluntad por su parte de confirmar su evaluación inicial.

152. No corresponde al Tribunal de Justicia, en el marco de una remisión prejudicial, examinar los hechos que originaron el litigio que condujo al órgano jurisdiccional nacional a llevar a cabo dicha remisión prejudicial. [57]

153. Por consiguiente, me basaré en los hechos expuestos por el órgano jurisdiccional remitente en su petición de decisión prejudicial, hechos que, por lo demás, la Comisión considera, en términos generales, probados. [58]

154. Las alegaciones formuladas ante el Tribunal de Justicia para impugnar la evaluación de la Comisión según la cual el régimen de puerto seguro garantiza un nivel de protección adecuado de los datos personales transferidos desde la Unión a Estados Unidos pueden describirse de la siguiente manera.

155. En su petición de decisión prejudicial, el órgano jurisdiccional remitente parte de los dos hechos siguientes. Por una parte, los datos personales transferidos por empresas como Facebook Ireland a su sociedad matriz establecida en Estados Unidos pueden ser posteriormente susceptibles de ser consultados por la NSA y otras agencias de seguridad estadounidenses en el marco de actividades de vigilancia e interceptación masivas e indiferenciadas. En efecto, en la estela de las revelaciones del Sr. Snowden, las pruebas disponibles no admiten ninguna otra conclusión realista. [59] Por otra parte, los ciudadanos de la Unión Europea no tienen un derecho efectivo a ser oídos en relación con la vigilancia y la interceptación de sus datos por parte de la NSA y otras agencias de seguridad estadounidenses. [60]

156. La determinación de los hechos llevada a cabo por la High Court a este respecto está respaldada por las observaciones formuladas por la propia Comisión.

157. En este sentido, en su Comunicación sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, antes citada, la Comisión partió del postulado de que, durante el año 2013, ciertas informaciones sobre la magnitud y el alcance de los programas de vigilancia estadounidenses suscitaron preocupación en relación con la continuidad de la protección de los datos personales legalmente transferidos a Estados Unidos en el marco del régimen de puerto seguro. Señaló que aparentemente todas las empresas involucradas en el programa PRISM, y que conceden a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro. A su parecer, el régimen de puerto seguro ha pasado a ser uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que han sido tratados inicialmente en la Unión. [61]

158. De dichos elementos resulta que el Derecho y la práctica de Estados Unidos permiten recopilar, a gran escala, los datos personales de ciudadanos de la Unión que son transferidos en el marco del régimen de puerto seguro, sin que éstos gocen de una tutela judicial efectiva.

159. Dichos hechos demuestran, en mi opinión, que la Decisión 2000/520 no contiene suficientes garantías. Dada tal falta de garantías, la aplicación de dicha Decisión no cumple los requisitos exigidos por la Carta y por la Directiva 95/46.

57 — Véase, en especial, la sentencia Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335), apartado 22 y la jurisprudencia citada.

58 — Véanse la Comunicación de la Comisión citada en la nota 2 y la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE [COM(2013) 847 final].

59 — Apartado 7, letra c), de la resolución de remisión.

60 — Apartado 7, letra b), de la resolución de remisión.

61 — Página 19 de su Comunicación.

160. Pues bien, una decisión adoptada por la Comisión sobre la base del artículo 25, apartado 6, de la Directiva 95/46 tiene por objeto hacer constar que un país tercero «garantiza» un nivel de protección adecuado. El término «garantiza», conjugado en presente de indicativo, implica que, para que se pueda mantener, tal decisión debe referirse a un país tercero que, tras la adopción de dicha decisión, siga garantizando un nivel de protección adecuado.

161. En realidad, las revelaciones invocadas sobre las actuaciones de la NSA, que utiliza datos transferidos en el marco del régimen de puerto seguro, han puesto de manifiesto las deficiencias de la Decisión 2000/520 como base legal.

162. Las deficiencias puestas de manifiesto durante el presente procedimiento figuran más concretamente en el anexo I, párrafo cuarto, de dicha Decisión.

163. Procede recordar que, con arreglo a dicha disposición, «la adhesión a [los] principios [de puerto seguro] puede limitarse: a) cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones».

164. El problema se origina esencialmente por la aplicación que hacen las autoridades estadounidenses de las excepciones previstas en dicha disposición. Dados los términos demasiado generales de su redacción, la aplicación de dichas excepciones por dichas autoridades no se limita a lo estrictamente necesario.

165. A dicha redacción en términos demasiado generales se añade la circunstancia de que los ciudadanos de la Unión no disponen de ninguna vía de recurso adaptada contra el tratamiento de sus datos personales con fines distintos de aquellos por los que fueron inicialmente recopilados y posteriormente transferidos a Estados Unidos.

166. Las excepciones previstas por la Decisión 2000/520 a la aplicación de los principios del régimen de puerto seguro, en particular por motivos de seguridad nacional, deberían haber ido acompañadas de la creación de un mecanismo de control independiente para evitar las violaciones detectadas del derecho a la vida privada.

167. En este sentido, las revelaciones sobre las prácticas de los servicios de inteligencia estadounidenses en lo que atañe a la vigilancia generalizada de los datos transferidos en el marco del régimen de puerto seguro pusieron de manifiesto determinadas deficiencias de la Decisión 2000/520.

168. Los hechos que se han expuesto en el marco del presente asunto no constituyen una infracción de los principios del régimen de puerto seguro por parte de Facebook. Puede considerarse que una empresa certificada, como Facebook USA, proporciona a las autoridades estadounidenses acceso a los datos que le han sido transferidos desde un Estado miembro para ajustarse a la legislación estadounidense. Habida cuenta del hecho de que dicha situación se encuentra expresamente reconocida por la Decisión 2000/520, dada la formulación amplia de las excepciones que contiene, la cuestión que realmente se suscita en el caso de autos es si tales excepciones son compatibles con el Derecho primario de la Unión.

169. Conviene, a este respecto, recalcar que de reiterada jurisprudencia del Tribunal de Justicia se desprende que el respeto de los derechos humanos constituye un requisito de legalidad de los actos de la Unión y que no pueden admitirse en la Unión medidas incompatibles con el respeto de los derechos humanos. [62]

170. Por otro lado, resulta de la jurisprudencia del Tribunal de Justicia que la comunicación de datos personales a un tercero, ya sea una entidad pública o privada, lesiona el derecho al respeto de la vida privada de los interesados, «sea cual fuere la utilización posterior de los datos comunicados de este modo». [63] Además, en su sentencia Digital Rights Ireland y otros, [64] el Tribunal de Justicia confirmó que el hecho de autorizar el acceso de las autoridades nacionales competentes a dichos datos constituye una injerencia adicional y distinta en ese derecho fundamental. [65] Además, toda forma de tratamiento de datos personales está incluida en el alcance del artículo 8 de la Carta y constituye una injerencia en el derecho a la protección de datos de carácter personal. [66] El acceso que los servicios de inteligencia estadounidenses tienen a los datos transferidos es, por consiguiente, también constitutivo de una injerencia en el derecho fundamental a la protección de datos personales garantizado por el artículo 8 de la Carta, por cuanto que tal acceso constituye un tratamiento de dichos datos.

171. Tal y como constató el Tribunal de Justicia en dicha sentencia, la injerencia detectada resulta de gran magnitud y debe considerarse especialmente grave, habida cuenta del elevado número de usuarios afectados y de las cantidades de datos transferidos. Dichos elementos, asociados al carácter secreto del acceso por parte de las autoridades estadounidenses a los datos personales transferidos a empresas establecidas en Estados Unidos, hacen que la injerencia resulte sumamente grave.

172. A ello se añade la circunstancia de que los ciudadanos de la Unión, usuarios de Facebook, no están informados de que las agencias de seguridad estadounidenses podrán acceder de manera general a sus datos personales.

173. Conviene asimismo hacer hincapié en que el órgano jurisdiccional remitente declaró que, en Estados Unidos, los ciudadanos de la Unión no tienen un derecho efectivo a ser oídos en relación con la vigilancia y la interceptación de sus datos. Pese a que la FISC competente ejerce cierta supervisión, el procedimiento que se sustancia ante ella es secreto y no contradictorio. [67] Considero que en este caso se trata de una injerencia en el derecho de los ciudadanos de la Unión a la tutela judicial efectiva amparado por el artículo 47 de la Carta.

174. Se establece, por tanto, la injerencia permitida por las excepciones a los principios del régimen de puerto seguro que figuran en el anexo I, párrafo cuarto, de la Decisión 2000/520, en los derechos fundamentales protegidos por los artículos 7, 8 y 47 de la Carta.

175. Procede ahora comprobar si dicha injerencia está o no justificada.

176. De conformidad con el artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ella deberá ser establecida por la ley y deberá respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y de las libertades de los demás.

62 — Véase, en especial, la sentencia Kadi y Al Barakaat International Foundation/Consejo y Comisión (C-402/05 P y C-415/05 P, EU:C:2008:461), apartado 284 y jurisprudencia citada.

63 — Sentencia Österreichischer Rundfunk y otros (C-465/00, C-138/01 y C-139/01, EU:C:2003:294), apartado 74.

64 — C-293/12 y C-594/12, EU:C:2014:238.

65 — Apartado 35.

66 — Apartado 36.

67 — Apartado 7, letra b), de la resolución de remisión.

177. A la luz de los requisitos establecidos para poder admitir limitaciones al ejercicio de los derechos y de las libertades protegidos por la Carta, pongo seriamente en duda que se pueda considerar que las limitaciones objeto del caso de autos respeten el contenido esencial de los artículos 7 y 8 de la Carta. En efecto, aparentemente, el acceso por parte de los servicios de inteligencia estadounidenses a los datos transferidos se extiende al contenido de las comunicaciones electrónicas, lo que constituye una vulneración del contenido esencial del derecho fundamental al respeto de la vida privada y de los demás derechos consagrados en el artículo 7 de la Carta. Además, en la medida en que la formulación amplia de las limitaciones previstas en el anexo I, párrafo cuarto, de la Decisión 2000/520 permite potencialmente excluir la aplicación de todos los principios del régimen de puerto seguro, cabe considerar que dichas limitaciones vulneran el contenido esencial del derecho fundamental a la protección de datos de carácter personal. [68]

178. En cuanto a si la injerencia puesta de manifiesto responde a un objetivo de interés general, ha de señalarse en primer lugar que, en virtud del anexo I, párrafo cuarto, letra b), de la Decisión 2000/520, la adhesión a los principios de puerto seguro puede limitarse «por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones».

179. Ha de observarse que no se precisan los «intereses legítimos» que se mencionan en dicha disposición. Ello genera incertidumbre en cuanto al ámbito de aplicación, que puede ser sumamente amplio, de dicha excepción a la aplicación de los principios del régimen de puerto seguro por las empresas que se adhieren a dicho régimen.

180. La lectura de las explicaciones que figuran en el título B del anexo IV de la Decisión 2000/520, titulado «Autorizaciones legales explícitas», confirma esta impresión, en particular la afirmación según la cual «es evidente que, si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de los principios de puerto seguro». Por otro lado, con respecto a las autorizaciones explícitas, se indica que «aunque estos principios [de puerto seguro] tienen como finalidad salvar las diferencias entre los regímenes estadounidense y europeo de protección de la intimidad, debemos respetar las facultades legislativas de nuestros legisladores».

181. De ello resulta, en mi opinión, que dicha excepción es contraria a los artículos 7, 8 y 52, apartado 1, de la Carta, en la medida en que no persigue un objetivo de interés general definido de manera suficientemente precisa.

182. En todo caso, la facilidad y la generalidad con las que la propia Decisión 2000/520, en sus anexos I, párrafo cuarto, letra b), y IV B, prevé que se pueden eludir los principios de puerto seguro en aplicación de la legislación estadounidense, son incompatibles con el requisito según el cual las excepciones a las normas relativas a la protección de datos de carácter personal deben limitarse a lo estrictamente necesario. Ciertamente, se menciona el requisito de necesidad, pero, además de que la carga de demostrar que se cumple dicho requisito se atribuye a la empresa, no alcanzo a ver cómo puede una empresa eludir la obligación de apartarse de los principios de puerto seguro derivada de normas de Derecho que está obligada a cumplir.

183. Por consiguiente, opino que debe declararse inválida la Decisión 2000/520 en la medida en que la existencia de una excepción que permite de manera tan general e imprecisa eludir los principios del régimen de puerto seguro impide por sí misma considerar que dicho régimen garantiza un nivel de protección adecuado de los datos personales que son transferidos desde la Unión a Estados Unidos.

68 — Véase, en este sentido, la sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), apartados 39 y 40.

184. Por lo que se refiere a la primera categoría de límites previstos en el anexo I, párrafo cuarto, letra a), de la Decisión 2000/520, para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley estadounidense, sólo el primero de los objetivos me parece ser lo suficientemente preciso para ser considerado un objetivo de interés general reconocido por la Unión en el sentido del artículo 52, apartado 1, de la Carta.

185. Conviene ahora comprobar la proporcionalidad de la injerencia constatada.

186. A este respecto, procede recordar que según jurisprudencia reiterada del Tribunal de Justicia, «el principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos». [69]

187. En lo que atañe al control jurisdiccional de la observancia de estos requisitos, «dado que se trata de injerencias en los derechos fundamentales, el alcance de la facultad de apreciación del legislador de la Unión puede resultar limitado en función de una serie de factores, entre los que figuran, en particular, el ámbito afectado, el carácter del derecho en cuestión garantizado por la Carta, la naturaleza y la gravedad de la injerencia, así como la finalidad de ésta». [70]

188. Considero que las decisiones que la Comisión adopta sobre la base del artículo 25, apartado 6, de la Directiva 95/46 están sujetas al control integral del Tribunal de Justicia en lo que se refiere a la proporcionalidad de la evaluación realizada por dicha institución en relación con el carácter adecuado del nivel de protección ofrecido por un país tercero a la vista «de su legislación interna o de sus compromisos internacionales».

189. A este respecto, conviene señalar que, en su sentencia Digital Rights Ireland y otros, [71] el Tribunal de Justicia consideró que «debido, por una parte, al importante papel que desempeña la protección de los datos de carácter personal en lo que respecta al derecho fundamental al respeto de la vida privada y, por otra parte, a la magnitud y gravedad de la injerencia en este derecho que supone la Directiva [impugnada], la facultad de apreciación del legislador de la Unión resulta reducida, por lo que el control de dicha facultad debe ser estricto». [72]

190. Tal injerencia debe ser adecuada para lograr el objetivo perseguido por el acto de la Unión impugnado y necesaria para el logro de dicho objetivo.

191. En este sentido, «en lo que respecta al derecho a la intimidad, la protección de este derecho fundamental exige [...], conforme a la jurisprudencia reiterada del Tribunal de Justicia, que las excepciones a la protección de los datos personales y las restricciones a dicha protección se establezcan sin sobrepasar los límites de lo estrictamente necesario». [73]

192. Al ejercer su control, el Tribunal de Justicia también debe tener en cuenta que «la protección de los datos de carácter personal, que resulta de la obligación expresa establecida en el artículo 8, apartado 1, de la Carta, tiene una importancia especial para el derecho al respeto de la vida privada consagrado en el artículo 7 de ésta». [74]

69 — Sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), apartado 46 y jurisprudencia citada.

70 — *Ibídem*, apartado 47 y jurisprudencia citada.

71 — C-293/12 y C-594/12, EU:C:2014:238.

72 — Apartado 48.

73 — Sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), apartado 52 y jurisprudencia citada.

74 — *Ibídem*, apartado 53.

193. Según el Tribunal de Justicia, que, en este sentido, se remite a la jurisprudencia del Tribunal Europeo de Derechos Humanos, «la normativa de la Unión de que se trate debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos».[75] El Tribunal de Justicia señala que «la necesidad de disponer de tales garantías es especialmente importante cuando [...] los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a dichos datos».[76]

194. En mi opinión, existe una analogía entre el anexo I, párrafo cuarto, letra a), de la Decisión 2000/520, y el artículo 13, apartado 1, de la Directiva 95/46. En la primera disposición, se establece que la adhesión a los principios de puerto seguro puede limitarse para cumplir «las exigencias de seguridad nacional, interés público y cumplimiento de la ley [estadounidense]». En la segunda, se prevé que los Estados miembros pueden adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en los artículos 6, apartado 1, 10, 11, apartado 1, 12 y 21 de dicha Directiva, siempre que dicha limitación constituya una medida necesaria, especialmente por motivos de seguridad del Estado, defensa, seguridad pública y prevención, investigación, detección y represión de infracciones penales.

195. Como señaló el Tribunal de Justicia en su sentencia IPI,[77] del artículo 13, apartado 1, de la Directiva 95/4 se desprende que los Estados miembros únicamente podrán adoptar las medidas previstas en dicha disposición si éstas son necesarias. El carácter «necesario» de las medidas condiciona la facultad concedida a los Estados miembros en dicha disposición.[78] En lo que respecta a los tratamientos de datos de carácter personal dentro de la Unión, los límites previstos en el artículo 13 de dicha Directiva deben entenderse como restringidos a los casos estrictamente necesarios para alcanzar el objetivo perseguido. A mi parecer, el mismo razonamiento habrá de aplicarse en lo que concierne a los límites a los principios de puerto seguro previstos en el anexo I, párrafo cuarto, de la Decisión 2000/520.

196. Pues bien, es preciso observar que no todas las versiones lingüísticas hacen mención al requisito de necesidad en la redacción del anexo I, párrafo cuarto, letra a), de la Decisión 2000/520. Así ocurre, en particular, en la versión en lengua francesa, que dispone que «l'adhésion aux principes peut être limitée par […] les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis», mientras que, por ejemplo, las versiones en lengua española, alemana e inglesa establecen que las limitaciones instauradas deben ser necesarias para alcanzar los objetivos anteriormente mencionados.

197. Sea como fuere, los elementos fácticos que invoca el órgano jurisdiccional remitente y la Comisión en sus Comunicaciones, antes citadas, demuestran claramente que, en la práctica, la aplicación de dichas limitaciones no se limita a lo estrictamente necesario para alcanzar los objetivos previstos.

198. A este respecto, cabe observar que el acceso a los datos de carácter personal transferidos del que disponen los servicios de inteligencia estadounidenses abarca de manera generalizada a todas las personas y a la totalidad de los medios de comunicación electrónica y de los datos transferidos, incluido el contenido de las comunicaciones, sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de interés general perseguido.[79]

75 — *Ibídem*, apartado 54 y jurisprudencia citada.

76 — *Ibídem*, apartado 55 y jurisprudencia citada.

77 — C-473/12, EU:C:2013:715.

78 — Apartado 32.

79 — Véase, por analogía, la sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), apartado 57 y jurisprudencia citada.

199. En efecto, el acceso de los servicios de inteligencia norteamericanos a los datos transferidos afecta, con carácter general, a todas las personas que utilizan servicios de comunicaciones electrónicas, sin exigirse que las personas afectadas representen una amenaza para la seguridad pública. [80]

200. Tal vigilancia masiva e indiferenciada es desproporcionada por naturaleza y constituye una injerencia injustificada en los derechos garantizados por los artículos 7 y 8 de la Carta.

201. Como señaló acertadamente el Parlamento en sus observaciones, puesto que el legislador de la Unión o los Estados miembros no pueden adoptar disposiciones legislativas que, en violación de la Carta, prevean una vigilancia masiva e indiferenciada, con mayor razón no puede considerarse que un país tercero garantiza un nivel de protección adecuado de los datos de carácter personal de los ciudadanos de la Unión si su reglamentación autoriza efectivamente la vigilancia y la interceptación masivas e indiscriminadas de datos de este tipo.

202. Además, es importante recalcar que el régimen de puerto seguro, definido en la Decisión 2000/520, no contiene las garantías adecuadas para evitar un acceso masivo y generalizado a los datos transferidos.

203. A este respecto, cabe observar que el Tribunal de Justicia puso de relieve en su sentencia Digital Rights Ireland y otros [81] la importancia de prever «reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta». [82] Según el Tribunal de Justicia, esa injerencia debe estar «regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario». [83] En esa misma sentencia el Tribunal de Justicia insistió en la necesidad de prever «garantías suficientes, como las que exige el artículo 8 de la Carta, que permitan asegurar una protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos». [84]

204. Pues bien, es preciso señalar que los mecanismos de arbitraje privado y la FTC, habida cuenta de su función limitada a los litigios de carácter comercial, no son mecanismos que permiten impugnar el acceso de los servicios de inteligencia estadounidenses a los datos de carácter personal transferidos desde la Unión.

205. La jurisdicción de la FTC se extiende a los actos o las prácticas desleales o fraudulentos relacionados con el comercio y, por tanto, no tiene jurisdicción respecto a la recogida y utilización de información personal con fines no comerciales. [85] El limitado ámbito de competencia de la FTC restringe el derecho de los particulares a la protección de sus datos de carácter personal. La FTC no fue creada para garantizar, como hacen las autoridades de control nacionales dentro de la Unión, la protección del derecho individual a la vida privada, sino para velar por un comercio leal y fiable para los consumidores, lo que, *de facto*, limita sus capacidades de intervención en el ámbito de la protección de datos de carácter personal. Por consiguiente, la FTC no desempeña una función comparable a la de las autoridades de control nacionales previstas en el artículo 28 de la Directiva 95/46.

80 — *Ibídem*, apartados 58 y 59.

81 — C-293/12 y C-594/12, EU:C:2014:238.

82 — Apartado 65.

83 — *Ibídem.*

84 — *Ibídem*, apartado 66.

85 — Véanse, a este respecto, el anexo II, FAQ 11, de la Decisión 2000/520, en el apartado titulado «Recurso ante la FTC», y los anexos III, V y VII de dicha Decisión.

206. Los ciudadanos de la Unión cuyos datos han sido transferidos pueden dirigirse a organismos de arbitraje especializados establecidos en Estados Unidos, como TRUSTe y BBBOnline, para solicitar que se precise si la empresa que posee sus datos de carácter personal vulnera los requisitos del régimen de autocertificación. El arbitraje privado a cargo de organismos como TRUSTe no puede abordar violaciones del derecho a la protección de datos de carácter personal cometidas por entidades o autoridades distintas de las empresas autocertificadas. Dichos organismos de arbitraje no son competentes para pronunciarse sobre la legalidad de las actuaciones de las agencias de seguridad estadounidenses.

207. Por consiguiente, ni la FTC, ni los organismos de arbitraje privados son competentes para controlar eventuales violaciones de los principios de protección de datos de carácter personal cometidos por entidades públicas, como las agencias de seguridad estadounidenses. Sin embargo, tal competencia es esencial para garantizar plenamente el derecho a la protección efectiva de dichos datos. Por consiguiente, la Comisión no podía hacer constar, al adoptar la Decisión 2000/520 y mantenerla en vigor, que todos los datos de carácter personal transferidos a Estados Unidos serían objeto de una protección adecuada del derecho consagrado en el artículo 8, apartado 3, de la Carta, esto es, que una autoridad independiente ejercería un control efectivo del cumplimiento de los requisitos de protección y seguridad de dichos datos.

208. Así pues, cabe destacar la inexistencia, en el marco del régimen de puerto seguro previsto por la Decisión 2000/520, de una autoridad independiente que pueda controlar que la aplicación de las excepciones a los principios de puerto seguro se ciña a los casos estrictamente necesarios. Pues bien, como se ha indicado, el control llevado a cabo por una autoridad independiente constituye, desde la perspectiva del Derecho de la Unión, un elemento esencial del respeto a la protección de las personas en lo que respecta al tratamiento de datos personales. [86]

209. A este respecto, conviene subrayar la función que ejercen, en el sistema de protección de datos personales en vigor dentro de la Unión, las autoridades de control nacionales en materia de control de las limitaciones previstas en el artículo 13 de la Directiva 95/46. En virtud del artículo 28, apartado 4, párrafo segundo, de dicha Directiva, «toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva». Por analogía, estimo que la alusión que figura en el anexo I, párrafo cuarto, de la Decisión 2000/520 a los límites a la aplicación de los principios de puerto seguro, debería haber ido acompañada del establecimiento de un mecanismo de control aplicado por una autoridad independiente especializada en materia de protección de datos personales.

210. La intervención de autoridades de control independientes constituye, en efecto, el núcleo del sistema europeo de protección de datos de carácter personal. Por consiguiente, es natural que la existencia de tales autoridades se considere uno de los requisitos necesarios para hacer constar la adecuación del nivel de la protección ofrecida por los países terceros. Se trata de un requisito para que no se prohíban los flujos de datos desde el territorio de los Estados miembros al territorio de países terceros con arreglo al artículo 25 de la Directiva 95/46. [87] Como se apunta en el documento de debate adoptado por el Grupo de trabajo creado por el artículo 29 de esta Directiva, en Europa existe un amplio consenso sobre que «un sistema de "supervisión externa" en forma de una autoridad independiente es una característica necesaria de todo sistema de cumplimiento de la protección de datos». [88]

86 — Sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), apartado 68 y jurisprudencia citada.

87 — Véase Poullet, Y., «L'autorité de contrôle: "vues" de Bruxelles», *Revue française d'administration publique*, nº 89, enero-marzo 1999, pp. 69 y ss., en especial, p. 71.

88 — Véase la página 7 del documento de trabajo WP 12 de la Comisión, citado en la nota 56 a pie de página.

211. Además, cabe señalar que la FISC no ofrece una tutela judicial efectiva a los ciudadanos de la Unión cuyos datos de carácter personal son transferidos a Estados Unidos. En efecto, las salvaguardias contra la vigilancia efectuada por los servicios gubernamentales en el marco del artículo 702 de la Ley de 1978 relativa a la vigilancia de los servicios de inteligencia extranjeros se aplican únicamente a los ciudadanos estadounidenses y a los extranjeros que residen legalmente y de manera permanente en Estados Unidos. Como señaló la propia Comisión, la supervisión de los programas estadounidenses de recogida de datos podría mejorarse fortaleciendo el papel de la FISC y estableciendo vías de recurso para los particulares. Estos mecanismos podrían reducir el tratamiento de los datos personales de los ciudadanos europeos que no son pertinentes con fines de seguridad nacional. [89]

212. Por otro lado, la propia Comisión indicó que no está prevista la posibilidad de que los ciudadanos de la Unión puedan acceder a sus datos, rectificarlos o suprimirlos, ni obtener reparación administrativa o judicial, en lo que respecta a la recogida y el tratamiento posterior de sus datos personales en virtud de los programas de vigilancia estadounidenses. [90]

213. Por último, conviene mencionar que las normas estadounidenses relativas a la protección de la vida privada pueden ser objeto de una aplicación diferenciada entre los ciudadanos estadounidenses y los ciudadanos extranjeros. [91]

214. De lo anterior resulta que la Decisión 2000/520 no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta. Por lo tanto, debe considerarse que esta Decisión y la aplicación que se hace de ella suponen una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, que no está regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario.

215. Por tanto, al adoptar y, posteriormente, mantener en vigor la Decisión 2000/520, la Comisión rebasó los límites que impone el respeto del principio de proporcionalidad con respecto a los artículos 7, 8 y 52, apartado 1, de la Carta. A ello se añade la constatación de una injerencia no justificada en el derecho de los ciudadanos de la Unión a una tutela judicial efectiva amparado por el artículo 47 de la Carta.

216. Por consiguiente, procede declarar la nulidad de dicha Decisión en la medida en que, habida cuenta de las violaciones de los derechos fundamentales anteriormente descritas, no cabe considerar que el régimen de puerto seguro por ella instaurado garantiza un nivel de protección adecuado de los datos de carácter personal transferidos desde la Unión a Estados Unidos con arreglo a dicho régimen.

217. Frente a tal constatación de la violación de los derechos fundamentales de los ciudadanos de la Unión, estimo que la Comisión debería haber suspendido la aplicación de la Decisión 2000/520.

218. La vigencia de dicha Decisión es de carácter indefinido. Pues bien, el caso de autos demuestra que el carácter adecuado del nivel de protección ofrecido por un país tercero puede evolucionar a lo largo del tiempo en función de la alteración de las circunstancias fácticas y jurídicas subyacentes a la adopción de dicha Decisión.

219. Procede señalar que la propia Decisión 2000/520 contiene disposiciones que prevén la posibilidad de que la Comisión adapte su contenido en función de las circunstancias.

89 — Véanse las páginas 10 y 11 de la Comunicación de la Comisión mencionada en la nota 2.

90 — Véase el punto 7.2, páginas 18 y 19, de la Comunicación de la Comisión mencionada en la nota 58.

91 — Véase, a este respecto, Kuner, C., «Foreign Nationals and Data Protection Law: A Transatlantic Analysis», *Data Protection Anno 2014: How To Restore Trust*?, Intersentia, Cambridge, 2014, p. 213, en especial, p. 216 y siguientes.

220. En este sentido, resulta del considerando 9 de dicha Decisión que «el "puerto seguro" creado por los principios y las FAQ puede precisar ser objeto de revisión teniendo en cuenta la experiencia adquirida, las novedades relativas a la protección de la vida privada en circunstancias en que la tecnología hace cada vez más fácil la transferencia y tratamiento de datos personales, y los informes de aplicación elaborados por las autoridades correspondientes».

221. Asimismo, en virtud del artículo 3, apartado 4, de dicha Decisión, «si la información recogida con arreglo a los apartados 1 a 3 demuestra que un organismo responsable del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no está ejerciendo su función, la Comisión lo notificará al Departamento de Comercio de Estados Unidos [...] y, si procede, presentará un proyecto de medidas [...] a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación».

222. Además, según el artículo 4, apartado 1, de la Decisión 2000/520, ésta «podrá adaptarse en cualquier momento de conformidad con la experiencia resultante de su aplicación o si el nivel de protección establecido por los principios y las FAQ es superado por los requisitos de la legislación estadounidense. La Comisión analizará en todo caso, basándose en la información disponible, la aplicación de la presente Decisión tres años después de su notificación a los Estados miembros e informará de cualquier resultado pertinente al Comité previsto en el artículo 31 de la Directiva 95/46, en particular de toda prueba que pueda afectar a la evaluación de que las disposiciones del artículo 1 de la presente Decisión proporcionan protección adecuada a efectos del artículo 25 de la Directiva 95/46». Con arreglo al artículo 4, apartado 2, de la Decisión 2000/520, «la Comisión presentará, si procede, proyectos de medidas de conformidad con el procedimiento establecido en el artículo 31 de la Directiva 95/46».

223. La Comisión hizo constar en sus observaciones que existe «una alta probabilidad de que la limitación de la adhesión a los principios de puerto seguro se haya efectuado de manera que ya no cumpla las exigencias estrictamente definidas de la excepción prevista en materia de seguridad nacional».[92] A este respecto, observa que «las revelaciones en cuestión ponen de manifiesto la existencia de una vigilancia indiscriminada a gran escala que no es compatible con el requisito de necesidad previsto en dicha excepción ni, en términos más generales, con el derecho a la protección de datos personales consagrado en el artículo 8 de la Carta».[93] Además, la propia Comisión señaló que «el alcance de estos programas de vigilancia, combinado con la desigualdad de trato de los ciudadanos de la Unión, pone en cuestión el nivel de protección que ofrece el régimen de puerto seguro».[94]

224. Por otro lado, la Comisión reconoció expresamente en la vista que, en el marco de la Decisión 2000/520, tal como se aplica actualmente, no existe ninguna seguridad de que vaya a garantizarse el derecho de los ciudadanos de la Unión a la protección de sus datos. No obstante, según la Comisión, dicho reconocimiento no permite declarar inválida dicha Decisión. Si bien la Comisión está de acuerdo con la afirmación según la cual debe actuar en caso de concurrir circunstancias nuevas, considera que adoptó medidas apropiadas y proporcionadas al entablar negociaciones con Estados Unidos con el fin de reformar el régimen de puerto seguro.

225. No comparto esta opinión. En efecto, entretanto, las transferencias de datos de carácter personal a Estados Unidos deben poder suspenderse a iniciativa de las autoridades de control nacionales o en respuesta a denuncias presentadas ante ellas.

92 — Apartado 44.

93 — *Ibídem.*

94 — Véase la página 5 de la Comunicación de la Comisión mencionada en la nota 2.

226. Además, estimo que en respuesta a tales constataciones la Comisión debería haber suspendido la aplicación de la Decisión 2000/520. En efecto, el objetivo de protección de datos personales perseguido por la Directiva 95/46 y por el artículo 8 de la Carta no sólo impone obligaciones a los Estados miembros, sino también a las instituciones de la Unión, como resulta del artículo 51, apartado 1, de la Carta.

227. En su evaluación del nivel de protección ofrecido por un país tercero, la Comisión no sólo debe examinar la legislación interna y los compromisos internacionales de dicho país, sino también la manera en que se garantiza en la práctica en dicho país tercero la protección de los datos de carácter personal. Si la evaluación de la práctica pone de manifiesto la existencia de disfunciones, la Comisión debe actuar en consecuencia y, en su caso, suspender y/o adaptar sin demora su Decisión.

228. Como ya se ha apuntado en las consideraciones anteriores, la obligación que recae sobre los Estados miembros consiste principalmente en garantizar, a través de sus autoridades de control nacionales, el respeto de las normas previstas por la Directiva 95/46.

229. La obligación que incumbe a la Comisión es suspender la aplicación de una decisión que ha adoptado sobre la base del artículo 25, apartado 6, de dicha Directiva en caso de constatarse la existencia de incumplimientos por parte del país tercero de que se trate, mientras mantenga con dicho país tercero negociaciones encaminadas a subsanar dichos incumplimientos.

230. Es importante recordar que una decisión adoptada por la Comisión en base a dicha disposición tiene por objeto hacer constar que un país tercero «garantiza» un nivel de protección adecuado de los datos personales que son transferidos a dicho país tercero. El término «garantiza», conjugado en presente de indicativo, implica que, para que se pueda mantener, tal decisión debe referirse a un país tercero que, tras la adopción de dicha decisión, siga garantizando un nivel de protección adecuado.

231. Según el considerando 57 de la Directiva 95/46, «cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales».

232. En virtud del artículo 25, apartado 4, de dicha Directiva, «cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate». Además, el artículo 25, apartado 5, de la Directiva 95/46 dispone que «la Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4».

233. De esta última disposición resulta que, en el sistema establecido por el artículo 25 de la Directiva 95/46, las negociaciones entabladas con un país tercero tienen por objeto subsanar la falta de adecuación del nivel de protección constatada de conformidad con el procedimiento previsto en el artículo 31, apartado 2, de dicha Directiva. En el caso de autos, la Comisión no hizo constar expresamente, de conformidad con dicho procedimiento, que el régimen de puerto seguro ya no garantizaba un nivel de protección adecuado. Sin embargo, la decisión de la Comisión de entablar negociaciones con Estados Unidos, se debió, sin duda, a que previamente consideró que el nivel de protección garantizada por dicho país tercero ya no era adecuado.

234. Si bien tenía conocimiento de la existencia de disfunciones en la aplicación de la Decisión 2000/520, la Comisión ni la suspendió ni la adaptó, lo que dio lugar a la violación continuada de los derechos fundamentales de las personas cuyos datos de carácter personal fueron y siguen siendo transferidos en el marco del régimen de puerto seguro.

235. Pues bien, el Tribunal de Justicia ya ha declarado, si bien en otro contexto, que corresponde a la Comisión velar por que se adapte la normativa a los nuevos datos. [95]

236. Tal inacción de la Comisión, que atenta directamente contra los derechos fundamentales protegidos por los artículos 7, 8 y 47 de la Carta, constituye, a mi parecer, un motivo complementario para declarar inválida la Decisión 2000/520 en el marco de la presente remisión prejudicial. [96]

III. **Conclusión**

237. A la luz de las consideraciones anteriores, procede responder a las cuestiones planteadas por la High Court del siguiente modo:

«El artículo 28 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, leído a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que la existencia de una Decisión adoptada por la Comisión Europea sobre la base del artículo 25, apartado 6, de la Directiva 95/46 no tiene por efecto impedir que una autoridad de control nacional investigue una denuncia en la que se alega que un país tercero no garantiza un nivel de protección adecuado de los datos de carácter personal y, en su caso, suspenda la transferencia de dichos datos.

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, es nula.»

95 — Véase, en este sentido, la sentencia Agrarproduktion Staebelow (C-504/04, EU:C:2006:30), apartado 40.

96 — Si bien el Tribunal de Justicia consideró en su sentencia T. Port (C-68/95, EU:C:1996:452) que «el Tratado no ha previsto la posibilidad de una remisión mediante la cual un órgano jurisdiccional nacional pueda solicitar al Tribunal de Justicia que declare con carácter prejudicial la omisión de una Institución» (apartado 53), aparentemente adoptó una postura más favorable frente a dicha posibilidad en su sentencia Ten Kate Holding Musselkanaal y otros (C-511/03, EU:C:2005:625), apartado 29.