Recopilación de la Jurisprudencia

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala)

de 6 de octubre de 2015*

«Procedimiento prejudicial — Datos personales — Protección de las personas físicas frente al tratamiento de esos datos — Carta de los Derechos Fundamentales de la Unión Europea — Artículos 7, 8 y 47 — Directiva 95/46/CE — Artículos 25 y 28 — Transferencia de datos personales a países terceros — Decisión 2000/520/CE — Transferencia de datos personales a Estados Unidos — Nivel de protección inadecuado — Validez — Reclamación de una persona física cuyos datos han sido transferidos desde la Unión Europea a Estados Unidos — Facultades de las autoridades nacionales de control»

En el asunto C-362/14,

que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la High Court (Irlanda), mediante resolución de 17 de julio de 2014, recibida en el Tribunal de Justicia el 25 de julio de 2014, en el procedimiento entre

Maximillian Schrems

y

Data Protection Commissioner,

con intervención de:

Digital Rights Ireland Ltd,

EL TRIBUNAL DE JUSTICIA (Gran Sala),

integrado por el Sr. V. Skouris, Presidente, el Sr. K. Lenaerts, Vicepresidente, el Sr. A. Tizzano, la Sra. R. Silva de Lapuerta, los Sres. T. von Danwitz (Ponente) y S. Rodin y la Sra. K. Jürimäe, Presidentes de Sala, y los Sres. A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský y D. Šváby, la Sra. M. Berger y los Sres. F. Biltgen y C. Lycourgos, Jueces;

Abogado General: Sr. Y. Bot;

Secretario: Sra. L. Hewlett, administradora principal;

habiendo considerado los escritos obrantes en autos y celebrada la vista el 24 de marzo de 2015;

consideradas las observaciones presentadas:

— en nombre del Sr. Schrems, por el Sr. N. Travers, SC, el Sr. P. O'Shea, BL, el Sr. G. Rudden, Solicitor, y el Sr. H. Hofmann, Rechtsanwalt;

* Lengua de procedimiento: inglés.

— en nombre del Data Protection Commissioner, por el Sr. P. McDermott, BL, la Sra. S. More O'Ferrall y el Sr. D. Young, Solicitors;

— en nombre de Digital Rights Ireland Ltd, por el Sr. F. Crehan, BL, y los Sres. S. McGarr y E. McGarr, Solicitors;

— en nombre de Irlanda, por los Sres. A. Joyce y B. Counihan y la Sra. E. Creedon, en calidad de agentes, asistidos por el Sr. D. Fennelly, BL;

— en nombre del Gobierno belga, por el Sr. J.-C. Halleux y la Sra. C. Pochet, en calidad de agentes;

— en nombre del Gobierno checo, por los Sres. M. Smolek y J. Vláčil, en calidad de agentes;

— en nombre del Gobierno italiano, por la Sra. G. Palmieri, en calidad de agente, asistida por el Sr. P. Gentili, avvocato dello Stato;

— en nombre del Gobierno austriaco, por los Sres. G. Hesse y G. Kunnert, en calidad de agentes;

— en nombre del Gobierno polaco, por las Sras. M. Kamejsza y M. Pawlicka y el Sr. B. Majczyna, en calidad de agentes;

— en nombre del Gobierno esloveno, por las Sras. A. Grum y V. Klemenc, en calidad de agentes;

— en nombre del Gobierno del Reino Unido, por el Sr. L. Christie y la Sra. J. Beeko, en calidad de agentes, asistidos por el Sr. J. Holmes, Barrister;

— en nombre del Parlamento Europeo, por los Sres. D. Moore y A. Caiola y la Sra. M. Pencheva, en calidad de agentes;

— en nombre de la Comisión Europea, por los Sres. B. Schima, B. Martenczuk y B. Smulders y la Sra. J. Vondung, en calidad de agentes;

— en nombre del Supervisor Europeo de Protección de Datos (SEPD), por los Sres. C. Docksey, A. Buchta y V. Pérez Asinari, en calidad de agentes;

oídas las conclusiones del Abogado General, presentadas en audiencia pública el 23 de septiembre de 2015;

dicta la siguiente

Sentencia

1 La petición de decisión prejudicial tiene por objeto la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»), de los artículos 25, apartado 6, y 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 respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), en su versión modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003 (DO L 284, p. 1) (en lo sucesivo, «Directiva 95/46»), así como, en sustancia, la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215, p. 7).

2 Esa petición se ha presentado en el marco de un litigio entre el Sr. Schrems y el Data Protection Commissioner (comisario para la protección de datos; en lo sucesivo, «comisario»), acerca de la negativa de éste a instruir una reclamación presentada por el Sr. Schrems, basada en que Facebook Ireland Ltd (en lo sucesivo, «Facebook Ireland») transfiere a Estados Unidos los datos personales de sus usuarios y los conserva en sus servidores situados en ese país.

Marco jurídico

Directiva 95/46

3 Los considerandos 2, 10, 56, 57, 60, 62 y 63 de la Directiva 95/46 están así redactados:

«(2) [...] los sistemas de tratamiento de datos están al servicio del hombre; […] deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la [vida privada], y contribuir […] al bienestar de los individuos;

[...]

(10) [...] las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[, firmado en Roma el 4 de noviembre de 1950], así como en los principios generales del Derecho comunitario; [...] por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;

[...]

(56) [...] los flujos transfronterizos de datos personales son necesarios para [el] desarrollo del comercio internacional; [...] la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; [...] el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;

(57) [...] por otra parte, [...] cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;

[...]

(60) [...] en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente Directiva, y, en particular, de su artículo 8;

[...]

(62) [...] 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;

(63) [...] dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; [...]»

4 Los artículos 1, 2, 25, 26, 28 y 31 de la Directiva 95/46 disponen:

«*Artículo 1*

Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la [vida privada], en lo que respecta al tratamiento de los datos personales.

[...]

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

a) "datos personales": toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b) "tratamiento de datos personales" ("tratamiento"): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

[...]

d) "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

[...]

Artículo 25

Principios

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

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

3. 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.

4. 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.

5. 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.

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

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

Artículo 26

Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

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

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

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

[...]

Artículo 28

Autoridad de control

1. 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.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

3. La autoridad de control dispondrá, en particular, de:

— poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control,

— poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales,

— capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o [capacidad para] poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

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. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

[...]

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

[...]

Artículo 31

[...]

2. En los casos en que se haga referencia al presente artículo, serán de aplicación los artículos 4 y 7 de la Decisión 1999/468/CE [del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión (DO L 184, p. 23)], observando lo dispuesto en su artículo 8.

[...]»

Decisión 2000/520

5 La Decisión 2000/520 fue adoptada por la Comisión con fundamento en el artículo 25, apartado 6, de la Directiva 95/46.

6 Los considerandos 2, 5 y 8 de esa Decisión están así redactados:

«(2) La Comisión puede determinar que un tercer país garantiza un nivel de protección adecuado. En tal caso, pueden transferirse datos personales desde los Estados miembros sin que sea necesaria ninguna garantía adicional.

[...]

(5) El nivel adecuado de protección de la transferencia de datos desde la Comunidad a Estados Unidos de América, reconocido por la presente Decisión, debe alcanzarse si las entidades cumplen los principios de puerto seguro para la protección de la vida privada, con objeto de proteger los datos personales transferidos de un Estado miembro a Estados Unidos de América (en lo sucesivo denominados “los principios”), así [como] las preguntas más frecuentes (en lo sucesivo denominadas “FAQ”), en las que se proporciona orientación para aplicar los principios, publicadas por el Gobierno de Estados Unidos de América con fecha 21 de julio de 2000.

Además, las entidades deben dar a conocer públicamente sus políticas de protección de la vida privada y someterse a la jurisdicción de la Federal Trade Commission (Comisión Federal de Comercio, FTC) a tenor de lo dispuesto en el artículo 5 de la Federal Trade Commission Act, en la que se prohíben actos o prácticas desleales o fraudulentas en el comercio o en relación con él, o a la jurisdicción de otros organismos públicos que garanticen el cumplimiento efectivo de los principios y su aplicación de conformidad con las FAQ.

[...]

(8) 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.»

7 A tenor de los artículos 1 a 4 de la Decisión 2000/520:

«*Artículo 1*

1. A los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, para todas las actividades cubiertas por la misma, se considerará que los principios de puerto seguro (en lo sucesivo denominados "los principios"), que figuran en el anexo I de la presente Decisión, aplicados de conformidad con la orientación que proporcionan las preguntas más frecuentes (en lo sucesivo denominadas "FAQ") publicadas por el Departamento de Comercio de Estados Unidos de América con fecha 21 de julio de 2000, que figuran en el anexo II de la presente Decisión, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a entidades establecidas en Estados Unidos de América, habida cuenta de los siguientes documentos publicados por el Departamento de Comercio de Estados Unidos de América:

a) Estudio de aplicación, que figura en el anexo III;

b) Memorando sobre daños y perjuicios por violación de la vida privada y autorizaciones explícitas en la legislación estadounidense, que figura en el anexo IV;

c) Carta de la Comisión Federal de Comercio, que figura en el anexo V;

d) Carta del Departamento estadounidense de Transporte, que figura en el anexo VI.

2. En relación con cada transferencia de datos deberán cumplirse las condiciones siguientes:

a) la entidad receptora de los datos deberá haber manifestado de forma inequívoca y pública su compromiso de cumplir los principios aplicados de conformidad con las FAQ;

b) la entidad estará sujeta a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el anexo VII de la presente Decisión, que estará facultado para investigar las quejas que se presenten y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como reparaciones para los particulares, independientemente de su país de residencia o de su nacionalidad, en caso de incumplimiento de los principios y su aplicación de conformidad con las FAQ.

3. Se considerará que la entidad que autocertifica su adhesión a los principios y su aplicación de conformidad con las FAQ cumple las condiciones mencionadas en el apartado 2 a partir de la fecha en que notifique al Departamento de Comercio de Estados Unidos de América o a su representante el compromiso a que se refiere la letra a) del apartado 2, así como la identidad del organismo público a que se refiere la letra b) del apartado 2.

Artículo 2

La presente Decisión se refiere únicamente a la adecuación de la protección proporcionada en Estados Unidos de América con arreglo a los principios y su aplicación de conformidad con las FAQ a fin de ajustarse a los requisitos del apartado 1 del artículo 25 de la Directiva 95/46/CE, y no afecta a la aplicación de las demás disposiciones de dicha Directiva [correspondientes] al tratamiento de datos personales en los Estados miembros, y en particular a su artículo 4.

Artículo 3

1. Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios y su aplicación de conformidad con las FAQ, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos siguientes:

a) el organismo público de Estados Unidos de América contemplado en el anexo VII de la presente Decisión, o un [órgano] independiente de recurso, a efectos de la letra a) del principio de aplicación, que figura en el anexo I de la presente Decisión, ha resuelto que la entidad ha vulnerado los principios y su aplicación de conformidad con las FAQ; o

b) existen grandes probabilidades de que se estén vulnerando los principios; existen razones para creer que el [órgano] 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.

La suspensión cesará en cuanto esté garantizado el cumplimiento de los principios y su aplicación de conformidad con las FAQ y las autoridades correspondientes de la Unión Europea hayan sido notificadas de ello.

2. Los Estados miembros informarán a la Comisión a la mayor brevedad de la adopción de medidas con arreglo al apartado 1.

3. Asimismo, los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no garantice dicho cumplimiento.

4. 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 de América y, si procede, presentará un proyecto de medidas con arreglo al procedimiento que establece el artículo 31 de la Directiva, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.

Artículo 4

1. La presente Decisión 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/CE, 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/CE y de toda prueba de que la presente Decisión se está aplicando de forma discriminatoria.

2. La Comisión presentará, si procede, proyectos de medidas de conformidad con el procedimiento establecido en el artículo 31 de la Directiva 95/46/CE.»

8 El anexo I de la Decisión 2000/520 tiene la siguiente redacción:

«Principios de puerto seguro (protección de la vida privada) Publicados por el Departamento de Comercio de Estados Unidos de América el 21 de julio de 2000 [...] [...] el Departamento Federal de Comercio publica el presente documento más las preguntas más frecuentes ("los principios"), o FAQ, en su calidad de autoridad competente para estimular, fomentar y desarrollar el comercio internacional. Dichos principios se formularon en consulta con la industria y la opinión pública para facilitar el comercio y las transacciones entre Estados Unidos de América y la Unión Europea. 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". Puesto que los principios se concibieron exclusivamente para lograr este objetivo concreto, resultaría impropia su utilización con otros fines. [...] La decisión de adherirse a los requisitos de "puerto seguro" es totalmente voluntaria, pero éstos pueden cumplirse de distintas maneras [...] La adhesión a estos principios puede limitarse: a) [en] cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]; 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; c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables. A fin de ser coherentes con el objetivo de mejorar la protección de la vida privada, las entidades deberán esforzarse en aplicar estos principios de manera completa y transparente, lo que incluye indicar en sus políticas de protección de la vida privada cuándo se aplicarán de manera regular las limitaciones a los principios permitidas por la anterior letra b). Por esta misma razón, cuando se permita la opción a tenor de los principios y/o de la legislación de Estados Unidos de América, se espera que las entidades opten por el mayor nivel de protección posible. [...]»

9 El anexo II de la Decisión 2000/520 está redactado como sigue:

«Preguntas más frecuentes (FAQ)

[...] FAQ nº 6 — Autocertificación

P: *¿De qué modo una entidad autocertifica su adhesión a los principios de puerto seguro?*

R: Los beneficios del puerto seguro se garantizan desde la fecha en que una entidad autocertifica ante el Departamento de Comercio, o su representante, su adhesión a los principios de conformidad con las directrices que se indican a continuación.

Para proceder a la autocertificación, las entidades pueden proporcionar al Departamento de Comercio (o a su representante) una carta firmada por uno de los responsables de la empresa en nombre de la entidad que se adhiere al puerto seguro, que contendrá cuando menos la información siguiente:

1) nombre de la entidad, señas postales y de correo electrónico, teléfono y fax;

2) descripción de las actividades de la entidad en lo relativo a la información personal recibida de la Unión Europea; y

3) descripción de su política de protección de la vida privada respecto de dicha información personal, con indicación de: a) el lugar donde puede consultarla el público; b) la fecha de entrada en vigor de dicha política; c) una oficina de contacto para la tramitación de las quejas, las solicitudes de acceso y cualquier otra cuestión relacionada con los principios de puerto seguro; d) el organismo oficial concreto con jurisdicción para entender de cualquier queja contra la entidad por posibles prácticas desleales o fraudulentas y vulneraciones de las leyes o normas sobre la vida privada (y citado en el anexo de los principios); e) el nombre de los programas de protección de la vida privada a los que esté adscrita la entidad; f) el método de verificación (por ejemplo, interna, por terceros) […]; y g) la instancia independiente de recurso que se ocupará de investigar las quejas no resueltas.

Si la entidad desea que los beneficios del puerto seguro se apliquen a la información sobre recursos humanos transferida desde la Unión Europea para usarla en el contexto de la relación laboral, puede hacerlo siempre que exista un organismo oficial con jurisdicción para entender de cualquier queja contra la entidad provocada por información sobre recursos humanos citado en el anexo de los principios. [...]

El Departamento (o su representante) llevará una lista de las entidades que presenten dichas cartas, dispensándoles por consiguiente los beneficios del puerto seguro. Asimismo, actualizará la lista con las cartas anuales y las notificaciones recibidas de conformidad con la FAQ nº 11. [...]

[...] FAQ nº 11 — Resolución de litigios y ejecución

P: *¿Cómo deberán cumplirse los requisitos de resolución de litigios impuestos por el principio de aplicación y cómo se deberá actuar ante el caso de que una entidad incumpla sistemáticamente los principios?*

R: El principio de aplicación establece los requisitos en virtud de los cuales se regulan los mecanismos de aplicación del puerto seguro. La FAQ sobre verificación (FAQ nº 7) establece la forma de reunir los requisitos de la letra b) del principio. En la presente FAQ nº 11 se abordan las letras a) y c), que requieren instancias independientes de recurso. Dichas instancias pueden adoptar formas diversas, pero siempre deben reunir los requisitos exigidos por el principio de aplicación. Las entidades podrán cumplirlos de la manera siguiente: 1) conformidad con programas de protección de la vida privada concebidos por el sector privado que incorporen los principios de puerto seguro en sus normas y cuenten con mecanismos de aplicación eficaces, similares a los descritos en el principio de aplicación; 2) conformidad con lo dispuesto por las autoridades de control establecidas legal o reglamentariamente [encargadas de] la tramitación de las quejas individuales y la resolución de litigios; o 3) compromiso de colaboración con las autoridades de protección de datos establecidas en la Comunidad Europea o sus representantes autorizados. Esta lista se ofrece a título ilustrativo y no es de ninguna manera taxativa. El sector

privado puede crear otros mecanismos de aplicación, siempre que reúnan los requisitos contemplados en el principio de aplicación y en las FAQ. Obsérvese que los requisitos del principio de aplicación se añaden al requisito expuesto en el apartado 3 de la introducción a los principios, en el sentido de que las iniciativas autorreguladoras deberán ser vinculantes con arreglo al artículo 5 de la Federal Trade Commission Act (Ley de la Comisión Federal de Comercio) o legislación similar.

Instancias de recurso

Se alentará a los consumidores a presentar cualquier queja que tengan ante la entidad correspondiente antes de acudir a las instancias de recurso independientes. [...]

[...]

Recurso ante la FTC

La FTC se ha comprometido a tramitar prioritariamente los casos presentados por los organismos de autorregulación privados, como BBBOnline y TRUSTe, y [por] los Estados miembros de la Unión Europea que aleguen el incumplimiento de los principios de puerto seguro, a fin de determinar si se ha vulnerado el artículo 5 de la Ley FTC, por la que se prohíben los actos o prácticas desleales o fraudulentos en el comercio. [...] [...]»

10 A tenor del anexo IV de la Decisión 2000/520:

«Memorando sobre [indemnización] por violación de las reglas sobre protección de la [vida privada], autorizaciones explícitas y fusiones y absorciones en el Derecho estadounidense

Este documento viene a responder a las aclaraciones solicitadas por la Comisión Europea sobre la legislación estadounidense en materia de: a) demandas de indemnización de daños y perjuicios por violación del derecho [al respeto de la vida privada], b) "autorizaciones explícitas" para la utilización de datos personales sin atenerse a los principios […] de puerto seguro y c) efectos de las fusiones y absorciones sobre las obligaciones contraídas en virtud de dichos principios.

[...]

B. Autorizaciones legales explícitas Los principios de puerto seguro recogen una excepción cuando las normas legales o reglamentarias o la jurisprudencia crean "obligaciones en contrario o autorizaciones explícitas, siempre que en el ejercicio de tal autorización la entidad acredite que el incumplimiento de dichos principios se limita a lo necesario para satisfacer los intereses legítimos que tal autorización considera deben prevalecer". 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. Con respecto a las autorizaciones explícitas, aunque estos principios tienen como finalidad salvar las diferencias entre los regímenes estadounidense y europeo de protección de la [vida privada], debemos respetar las facultades legislativas de nuestros legisladores. Esta limitada excepción del cumplimiento estricto de los principios de puerto seguro trata de encontrar un equilibrio entre los intereses legítimos de cada parte. La excepción se circunscribe a los casos en los que haya una autorización explícita. Por tanto, como cuestión de partida, la norma legal o reglamentaria o la resolución judicial en cuestión debe autorizar expresamente la conducta concreta de las entidades adheridas a los principios de puerto seguro. [Con otras palabras, la excepción no será aplicable si la ley guarda silencio]. [Además,] la excepción sólo será aplicable si la autorización explícita entra en conflicto con el cumplimiento de dichos principios. Aun en tal caso, la excepción "está limitada a lo necesario para satisfacer los intereses legítimos que tal autorización considera deben prevalecer". A modo de ejemplo, si la Ley se limita a autorizar a una empresa a proporcionar datos personales a las

autoridades públicas, la excepción no sería de aplicación. Por el contrario, si la Ley autoriza expresamente a la empresa a proporcionar información personal a organismos oficiales sin el consentimiento del interesado, esto constituiría una "autorización explícita" para actuar de modo contrario a lo establecido en los principios de puerto seguro. Por su parte, las excepciones concretas a los requisitos expresos de notificar y prestar consentimiento caerían en el ámbito de la excepción (dado que sería equivalente a una autorización explícita a revelar los datos sin notificación ni consentimiento). Por ejemplo, una ley que autorice a los médicos a proporcionar los historiales médicos de sus pacientes a las autoridades sanitarias sin el previo consentimiento de éstos puede permitir una excepción de los principios de notificación y opción. Esta autorización no permitiría al médico entregar estos mismos historiales a las organizaciones de protección de la salud o los laboratorios farmacéuticos comerciales, que quedarían fuera del ámbito de los fines autorizados por la ley y, por tanto, de la excepción.[…]. La autorización legal en cuestión puede ser una autorización "aislada" para hacer determinadas cosas con los datos personales, pero, como ilustran los ejemplos siguientes, será probablemente una excepción a una norma más amplia que prohíba obtener, utilizar o revelar datos personales. [...]»

Comunicación COM(2013) 846 final

11 El 27 de noviembre de 2013 la Comisión adoptó la Comunicación 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; en lo sucesivo, «Comunicación COM(2013) 846 final»]. Acompañaba a esa Comunicación un informe, también de fecha 27 de noviembre de 2013, que contiene las «conclusiones de los copresidentes de la Unión Europea del grupo de trabajo *ad hoc* Unión Europea-Estados Unidos sobre protección de datos personales» («Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection»). Como expone su punto 1, ese informe se había elaborado en cooperación con Estados Unidos a raíz de la revelación de la existencia en ese país de varios programas de vigilancia que comprendían la recogida y el tratamiento de información a gran escala de datos personales. Ese informe contenía, en particular, un análisis detallado del ordenamiento jurídico de Estados Unidos en lo que concierne especialmente a las bases legales que autorizan la existencia de programas de vigilancia y la recogida y el tratamiento de datos personales por autoridades estadounidenses.

12 En el punto 1 de la Comunicación COM(2013) 846 final la Comisión precisó que «los intercambios comerciales son objeto de la Decisión [2000/520]», y añadió que «dicha Decisión establece una base jurídica para la transferencia de datos personales desde la UE a las empresas establecidas en Estados Unidos que se han adherido a los principios del régimen de puerto seguro.» Además, en ese mismo punto 1 la Comisión puso énfasis en la creciente importancia de los flujos de datos personales, ligada en especial al desarrollo de la economía digital, que «ha dado lugar a un crecimiento exponencial de la cantidad, calidad, diversidad y naturaleza de las actividades de tratamiento de datos».

13 En el punto 2 de esa Comunicación la Comisión manifiesta que «ha aumentado la preocupación por el nivel de protección de los datos personales de los ciudadanos de la [Unión] transferidos a Estados Unidos en el marco del régimen de puerto seguro» y que «el carácter voluntario y declarativo del régimen ha centrado la atención en su transparencia y cumplimiento.»

14 Además, la Comisión expuso en el referido punto 2 que «las autoridades estadounidenses pueden acceder y seguir tratando los datos personales de los ciudadanos de la [Unión] enviados a Estados Unidos en el marco del régimen de puerto seguro de forma incompatible con los motivos por los que se recogieron inicialmente dichos datos en la [Unión] y con los fines por los que se transfirieron a Estados Unidos» y que «la mayoría de las empresas estadounidenses de internet relacionadas más directamente con [los] programas [de vigilancia] están certificadas en el marco del régimen de puerto seguro.»

15 En el punto 3.2 de la Comunicación COM(2013) 846 final la Comisión señaló la existencia de diversas deficiencias en la aplicación de la Decisión 2000/520. Puso de manifiesto que algunas empresas estadounidenses certificadas no respetaban los principios enunciados en el artículo 1, apartado 1, de la Decisión 2000/520 (en lo sucesivo, «principios de puerto seguro»), y que, mediante mejoras de esa Decisión, «deben subsanarse las deficiencias estructurales relacionadas con la transparencia y la aplicación y deben reforzarse los principios sustantivos del régimen de puerto seguro y la aplicación de la excepción por motivos de seguridad nacional». Por otra parte, observó que «el régimen de puerto seguro sirve asimismo de interfaz para la transferencia de los datos personales de los ciudadanos [europeos] desde la [Unión Europea] a los Estados Unidos por parte de las empresas [a] las que se pide que suministren datos a los servicios de información de los Estados Unidos en el marco de los programas de recogida de información de los Estados Unidos».

16 La Comisión concluyó en ese mismo punto 3.2 que, «habida cuenta de las deficiencias halladas, no puede mantenerse la aplicación actual del régimen de puerto seguro. Sin embargo, su derogación afectaría negativamente a los intereses de las empresas de la [Unión Europea] y de los Estados Unidos que se han adherido al mismo.». Finalmente, la Comisión añadió también en el mismo punto 3.2 que «con carácter de urgencia, la Comisión debatirá con las autoridades de Estados Unidos las deficiencias detectadas».

Comunicación COM(2013) 847 final

17 El mismo día 27 de noviembre de 2013 la Comisión adoptó la Comunicación 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; en lo sucesivo, «Comunicación COM(2013) 847 final»]. Según resulta de su punto 1, esa Comunicación se basa en particular en las informaciones recibidas por el Grupo de trabajo *ad hoc* Unión Europea-Estados Unidos y constituye la continuación de los dos informes de evaluación de la Comisión, publicados respectivamente en 2002 y en 2004.

18 El punto 1 de esa Comunicación precisa que el funcionamiento de la Decisión 2000/520 «se basa en los compromisos y la autocertificación de las entidades que lo han suscrito» y añade que «si bien la firma de estos acuerdos es voluntaria, sus reglas son vinculantes para los que los suscriben».

19 Además, del punto 2.2 de la Comunicación COM(2013) 847 final resulta que, a 26 de septiembre de 2013, estaban certificadas 3 246 entidades de numerosas industrias y sectores de servicios. Esas empresas prestaban principalmente servicios en el mercado interior de la Unión, en particular en el sector de Internet, y algunas de ellas eran empresas de la Unión que tenían filiales en Estados Unidos. Parte de esas empresas trataban los datos de sus empleados en Europa, datos que transferían a Estados Unidos para la gestión de sus recursos humanos.

20 En ese mismo punto 2.2 la Comisión puso de relieve que «cualquier fallo en la transparencia o en la aplicación por parte estadounidense [hacía] que la responsabilidad [pasara] a las autoridades de protección de datos y las empresas europeas que utilizan el sistema».

21 De los puntos 3 a 5 y 8 de la Comunicación COM(2013) 847 final se deduce que en la práctica un número elevado de empresas certificadas no respetaban, o no lo hacían plenamente, los principios de puerto seguro.

22 Además, en el punto 7 de la misma Comunicación la Comisión manifiesta que «aparentemente todas las empresas involucradas en el programa PRISM [programa de recogida de informaciones a gran escala], y que conceden a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro» y que ello «ha hecho de puerto seguro 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]». En ese sentido, la Comisión constató en el punto 7.1 de la referida Comunicación que «diversas bases legales con arreglo al ordenamiento jurídico estadounidense permiten la recogida y el tratamiento a gran escala de datos personales almacenados o tratados de otra forma por entidades basadas en Estados Unidos» y que «al tratarse de programas a gran escala, puede ocurrir que las autoridades estadounidenses accedan y procesen los datos transferidos al amparo del puerto seguro más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional, como reza la excepción prevista en la Decisión [2000/520].»

23 En el punto 7.2 de la Comunicación COM(2013) 847 final, titulado «Limitaciones y posibilidades de reparación», la Comisión puso de relieve que «las garantías previstas por la legislación estadounidense se refieren fundamentalmente a los ciudadanos estadounidenses o a los residentes legales», y que «es más, no está prevista la posibilidad de que los titulares de los datos, ya sean estadounidenses o 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».

24 Según el punto 8 de la Comunicación COM(2013) 847 final, entre las empresas certificadas se encontraban «las empresas de la red, como Google, Facebook, Microsoft, Apple o Yahoo», que «tienen centenares de millones de clientes en Europa» y transfieren datos personales a Estados Unidos para su tratamiento.

25 La Comisión concluyó en ese mismo punto 8 que «el acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos a Estados Unidos por entidades con certificación de puerto seguro suscita serias cuestiones adicionales en lo que respecta al derecho de los europeos a que sus datos sigan estando protegidos cuando se transfieren a ese país».

Litigio principal y cuestiones prejudiciales

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

27 Toda persona residente en el territorio de la Unión que desee utilizar Facebook está obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos. Los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento.

28 El 25 de junio de 2013 el Sr. Schrems presentó ante el comisario una reclamación en la que le solicitaba en sustancia que ejerciera sus competencias estatutarias, prohibiendo a Facebook Ireland transferir sus datos personales a Estados Unidos. Alegaba que el Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas. El Sr. Schrems hacía referencia en ese sentido a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la National Security Agency (en lo sucesivo, «NSA»).

29 Considerando que no estaba obligado a investigar sobre los hechos denunciados por el Sr. Schrems en su reclamación, el comisario la desestimó por infundada. Apreció en efecto que no había pruebas de que la NSA hubiera accedido a los datos personales del interesado. El comisario añadió que las imputaciones formuladas por el Sr. Schrems en su reclamación no podían ser eficazmente aducidas,

ya que cualquier cuestión referida al carácter adecuado de la protección de los datos personales en Estados Unidos debía resolverse conforme a la Decisión 2000/520, en la que la Comisión había constatado que Estados Unidos garantizaba un nivel adecuado de protección.

30 El Sr. Schrems interpuso un recurso ante la High Court contra la decisión discutida en el litigio principal. Una vez examinadas las pruebas presentadas por las partes litigantes, ese tribunal apreció que la vigilancia electrónica y la interceptación de los datos personales transferidos desde la Unión a Estados Unidos servían a finalidades necesarias e indispensables para el interés público. No obstante, el referido tribunal añadió que las revelaciones del Sr. Snowden habían demostrado que la NSA y otros organismos federales habían cometido «importantes excesos».

31 Ahora bien, según ese mismo tribunal, los ciudadanos de la Unión no disponen de ningún derecho efectivo a ser oídos. La supervisión de las acciones de los servicios de información se realiza a través de un procedimiento secreto y no contradictorio. Una vez transferidos los datos personales a Estados Unidos, la NSA y otros organismos federales, como el Federal Bureau of Investigation (FBI), pueden acceder a ellos en el contexto de la vigilancia y de las interceptaciones indiferenciadas que ejecutan a gran escala.

32 La High Court constató que el Derecho irlandés prohíbe la transferencia de datos personales fuera del territorio nacional, excepto cuando el tercer país interesado asegura un nivel de protección adecuado de la vida privada y de los derechos y libertades fundamentales. La importancia de los derechos al respeto de la vida privada y a la inviolabilidad del domicilio, protegidos por la Constitución irlandesa, exige que toda injerencia en esos derechos sea proporcionada y ajustada a las exigencias previstas por la ley.

33 Ahora bien, el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa. Para que las interceptaciones de comunicaciones electrónicas puedan ser consideradas conformes con esa Constitución, debe aportarse la prueba de que esas interceptaciones tienen carácter selectivo, de que la vigilancia de determinadas personas o de determinados grupos de personas está objetivamente justificada en interés de la seguridad nacional o de la represión de la delincuencia y de que existen garantías adecuadas y comprobables. Así pues, según la High Court, si el asunto principal se tuviera que resolver con fundamento exclusivo en el Derecho irlandés, se debería apreciar que, dada la existencia de serias dudas de que Estados Unidos garantice un nivel adecuado de protección de los datos personales, el comisario habría debido llevar a cabo una investigación sobre los hechos denunciados por el Sr. Schrems en su reclamación, y que la desestimó indebidamente.

34 No obstante, la High Court estima que este asunto atañe a la aplicación del Derecho de la Unión, en el sentido del artículo 51 de la Carta, por lo que la legalidad de la decisión discutida en el asunto principal debe apreciarse a la luz del Derecho de la Unión. Ahora bien, según ese tribunal, la Decisión 2000/520 no se ajusta a las exigencias derivadas tanto de los artículos 7 y 8 de la Carta como de los principios enunciados por el Tribunal de Justicia en la sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238). El derecho al respeto de la vida privada garantizado por el artículo 7 de la Carta y por los valores esenciales comunes a las tradiciones de los Estados miembros quedaría privado de alcance alguno si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que esas prácticas se rodeen de garantías adecuadas y comprobables.

35 La High Court observa además que, en realidad, el Sr. Schrems impugna en su recurso la licitud del régimen de «puerto seguro» establecido por la Decisión 2000/520, de la cual deriva la decisión discutida en el litigio principal. Así pues, aunque el Sr. Schrems no haya impugnado formalmente la validez de la Directiva 95/46 ni de la Decisión 2000/520, según ese tribunal se suscita la cuestión de si, en virtud del artículo 25, apartado 6, de la Directiva 95/46, el comisario estaba vinculado por la

constatación realizada por la Comisión en esa Decisión, según la cual Estados Unidos garantiza un nivel de protección adecuado, o bien si el artículo 8 de la Carta autorizaba al comisario a separarse, en su caso, de esa constatación.

36 En esas 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 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?»

Sobre las cuestiones prejudiciales

37 Con sus cuestiones prejudiciales, que es oportuno examinar conjuntamente, el tribunal remitente pregunta en sustancia si, y en qué medida, el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una decisión, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, pueda examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen, que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona afirma que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

Sobre las facultades de las autoridades nacionales de control, a las que se refiere el artículo 28 de la Directiva 95/46, ante una Decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de esa Directiva

38 Se debe recordar previamente que las disposiciones de la Directiva 95/46, en cuanto regulan el tratamiento de datos personales, que puede vulnerar las libertades fundamentales y, en particular, el derecho al respeto de la vida privada, deben ser necesariamente interpretadas a la luz de los derechos fundamentales protegidos por la Carta (véanse las sentencias Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, EU:C:2003:294, apartado 68; Google Spain y Google, C-131/12, EU:C:2014:317, apartado 68, y Ryneš, C-212/13, EU:C:2014:2428, apartado 29).

39 Del artículo 1 y de los considerandos 2 y 10 de la Directiva 95/46 se deduce que ésta se propone garantizar no sólo una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas frente al tratamiento de los datos personales, sino también un elevado nivel de protección de esas libertades y derechos fundamentales. La jurisprudencia del Tribunal de Justicia destaca la importancia tanto del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta como del derecho fundamental a la protección de los datos personales que garantiza el artículo 8 de ésta (véanse las sentencias Rijkeboer, C-553/07, EU:C:2009:293, apartado 47; Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 53, y Google Spain y Google, C-131/12, EU:C:2014:317, apartados 53, 66 y 74 y la jurisprudencia citada).

40 En lo concerniente a las facultades de las que disponen las autoridades nacionales de control en materia de transferencia de datos personales a terceros países, se ha de señalar que el artículo 28, apartado 1, de la Directiva 95/46 impone a los Estados miembros la obligación de instituir una o varias autoridades públicas encargadas del control, con toda independencia, del cumplimiento de las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de datos personales. Esa exigencia deriva también del Derecho primario de la Unión, en particular del artículo 8, apartado 3, de la Carta y del artículo 16 TFUE, apartado 2 (véanse, en ese sentido, 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).

41 La garantía de independencia de las autoridades nacionales de control pretende asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas frente al tratamiento de datos personales y debe interpretarse a la luz de dicho objetivo. Esa garantía se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades. La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales, como señala el considerando 62 de la Directiva 95/46 (véanse las sentencias Comisión/Alemania, C-518/07, EU:C:2010:125, apartado 25 y Comisión/Hungría C-288/12, EU:C:2014:237, apartado 48 y la jurisprudencia citada).

42 Para garantizar esa protección, las autoridades nacionales de control han de lograr un justo equilibrio entre el respeto del derecho fundamental a la vida privada y los intereses que exigen la libre circulación de datos personales (véanse, en ese sentido, las sentencias Comisión/Alemania, C-518/07, EU:C:2010:125, apartado 24, y Comisión/Hungría C-288/12, EU:C:2014:237, apartado 51).

43 A tal efecto, las autoridades nacionales de control disponen de una amplia gama de facultades, y éstas, enumeradas de forma no exhaustiva por el artículo 28, apartado 3, de la Directiva 95/46, constituyen otros tantos medios necesarios para el cumplimiento de sus funciones, como destaca el considerando 63 de esa Directiva. Así pues, esas autoridades disponen, en particular, de facultades de investigación, como la de recabar toda la información necesaria para el cumplimiento de su misión de control, de facultades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio.

44 Del artículo 28, apartados 1 y 6, de la Directiva 95/46 resulta ciertamente que las facultades de las autoridades nacionales de control abarcan los tratamientos de datos personales realizados en el territorio del Estado miembro de esas autoridades, de modo que éstas no disponen, con fundamento en ese artículo 28, de facultades respecto a los tratamientos de datos realizados en el territorio de un tercer país.

45 No obstante, la operación consistente en hacer transferir datos personales desde un Estado miembro a un tercer país constituye por sí misma un tratamiento de datos personales, en el sentido del artículo 2, letra b), de la Directiva 95/46 (véase, en ese sentido, la sentencia Parlamento/Consejo y Comisión, C-317/04 y C-318/04, EU:C:2006:346, apartado 56), realizado en el territorio de un Estado miembro. En efecto, esa disposición define el «tratamiento de datos personales» como «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales», y cita como ejemplo «la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos».

46 El considerando 60 de la Directiva 95/46 precisa que las transferencias de datos personales hacia terceros países sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la misma Directiva. En ese sentido, el capítulo IV de ésta, en el que figuran los artículos 25 y 26, estableció un régimen dirigido a garantizar un control por los Estados miembros de las transferencias de datos personales hacia terceros países. Es un régimen

complementario del régimen general que establece el capítulo II de la misma Directiva, que enuncia las condiciones generales de licitud de los tratamientos de datos personales (véase, en ese sentido, la sentencia Lindqvist, C-101/01, EU:C:2003:596, apartado 63).

47 Como quiera que las autoridades nacionales de control, conforme al artículo 8, apartado 3, de la Carta y al artículo 28 de la Directiva 95/46, están encargadas del control del cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales, toda autoridad nacional de control está investida, por tanto, de la competencia para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad hacia un tercer país respeta las exigencias establecidas por la Directiva 95/46.

48 Al mismo tiempo que el considerando 56 de la Directiva 95/46 reconoce que las transferencias de datos personales desde los Estados miembros a terceros países son necesarias para el desarrollo del comercio internacional, la Directiva 95/46 establece en su artículo 25, apartado 1, el principio de que esa transferencia sólo se puede realizar si esos terceros países garantizan un nivel de protección adecuado.

49 Además, el considerando 57 de la misma Directiva precisa que, cuando un tercer país no ofrezca un nivel de protección adecuado, debe prohibirse la transferencia al mismo de datos personales.

50 El artículo 25 de la Directiva 95/46 impone diversas obligaciones a los Estados miembros y a la Comisión para controlar las transferencias de datos personales a terceros países en función del nivel de protección atribuido a éstos en cada uno de esos países. De ese artículo resulta, en particular, que la constatación de que un tercer país garantiza o no un nivel de protección adecuado pueden realizarla bien los Estados miembros o bien la Comisión, como ha señalado el Abogado General en el punto 86 de sus conclusiones.

51 La Comisión puede adoptar con fundamento en el artículo 25, apartado 6, de la Directiva 95/46, una decisión que constate que un tercer país garantiza un nivel de protección adecuado. Conforme al párrafo segundo de esa disposición, los destinatarios de esa decisión son los Estados miembros, que deberán adoptar las medidas necesarias para atenerse a ella. En virtud del artículo 288 TFUE, párrafo cuarto, esa decisión tiene carácter obligatorio para todos los Estados miembros destinatarios y vincula por tanto a todos sus órganos (véanse, en ese sentido, las sentencias Albako/BALM, 249/85, EU:C:1987:245, apartado 17, y Mediaset, C-69/13, EU:C:2014:71, apartado 23), en cuanto tiene el efecto de autorizar transferencias de datos personales desde los Estados miembros al tercer país al que se refiere dicha decisión.

52 Así pues, mientras la decisión de la Comisión no haya sido declarada inválida por el Tribunal de Justicia, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden ciertamente adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciara con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado. En efecto, los actos de las instituciones de la Unión disfrutan en principio de una presunción de legalidad, y producen por tanto efectos jurídicos mientras no hayan sido revocados, anulados en virtud de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad (sentencia Comisión/Grecia, C-475/01, EU:C:2004:585, apartado 18 y la jurisprudencia citada).

53 No obstante, una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, como la Decisión 2000/520, no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud, prevista en el artículo 28, apartado 4, de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos datos. De igual forma, una decisión de esa naturaleza no puede dejar sin efecto ni limitar las facultades expresamente

reconocidas a las autoridades nacionales de control por el artículo 8, apartado 3, de la Carta y por el artículo 28 de la referida Directiva, como ha expuesto el Abogado General en los puntos 61, 93 y 116 de sus conclusiones.

54 Ni el artículo 8, apartado 3, de la Carta, ni el artículo 28 de la Directiva 95/46 excluyen del ámbito de la competencia de las autoridades nacionales designadas a ese efecto el control de las transferencias de datos personales a terceros países a los que se refiera una decisión de la Comisión en virtud del artículo 25, apartado 6, de esa Directiva.

55 En particular, el artículo 28, apartado 4, párrafo primero, de la Directiva 95/46, que dispone que las autoridades nacionales de control entenderán de la solicitud que presente «cualquier persona […] en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales», no prevé ninguna excepción en ese sentido, en el supuesto de que la Comisión hubiera adoptado una decisión en virtud del artículo 25, apartado 6, de esa Directiva.

56 Además, sería contrario al sistema establecido por la Directiva 95/46 y a la finalidad de sus artículos 25 y 28 que una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de dicha Directiva tuviera el efecto de impedir que una autoridad nacional de control examine la solicitud de una persona para la protección de sus derechos y libertades frente al tratamiento de sus datos personales que hayan sido o pudieran ser transferidos desde un Estado miembro a un tercer país al que se refiere esa decisión de la Comisión.

57 Por el contrario, el artículo 28 de la Directiva 95/46 se aplica por su propia naturaleza a todo tratamiento de datos personales. Por tanto, incluso habiendo adoptado la Comisión una decisión en virtud del artículo 25, apartado 6, de esa Directiva, las autoridades nacionales de control, a las que una persona haya presentado una solicitud de protección de sus derechos y libertades frente al tratamiento de datos personales que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por la referida Directiva.

58 Si no fuera así, las personas cuyos datos personales hayan sido o pudieran ser transferidos al tercer país considerado quedarían privadas del derecho garantizado por el artículo 8, apartados 1 y 3, de la Carta de presentar a las autoridades nacionales de control una solicitud para la protección de sus derechos fundamentales (véase, por analogía, la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 68).

59 Une solicitud, prevista en artículo 28, apartado 4, de la Directiva 95/46, mediante la que una persona cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país alegue, como en el asunto principal, que el Derecho y las prácticas de ese país no garantizan un nivel de protección adecuado, no obstante lo constatado por la Comisión en una decisión adoptada en virtud del artículo 25, apartado 6, de esa Directiva, debe entenderse como concerniente en sustancia a la compatibilidad de esa decisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

60 Hay que recordar en ese sentido la reiterada jurisprudencia del Tribunal de Justicia según la cual la Unión es una Unión de Derecho en la que todos los actos de sus instituciones están sujetos al control de su conformidad, en particular, con los Tratados, con los principios generales del Derecho y con los derechos fundamentales (véanse, en ese sentido, las sentencias Comisión y otros/Kadi, C-584/10 P, C-593/10 P y C-595/10 P, EU:C:2013:518, apartado 66; Inuit Tapiriit Kanatami y otros/Parlamento y Consejo, C-583/11 P, EU:C:2013:625, apartado 91, y Telefónica/Comisión, C-274/12 P, EU:C:2013:852, apartado 56). Por tanto, las decisiones de la Comisión adoptadas en virtud del artículo 25, apartado 6, de la Directiva 95/46 no pueden quedar excluidas de ese control.

61 Sin perjuicio de ello, el Tribunal de Justicia es exclusivamente competente para declarar la invalidez de un acto de la Unión, como una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, competencia exclusiva cuyo objeto es garantizar la seguridad jurídica preservando la aplicación uniforme del Derecho de la Unión (véanse las sentencias Melki y Abdeli, C-188/10 y C-189/10, EU:C:2010:363, apartado 54, y CIVAD, C-533/10, EU:C:2012:347, apartado 40).

62 Aunque los tribunales nacionales están ciertamente facultados para examinar la validez de un acto de la Unión, como una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, carecen sin embargo de competencia para declarar ellos mismos su invalidez (véanse, en ese sentido, las sentencias Foto-Frost, 314/85, EU:C:1987:452, apartados 15 a 20, e IATA y ELFAA, C-344/04, EU:C:2006:10, apartado 27). *A fortiori*, al examinar una solicitud, prevista en el artículo 28, apartado 4, de la Directiva 95/46, concerniente a la compatibilidad de una decisión de la Comisión, adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46, con la protección de la vida privada y de las libertades y derechos fundamentales de las personas, las autoridades nacionales de control no están habilitadas para declarar la invalidez de la referida decisión.

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

64 En el supuesto de que la referida autoridad llegue a la conclusión de que los datos alegados en apoyo de esa solicitud son infundados y la desestime por ello, la persona que haya presentado la solicitud debe disponer de recursos jurisdiccionales que le permitan impugnar esa decisión lesiva para ella ante los tribunales nacionales, según resulta del artículo 28, apartado 3, párrafo segundo, de la Directiva 95/46, entendido a la luz del artículo 47 de la Carta. Conforme a la jurisprudencia citada en los apartados 61 y 62 de la presente sentencia, esos tribunales están obligados a suspender el procedimiento y plantear al Tribunal de Justicia una cuestión prejudicial de validez si estiman que uno o varios de los motivos de invalidez alegados por las partes o, en su caso, suscitados de oficio son fundados (véase, en ese sentido, la sentencia T & L Sugars y Sidul Açúcares/Comisión, C-456/13 P, EU:C:2015:284, apartado 48 y jurisprudencia citada).

65 En el supuesto contrario, cuando esa autoridad considere fundadas las alegaciones expuestas por la persona que le haya presentado una solicitud para la protección de sus derechos y libertades frente al tratamiento de sus datos personales, la referida autoridad debe tener capacidad para comparecer en juicio, conforme al artículo 28, apartado 3, párrafo primero, tercer guion, de la Directiva 95/46, entendido a la luz del artículo 8, apartado 3, de la Carta. A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta.

66 Por las anteriores consideraciones se ha de responder a las cuestiones planteadas que el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

Sobre la validez de la Decisión 2000/520

67 Según resulta de las explicaciones del tribunal remitente sobre las cuestiones planteadas, en el asunto principal el Sr. Schrems alega que el Derecho y las prácticas de Estados Unidos no garantizan un nivel de protección adecuado, en el sentido del artículo 25 de la Directiva 95/46. Como ha señalado el Abogado General en los puntos 123 y 124 de sus conclusiones, el Sr. Schrems manifiesta dudas, que ese tribunal parece compartir en sustancia, sobre la validez de la Decisión 2000/520. Siendo así, por las consideraciones expuestas en los apartados 60 a 63 de la presente sentencia, y para dar una respuesta completa al referido tribunal, es preciso apreciar si esa Decisión se ajusta a las exigencias derivadas de dicha Directiva entendida a la luz de la Carta.

Sobre las exigencias derivadas del artículo 25, apartado 6, de la Directiva 95/46

68 Como ya se ha observado en los apartados 48 y 49 de la presente sentencia, el artículo 25, apartado 1, de la Directiva 95/46 prohíbe las transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado.

69 No obstante, a efectos del control de esas transferencias el artículo 25, apartado 6, párrafo primero, de esa Directiva dispone que la Comisión «podrá hacer constar [...] que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 [de ese artículo], a la vista de su legislación interna o de sus compromisos internacionales […], a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

70 Es cierto que ni el artículo 25, apartado 2, de la Directiva 95/46 ni ninguna otra de sus disposiciones contienen una definición del concepto de «nivel de protección adecuado». En particular, el artículo 25, apartado 2, de esa Directiva se limita a enunciar que el carácter adecuado del nivel de protección que ofrece un tercer país «se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos», y enumera sin carácter exhaustivo las circunstancias que se deben considerar en esa apreciación.

71 No obstante, según resulta de los mismos términos del artículo 25, apartado 6, de la Directiva 95/46, esta disposición exige que un tercer país «garantice» un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales. Por otro lado, también conforme a esa disposición, el carácter adecuado del nivel de protección que ofrece un tercer país se ha de apreciar «a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

72 De esa forma, el artículo 25, apartado 6, de la Directiva 95/46 da cumplimiento a la obligación expresa de protección de los datos personales, prevista en el artículo 8, apartado 1, de la Carta, y pretende asegurar la continuidad del elevado nivel de protección en caso de transferencia de datos personales a un tercer país, como ha señalado el Abogado General en el punto 139 de sus conclusiones.

73 Es verdad que el término «adecuado» que figura en el artículo 25, apartado 6, de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo, como ha manifestado el Abogado General en el punto 141 de sus conclusiones, debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta. En efecto, a falta de esa exigencia el objetivo mencionado en el anterior apartado de la presente sentencia se frustraría. Además, el elevado nivel de protección garantizado por la Directiva 95/46 entendida a la luz de la Carta se podría eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en éstos.

74 De la redacción misma del artículo 25, apartado 6, de la Directiva 95/46 resulta que es el ordenamiento jurídico del tercer país al que se refiere la decisión de la Comisión el que debe garantizar un nivel de protección adecuado. Aunque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esa Directiva entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión.

75 Siendo así, al valorar el nivel de protección ofrecido por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país, conforme al artículo 25, apartado 2, de la Directiva 95/46.

76 De igual modo, dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión. En cualquier caso esa comprobación es obligada cuando hay indicios que generan una duda en ese sentido.

77 Además, como ha expuesto el Abogado General en los puntos 134 y 135 de sus conclusiones, al apreciar la validez de una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46 también se han de tener en cuenta las circunstancias sobrevenidas después de su adopción.

78 En ese sentido es preciso observar que, dado el importante papel que cumple la protección de los datos personales en relación con el derecho fundamental al respeto de la vida privada, así como el gran número de personas cuyos derechos fundamentales pueden ser vulnerados en caso de transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, la facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda reducida, por lo que se debe ejercer un control estricto de las exigencias derivadas del artículo 25 de la Directiva 95/46, entendido a la luz de la Carta (véase por analogía la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48).

Sobre el artículo 1 de la Decisión 2000/520

79 La Comisión manifestó en el artículo 1, apartado 1, de la Decisión 2000/520 que los principios que figuran en el anexo I de ésta, aplicados de conformidad con la orientación que proporcionan las FAQ enunciadas en el anexo II de la misma Decisión, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos. De esa disposición resulta que tanto esos principios como las FAQ han sido publicados por el Departamento de Comercio estadounidense.

80 La adhesión de una entidad a los principios de puerto seguro se lleva a cabo conforme a un sistema de autocertificación, como resulta del artículo 1, apartados 2 y 3, de esa Decisión, en relación con la FAQ nº 6 que figura en el anexo II de ésta.

81 Aunque el recurso por un tercer país a un sistema de autocertificación no es por sí mismo contrario a la exigencia enunciada en el artículo 25, apartado 6, de la Directiva 95/46 de que el tercer país considerado garantice un nivel de protección adecuado «a la vista de su legislación interna o de sus compromisos internacionales», la fiabilidad de ese sistema en relación con dicha exigencia descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan

identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales.

82 En el presente asunto, en virtud del anexo I, párrafo segundo, de la Decisión 2000/50, los principios de puerto seguro «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"». Por tanto, esos principios son aplicables únicamente a las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión, sin que se exija que las autoridades públicas estadounidenses se sometan a esos principios.

83 Además, en virtud del artículo 2 de la Decisión 2000/520, ésta «se refiere únicamente a la adecuación de la protección proporcionada en Estados Unidos de América con arreglo a los principios [de puerto seguro] y su aplicación de conformidad con las FAQ a fin de ajustarse a los requisitos del apartado 1 del artículo 25 de la Directiva [95/46]», sin contener no obstante las constataciones suficientes sobre las medidas con las que Estados Unidos garantiza un nivel de protección adecuado, en el sentido del artículo 25, apartado 6, de esa Directiva, a la vista de su legislación interna o de sus compromisos internacionales.

84 A ello se añade que, conforme al anexo I, párrafo cuarto, de la Decisión 2000/520, la aplicabilidad de esos principios puede limitarse, en especial, por «las exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]», así como 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».

85 En ese sentido, en el título B de su anexo IV la Decisión 2000/520 pone de relieve, respecto a los límites a los que está sometida la aplicabilidad de los principios de puerto seguro, que «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».

86 Así pues, la Decisión 2000/520 reconoce la primacía de las «exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]» sobre los principios de puerto seguro, primacía en virtud de la cual las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias y se manifiesten por tanto incompatibles con ellas.

87 Dado el carácter general de la excepción prevista en el anexo I, párrafo cuarto, de la Decisión 2000/520, ésta hace posibles así injerencias, fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos, en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la Unión a Estados Unidos. En ese sentido, para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 33 y la jurisprudencia citada).

88 Además, la Decisión 2000/520 no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional.

89 Se añade a ello el hecho de que la Decisión 2000/520 no pone de manifiesto la existencia de una protección jurídica eficaz contra injerencias de esa naturaleza. Como ha expuesto el Abogado General en los puntos 204 a 206 de sus conclusiones, los mecanismos de arbitraje privado y los procedimientos ante la Comisión Federal de Comercio, cuyas facultades, descritas en particular en las FAQ nº 11 que figuran en el anexo II de esa Decisión, se limitan a los litigios comerciales, atañen al cumplimiento por las empresas estadounidenses de los principios de puerto seguro, y no se pueden aplicar en litigios concernientes a la legalidad de injerencias en los derechos fundamentales derivadas de medidas de origen estatal.

90 Por otro lado, el análisis precedente de la Decisión 2000/520 se confirma por la apreciación que la misma Comisión ha realizado sobre la situación resultante de la aplicación de esa Decisión. En efecto, en particular en los puntos 2 y 3.2 de la Comunicación COM(2013) 846 final y en los puntos 7.1, 7.2 y 8 de la Comunicación COM(2013) 847 final, cuyo contenido se expone respectivamente en los apartados 13 a 16, y 22, 23 y 25 de la presente sentencia, la Comisión constató que las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional. De igual modo, la Comisión apreció que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión.

91 En lo que atañe al nivel de protección de las libertades y derechos fundamentales garantizado en la Unión, según reiterada jurisprudencia del Tribunal de Justicia, una normativa de ésta que haga posible una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a ellos (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55 y la jurisprudencia citada).

92 Además, y sobre todo, la protección del derecho fundamental al respeto de la vida privada al nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 52 y la jurisprudencia citada).

93 Pues bien, no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización [véase en ese sentido, acerca de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105, p. 54), la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 57 a 61].

94 En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta (véase, en ese sentido, la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 39).

95 De igual manera, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta. En efecto, el artículo 47, párrafo primero, de ésta establece que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva, respetando las condiciones establecidas en dicho artículo. En ese sentido, la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho (véanse, en ese sentido, las sentencias Les Verts/Parlamento, 294/83, EU:C:1986:166, apartado 23; Johnston, 222/84, EU:C:1986:206, apartados 18 y 19; Heylens y otros, 222/86, EU:C:1987:442, apartado 14, y UGT-Rioja y otros, C-428/06 a C-434/06, EU:C:2008:488, apartado 80).

96 Como se ha apreciado en particular en los apartados 71, 73 y 74 de la presente sentencia, la adopción por la Comisión de una decisión en virtud del artículo 25, apartado 6, de la Directiva 95/46 requiere la constatación debidamente motivada por esa institución de que el tercer país considerado garantiza efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión, según resulta de los anteriores apartados de esta sentencia.

97 Ahora bien, se ha de observar que la Comisión no manifestó en la Decisión 2000/520 que Estados Unidos «garantiza» efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales.

98 En consecuencia, y sin que sea preciso apreciar el contenido de los principios de puerto seguro, se debe concluir que el artículo 1 de esa Decisión vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y es inválido por esa causa.

Sobre el artículo 3 de la Decisión 2000/520

99 De las consideraciones expuestas en los apartados 53, 57 y 63 de la presente sentencia se sigue que, en virtud del artículo 28 de la Directiva 95/46, entendido a la luz del artículo 8 de la Carta, las autoridades nacionales de control deben poder examinar con toda independencia cualquier solicitud de protección de los derechos y libertades de una persona frente a un tratamiento de datos personales que la afecte. Así es, en particular, cuando esa persona suscite con ocasión de su solicitud interrogantes sobre la compatibilidad de una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de esa Directiva con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

100 No obstante, el artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520 establece una regulación específica de las facultades de las que disponen las autoridades nacionales de control ante una constatación realizada por la Comisión sobre el nivel de protección adecuado, en el sentido del artículo 25 de la Directiva 95/46.

101 De esa forma, a tenor de dicha disposición las referidas autoridades, «sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva [95/46], […] podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los

principios [de la Decisión 2000/520]», de manera restrictiva, ya que sólo es posible la intervención a partir de un alto umbral de condiciones. Aunque esa disposición no enerva las facultades de esas autoridades para tomar medidas encaminadas a asegurar el cumplimiento de las disposiciones nacionales adoptadas en aplicación de esa Directiva, excluye en cambio la posibilidad de que esas autoridades tomen medidas con objeto de asegurar el cumplimiento del artículo 25 de la misma Directiva.

102 Por tanto, el artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520 debe entenderse en el sentido de que priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46, en el supuesto de que una persona alegue, con ocasión de una solicitud basada en esa disposición, factores que puedan afectar a la compatibilidad de una decisión de la Comisión, que haya constatado con fundamento en el artículo 25, apartado 6, de esa Directiva que un tercer país garantiza un nivel de protección adecuado, con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

103 Ahora bien, la facultad de ejecución atribuida a la Comisión por el legislador de la Unión en el artículo 25, apartado 6, de la Directiva 95/46 no confiere a esa institución la competencia para restringir las facultades de las autoridades nacionales de control a las que se refiere el anterior apartado de esta sentencia.

104 Siendo así, es preciso apreciar que, al adoptar el artículo 3 de la Decisión 2000/520, la Comisión excedió los límites de la competencia que le atribuye el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y que dicho artículo 3 es inválido por esa causa.

105 Toda vez que los artículos 1 y 3 de la Decisión 2000/520 son indisociables de los artículos 2 y 4 y de los anexos de ésta, su invalidez tiene el efecto de afectar a la validez de esa Decisión en su conjunto.

106 Por todas las consideraciones precedentes se debe concluir que la Decisión 2000/520 es inválida.

Costas

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

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

1) **El artículo 25, apartado 6, de la de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la**

conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

2) La Decisión 2000/520 es inválida.

Firmas