II

(Actos no legislativos)

DECISIONES

DECISIÓN DE EJECUCIÓN (UE) 2016/1250 DE LA COMISIÓN

de 12 de julio de 2016

con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.

[notificada con el número C(2016) 4176]

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Vista 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 ([1]), y en particular su artículo 25, apartado 6,

Previa consulta al Supervisor Europeo de Protección de Datos ([2]),

1. INTRODUCCIÓN

(1) La Directiva 95/46/CE establece las normas que regulan las transferencias de datos personales desde los Estados miembros a terceros países en la medida en que tales transferencias se encuentren comprendidas en el ámbito de aplicación de dicho instrumento.

(2) El artículo 1 de la Directiva 95/46/CE y los considerandos 2 y 10 de su exposición de motivos pretenden garantizar no solo una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas, en particular el derecho fundamental al respeto de la vida privada en lo que respecta al tratamiento de los datos de carácter personal, sino también un alto nivel de protección de los derechos y libertades fundamentales ([3]).

(3) La importancia del derecho fundamental al respeto de la vida privada, garantizado por el artículo 7, y el derecho fundamental a la protección de los datos de carácter personal, garantizado por el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, ha sido subrayada en la jurisprudencia del Tribunal de Justicia ([4]).

(4) De conformidad con el artículo 25, apartado 1, de la Directiva 95/46/CE, los Estados miembros solo permitirán la transferencia de datos personales a un tercer país cuando este garantice un nivel de protección adecuado y se cumplan en él, con anterioridad a dicha transferencia, las disposiciones legales que los Estados miembros aprueben en aplicación de otros preceptos de la citada Directiva. La Comisión podrá hacer constar que un tercer país garantiza un nivel de protección adecuado a la vista de su legislación interna o de los compromisos internacionales que haya suscrito a efectos de la protección de los derechos de las personas. En tal caso, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la Directiva, los Estados miembros podrán transferir datos personales sin que sea necesaria ninguna garantía adicional.

([1]) DO L 281 de 23.11.1995, p. 31.
([2]) Véase el Dictamen 4/2016 sobre el proyecto de decisión de adecuación sobre el Escudo de la privacidad UE-EE., publicado el 30 de mayo de 2016.
([3]) Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems»), EU:C:2015:650, apartado 39.
([4]) Asunto C-553/07, Rijkeboer, EU:C:2009:293, apartado 47; asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y otros, EU:C:2014:238, apartado 53; asunto C-131/12, Google Spain y Google, EU:C:2014:317, apartados 53, 66 y 74.

(5) De conformidad con el artículo 25, apartado 2, de la Directiva 95/46/CE, el nivel de protección de datos ofrecido por un tercer país se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular las normas de Derecho, generales o sectoriales, vigentes en el tercer país de que se trate.

(6) En la Decisión 2000/520/CE de la Comisión ([5]), a efectos del artículo 25, apartado 2, de la Directiva 95/46/CE, los «principios de puerto seguro para la protección de la vida privada», aplicados de conformidad con la orientación que ofrecen las preguntas más frecuentes publicadas por el Departamento de Comercio de Estados Unidos, se considera que garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a organizaciones establecidas en Estados Unidos.

(7) En sus Comunicaciones COM(2013) 846 final ([6]) y COM(2013) 847 final de 27 de noviembre de 2013 ([7]), la Comisión consideró que el fundamento del régimen de puerto seguro debía revisarse y reforzarse en el marco de una serie de factores, entre los que cabe destacar el aumento exponencial de los flujos de datos y su importancia fundamental para la economía transatlántica, el rápido crecimiento del número de empresas estadounidenses que se adhieren al régimen de puerto seguro y la nueva información sobre la escala y el alcance de determinados programas de inteligencia de EE. UU. que suscitan dudas en cuanto al nivel de protección que se puede garantizar. Asimismo, la Comisión identificó una serie de insuficiencias y deficiencias en el régimen de puerto seguro.

(8) Sobre la base de las pruebas reunidas por la Comisión, incluida la información procedente de los trabajos del Grupo de Contacto UE-EE. UU. sobre protección de la vida privada ([8]) y la información sobre programas de inteligencia estadounidenses recibida en el grupo de trabajo *ad hoc* UE-EE. UU. ([9]), la Comisión formuló 13 recomendaciones para una revisión del régimen de puerto seguro. Estas recomendaciones se centraban en fortalecer los principios sustantivos de privacidad e incrementar la transparencia de las políticas de privacidad de las empresas autocertificadas de los EE. UU.; mejorar y hacer más eficaz el control por parte de las autoridades estadounidenses del cumplimiento de los principios por las empresas; facilitar mecanismos de resolución de conflictos para las reclamaciones de los ciudadanos; y garantizar que el recurso a la excepción en ámbitos de seguridad nacional, contemplada en la Decisión 2000/520/CE se limita a lo estrictamente necesario y proporcionado.

(9) En su sentencia de 6 de octubre de 2015 en el asunto C-362/14, Maximillian Schrems/Data Protection Commissioner ([10]), el Tribunal de Justicia de la Unión Europea declaró inválida la Decisión 2000/520/CE. Sin haber examinado el contenido de los principios de puerto seguro para la protección de la vida privada, el Tribunal observó que la Comisión no había manifestado en dicha Decisión que los Estados Unidos «garantizaran» efectivamente un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales ([11]).

(10) En este sentido, el Tribunal de Justicia explicó que, si bien la expresión «nivel de protección adecuado» que figura en el artículo 25, apartado 6, de la Directiva 95/46/CE no significa un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la UE, debe entenderse en el sentido de que exige que el tercer país interesado garantice efectivamente un nivel de protección de las libertades y derechos fundamentales «sustancialmente equivalente» al garantizado en la Unión por la Directiva 95/46/CE, entendida a la luz de la Carta de los Derechos Fundamentales. Aunque los medios de los que se sirva ese tercer país para garantizar dicho nivel de protección pueden ser diferentes de los aplicados en la Unión, deben ser eficaces en la práctica ([12]).

(11) El Tribunal de Justicia criticó que la Decisión 2000/520/CE no contuviera constataciones suficientes sobre la existencia en Estados Unidos de normas 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 las entidades públicas de ese país cuando persigan fines legítimos, como la seguridad nacional, y sobre la existencia de una tutela judicial efectiva contra injerencias de esa naturaleza ([13]).

([5]) Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215 de 28.8.2000, p. 7).

([6]) Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre cómo restablecer la confianza en los flujos de datos entre la UE y EE. UU. [COM(2013) 846 final de 27 de noviembre de 2013].

([7]) Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE [COM(2013) 847 final de 27 de noviembre de 2013].

([8]) Véase, por ejemplo, Consejo de la Unión Europea: Informe final del Grupo de Contacto de Alto Nivel entre la UE y los EE. UU. sobre el intercambio de información y la protección de la vida privada y los datos personales, nota 9831/08, 28 de mayo de 2008, disponible en inglés en: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf

([9]) Informe relativo a las conclusiones de los copresidentes de la UE del grupo de trabajo *ad hoc* UE-EE. UU. sobre protección de datos, de 27 de noviembre de 2013, disponible en la siguiente dirección de Internet: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

([10]) Véase la nota 3.

([11]) Schrems, apartado 97.

([12]) Schrems, apartados 73 y 74.

([13]) Schrems, apartados 88 y 89.

(12) En 2014 la Comisión inició conversaciones con las autoridades estadounidenses a fin abordar el refuerzo del régimen de puerto seguro en consonancia con las trece recomendaciones formuladas en la Comunicación COM (2013) 847 final. A raíz de la sentencia del Tribunal de Justicia de la Unión Europea en el asunto Schrems, estas conversaciones se intensificaron con miras a adoptar una nueva decisión de adecuación que cumpliera lo dispuesto en el artículo 25 de la Directiva 95/46/CE, tal como ha sido interpretado por el Tribunal de Justicia. Los documentos que se adjuntan a la presente Decisión y que también se publicarán en el Registro Federal de Estados Unidos son el resultado de estas conversaciones. Los principios de privacidad (anexo II), así como los compromisos y declaraciones oficiales de diversas autoridades estadounidenses recogidos en los documentos de los anexos I y III a VII, constituyen el denominado «Escudo de la privacidad UE-EE. UU.».

(13) La Comisión ha analizado con detenimiento el Derecho y las prácticas vigentes en los Estados Unidos, incluidos estos compromisos y declaraciones oficiales. Sobre la base de las constataciones expuestas en los considerandos 136 a 140, la Comisión concluye que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. desde la Unión a entidades autocertificadas establecidas en los Estados Unidos.

2. **ESCUDO DE LA PRIVACIDAD UE-EE. UU.**

(14) El Escudo de la privacidad UE-EE. UU. se basa en un sistema de autocertificación por el que las entidades estadounidenses se comprometen a cumplir una serie de principios de protección de la vida privada —a saber, los principios marco del Escudo de la privacidad UE-EE. UU., incluidos los principios complementarios (en lo sucesivo denominados conjuntamente «los principios»)— establecidos por el Departamento de Comercio de Estados Unidos y enumerados en el anexo II de la presente Decisión. Se aplica tanto a los responsables como a los encargados del tratamiento (agentes), con la particularidad de que los encargados deben estar obligados contractualmente a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la UE y asistir a este último a responder a las personas físicas que ejerzan sus derechos con arreglo a los principios ([14]).

(15) Sin perjuicio del cumplimiento de las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46/CE, la presente Decisión tiene por efecto que se autoricen las transferencias de un responsable o encargado del tratamiento en la Unión a organizaciones de los Estados Unidos que hayan autocertificado su adhesión a los principios con el Departamento de Comercio y se hayan comprometido a atenerse a ellos. Los principios se aplican únicamente al tratamiento de datos personales realizado por la organización de los EE. UU. siempre que el tratamiento por dichas organizaciones no entre en el ámbito de aplicación de la legislación de la Unión ([15]). El Escudo de la privacidad no afecta a la aplicación de la legislación de la Unión que regula el tratamiento de los datos personales en los Estados miembros ([16]).

([14]) Véase el anexo II, Sec. III.10.a. En línea con la definición de la Sec. I.8.c., el responsable de la UE determinará la finalidad y medios del tratamiento de los datos personales. Por otra parte, el contrato con el agente tiene que dejar claro si se pueden realizar transferencias ulteriores (véase Sec. III.10.a.ii.2.).

([15]) Esto también se aplica por lo que respecta a los datos de recursos humanos transferidos desde la Unión en el contexto de la relación laboral. Si bien los principios subrayan la «responsabilidad primaria» del empleador de la UE (véase el anexo II, Sec. III.9.d.i.), al mismo tiempo dejan claro que su comportamiento estará cubierto por las normas aplicables en la Unión o en el Estado miembro correspondiente, no por los principios. Véase el anexo II, Sec. III.9.a.i., b.ii., c.i., d.i.

([16]) Esto se aplica también al tratamiento que tiene lugar mediante el uso de equipos situados en la Unión, pero utilizados por un organismo establecido fuera de la Unión [véase el artículo 4, apartado 1, letra c), de la Directiva 95/46/CE]. A partir del 25 de mayo de 2018, el Reglamento general de protección de datos se aplicará al tratamiento de datos de carácter personal i) en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión (incluso si el tratamiento tiene lugar en los Estados Unidos), o ii) de los interesados que estén en la Unión por parte de un responsable o un encargado del tratamiento no establecido en la Unión, cuando las actividades objeto del tratamiento estén relacionadas con: a) la oferta de bienes o servicios, con independencia de si el interesado debe efectuar un pago a dichos interesados en la Unión; o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. Véase el artículo 3, apartados 1 y 2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1).

(16) La protección que confiere a los datos personales el Escudo de la privacidad se aplica a cualquier interesado de la UE ([17]) cuyos datos hayan sido transferidos desde la Unión a organizaciones en los Estados Unidos que hayan autocertificado su adhesión a los principios ante el Departamento de Comercio.

(17) Los principios se aplicarán inmediatamente después de la certificación. Una excepción está relacionada con el principio de responsabilidad de la transferencia ulterior en los casos en que una organización que autocertifique su adhesión al Escudo de la privacidad tenga relaciones comerciales preexistentes con terceros. Dado que puede transcurrir algún tiempo para adecuar dichas relaciones comerciales a las disposiciones aplicables en virtud del principio de responsabilidad de la transferencia ulterior, la organización estará obligada a hacerlo lo antes posible, y en cualquier caso en un plazo máximo de nueve meses a partir de la autocertificación, siempre que ello tenga lugar en los dos primeros meses siguientes a la fecha en que se haga efectiva la cobertura de del Escudo de la privacidad. Durante este período transitorio, la organización deberá aplicar el principio de notificación y opción (que permite al interesado de la UE la exclusión voluntaria) y, cuando se transfieran datos personales a un tercero que actúe como agente, deberá comprobar que este ofrece al menos el mismo nivel de protección que exigen los principios ([18]). Este período transitorio proporciona un equilibrio razonable entre el respeto del derecho fundamental a la protección de datos y las necesidades legítimas de las empresas de disponer de tiempo suficiente para adaptarse al nuevo marco cuando esto también dependa de sus relaciones comerciales con terceros.

(18) Este régimen será administrado y controlado por el Departamento de Comercio en virtud de los compromisos expuestos en las declaraciones del secretario de Comercio estadounidense (anexo I de la presente Decisión). En cuanto a la aplicación de los principios de privacidad, la Federal Trade Commission (en lo sucesivo, «FTC») y el Departamento de Transporte han formulado sendas declaraciones que se recogen, respectivamente, en los anexos IV y V de la presente Decisión.

2.1. *Principios de privacidad*

(19) Como parte de su autocertificación en el marco del Escudo de la privacidad UE-EE. UU., las entidades deben comprometerse a cumplir los principios ([19]).

(20) De conformidad con el *principio de notificación*, las entidades tienen la obligación de informar a los interesados sobre una serie de elementos fundamentales relativos al tratamiento de sus datos personales (por ejemplo, el tipo de datos recopilados, la finalidad del tratamiento, los derechos de acceso y de elección, las condiciones aplicables a las transferencias ulteriores y la responsabilidad). Existen otras salvaguardias aplicables, como la obligación de las entidades de hacer públicas sus políticas de privacidad (en consonancia con los principios) y de proporcionar enlaces al sitio web del Departamento de Comercio (con información más detallada sobre la autocertificación, los derechos de los interesados y los mecanismos de recurso existentes), a la lista del Escudo de la privacidad a la que se refiere el considerando 30 y al sitio web de un proveedor adecuado de modalidades alternativas de solución de conflictos.

(21) De acuerdo con el *principio de integridad de los datos y de limitación de la finalidad*, los datos personales deberán limitarse a lo pertinente para la finalidad del tratamiento, tener fiabilidad para el uso previsto y ser exactos, completos y actuales. Una entidad no podrá tratar datos personales de manera incompatible con los fines que motivaron en un principio su recogida o que el interesado haya aprobado posteriormente. Las organizaciones deben velar por que los datos personales sean fiables para su uso previsto, exactos, completos y actualizados.

([17]) La presente Decisión es pertinente a efectos del Espacio Económico Europeo (EEE). El Acuerdo sobre el EEE prevé la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La legislación de la Unión sobre protección de datos, en particular la Directiva 95/46/CE, está cubierta por el Acuerdo EEE y ha sido incorporado en el anexo XI del mismo. El Comité Mixto del EEE debe decidir sobre la incorporación de la presente Decisión al Acuerdo EEE. Una vez que la presente Decisión se aplique a Islandia, Liechtenstein y Noruega, el Escudo de la privacidad UE-EE. UU. también se aplicará a estos tres países y las referencias en el paquete del Escudo de la privacidad a la UE y sus Estados miembros deberán interpretarse en el sentido de que incluyen a Islandia, Liechtenstein y Noruega.

([18]) Véase el anexo II, Sec. III.6.e.

([19]) El tratamiento de los datos de recursos humanos recopilados en el ámbito laboral está sujeto a normas específicas que ofrecen garantías adicionales en virtud del principio complementario sobre «datos de recursos humanos» contenido en los principios (véase el anexo II, Sec. III.9). Por ejemplo, los empresarios deben respetar las preferencias de sus trabajadores en cuanto a la vida privada mediante la restricción del acceso a los datos personales, la disociación de determinados datos o la asignación de códigos o seudónimos. Y lo que es más importante, las entidades deben cooperar y acatar las recomendaciones de las autoridades de protección de datos de la Unión por lo que respecta a dichos datos.

(22) Cuando un fin nuevo (modificado) sea sustancialmente diferente pero compatible con la finalidad original, el *principio de opción* confiere a los interesados el derecho a oponerse (exclusión voluntaria). El *principio de opción* no anula la prohibición explícita de tratamiento incompatible ([20]). En el ámbito de la mercadotecnia directa se aplican normas específicas que, por lo general, permiten al interesado ejercer el derecho de exclusión de sus datos personales «en cualquier momento» ([21]). En el caso de los datos especialmente protegidos, las entidades deben obtener, normalmente, el consentimiento expreso del interesado (participación voluntaria).

(23) De acuerdo con el *principio de integridad de los datos y de limitación de la finalidad*, la información personal podrá conservarse de forma que identifique o haga identificable a un individuo (esto es, en forma de datos personales) únicamente mientras ello sirva al fin para el que se recogió inicialmente o se autorizó posteriormente. Esta obligación no impide a las organizaciones del Escudo de la privacidad continuar tratando datos personales durante períodos más largos, pero únicamente durante el tiempo y en la medida en que dicho tratamiento sirva razonablemente a uno o varios de los siguientes fines: archivo en el interés público, periodismo, literatura y arte, investigación científica e histórica y análisis estadístico. Un período más largo de conservación de datos personales para uno de estos fines estará sujeto a las salvaguardias previstas en los principios.

(24) Con arreglo al *principio de seguridad*, las entidades que creen, mantengan, utilicen o difundan datos personales deberán tomar medidas de seguridad «razonables y adecuadas», habida cuenta de los riesgos asociados al tratamiento de los datos y la naturaleza de estos. En el supuesto de subtratamiento, las entidades deberán celebrar un contrato con el subencargado del tratamiento que garantice el mismo nivel de protección que el proporcionado por los principios de privacidad, y tomar medidas para asegurar su debida aplicación.

(25) El *principio de acceso* ([22]) reconoce el derecho de los interesados a que, sin necesidad de una justificación ni tener que abonar una tasa excesiva, una entidad les confirme si trata datos personales relacionados con ellos y les comunique los datos en cuestión en un plazo razonable. Este derecho solo podrá restringirse en circunstancias excepcionales; cualquier denegación o limitación del derecho de acceso tendrá que ser necesaria y estar debidamente justificada, y corresponderá a la entidad demostrar el cumplimiento de tales requisitos. Los interesados deberán poder corregir, modificar o suprimir información personal cuando sea inexacta o se hayan incumplido los principios de privacidad en su tratamiento. En ámbitos en que las empresas tienen más probabilidades de recurrir al tratamiento automatizado de datos personales para adoptar decisiones que afectan al individuo (por ejemplo, concesión de créditos, ofertas hipotecarias, empleo), la legislación de los EE. UU. ofrece una protección específica contra las decisiones negativas ([23]). Estos actos suelen disponer que los individuos tendrán derecho a ser informados de los motivos específicos de la decisión (por ejemplo, la denegación de un crédito), a impugnar la información incompleta o inexacta (así como el hecho de que esté basada en factores ilegales), y a buscar reparación. Estas normas ofrecen protección en el probablemente limitado número de casos de decisiones automatizadas adoptadas por la propia organización del Escudo de la privacidad ([24]). Sin embargo, dado el uso cada vez mayor del tratamiento automatizado, incluida la elaboración de perfiles, como base para tomar decisiones que afectan a los individuos en la economía digital moderna, este es un ámbito que debe ser objeto de un estrecho seguimiento. Para facilitar este seguimiento, se ha acordado con las autoridades estadounidenses que un diálogo sobre la toma de decisiones automatizada, incluido un intercambio sobre las similitudes y diferencias en el enfoque de la UE y de los EE. UU. en este sentido, formará parte de la primera revisión anual, así como las revisiones posteriores, según proceda.

([20]) Esto se aplica a todas las transferencias de datos en el marco del Escudo de la privacidad, incluso cuando estas se refieran a los datos recogidos a través de la relación laboral. Mientras que una organización estadounidense autocertificada puede, en principio, utilizar los datos sobre recursos humanos para fines distintos no relacionados con el empleo (por ejemplo, determinadas comunicaciones publicitarias), debe respetar la prohibición de tratamiento incompatible y, además, únicamente podrá hacerlo de conformidad con los *principios de notificación* y *opción*. La prohibición para la organización de los EE. UU. de tomar medidas punitivas en contra del empleado por ejercer este derecho de opción, en particular cualquier restricción de las posibilidades de empleo, garantiza que, a pesar de la relación de subordinación y dependencia inherente, el empleado esté libre de presión y, por tanto, pueda optar con auténtica libertad de elección.

([21]) Véase el anexo II, Sec. III.12.

([22]) Véase también el nuevo principio de «acceso» (anexo II, Sec. III.8).

([23]) Véase, por ejemplo, la Equal Credit Opportunity Act (ECOA, 15 U.S.C. 1691 y ss.), Fair Credit Reporting Act (FRCA, 15 USC § 1681 y ss.), o la Fair Housing Act (FHA, 42 U.S.C. 3601 y ss.).

([24]) En el contexto de una transferencia de datos personales que hayan sido recopilados en la UE, la relación contractual con el individuo (cliente) será en la mayoría de los casos con el responsable del tratamiento de la UE, que debe respetar las normas de protección de datos de la UE (y, por consiguiente, las decisiones basadas en el tratamiento automatizado serán normalmente adoptadas por este responsable). Esto incluye situaciones en las que el tratamiento sea llevado a cabo por una organización del Escudo de la privacidad que actúe como agente en nombre del responsable de la UE.

(26) En virtud del *principio de recurso, aplicación y responsabilidad* ([25]), las organizaciones participantes deberán contar con mecanismos sólidos a fin de garantizar la observancia de los demás principios de privacidad y una vía de recurso para los interesados de la UE cuyos datos personales hayan sido tratados de manera irregular, incluida una tutela judicial efectiva. Cuando una entidad ha decidido voluntariamente autocertificarse ([26]) en el marco del Escudo de la privacidad, contrae la obligación de cumplir plenamente los principios. Al objeto de poder seguir acogiéndose al Escudo de la privacidad para recibir datos personales de la Unión, la entidad deberá renovar cada año su autocertificación de adhesión al marco. Asimismo, las entidades deberán tomar medidas para verificar ([27]) que las políticas de privacidad que han publicado se ajustan a los principios y se aplican en consecuencia. Dicha verificación puede llevarse a cabo, o bien mediante un sistema de autoevaluación, que deberá constar de una serie de procedimientos internos que garanticen que los trabajadores reciban formación con respecto a la aplicación de las políticas de privacidad y que se efectúen controles objetivos periódicos del cumplimiento, o bien mediante verificaciones por terceros, cuyos métodos pueden incluir auditorías o inspecciones aleatorias. Además, la entidad deberá establecer un mecanismo de recurso eficaz para tramitar las reclamaciones presentadas en este sentido (véase también, a este respecto, el considerando 43) y estar sujeta a los poderes de investigación y aplicación de la FTC, el Departamento de Transporte u otro organismo oficial autorizado de los Estados Unidos que garantice efectivamente el cumplimiento de los principios.

(27) Se aplicarán normas especiales para las llamadas «transferencias ulteriores», es decir, las transferencias de datos personales de una organización a un tercero responsable o encargado, con independencia de si este último está establecido en los Estados Unidos o en un tercer país fuera de los Estados Unidos (y de la Unión). El objetivo de estas normas es asegurar que las protecciones garantizadas a los datos personales de los interesados de la UE no se vean afectadas, y no puedan eludirse, al transmitirlos a terceros. Esto es especialmente pertinente en las cadenas de tratamiento más complejas que son típicas de la economía digital de hoy en día.

(28) Con arreglo al *principio de responsabilidad de la transferencia ulterior* ([28]), solo se podrán transferir datos: i) con fines limitados y específicos, ii) en virtud de un contrato (o de un acuerdo similar dentro de un grupo de empresas ([29])), y iii) únicamente si dicho contrato ofrece el mismo nivel de protección que el garantizado por los principios, lo que incluye el requisito de que la aplicación de los principios se limite únicamente a la medida necesaria a efectos de la seguridad nacional, la actuación policial y otros fines de interés público ([30]). Este principio debe interpretarse en relación con el *principio de notificación* y, en el caso de una transferencia ulterior a un tercero responsable ([31]), con el *principio de opción*, según el cual los interesados deben ser informados (entre otros) acerca del tipo o la identidad de cualquier tercero receptor, la finalidad de la transferencia ulterior, así como de la opción ofrecida, y pueden oponerse (exclusión voluntaria) a las transferencias ulteriores de sus datos o, en caso de datos especialmente protegidos, han de dar su «consentimiento expreso» (participación voluntaria) a tal efecto De acuerdo con el *principio de integridad de los datos y de limitación de la finalidad*, la obligación de proporcionar el mismo nivel de protección que el garantizado por los principios presupone que el tercero solo podrá tratar los datos personales que se le transfieran de manera que no sea incompatible con los fines que motivaron en un principio su recogida o que el interesado haya aprobado posteriormente.

(29) La obligación de proporcionar el mismo nivel de protección que exigen los principios se aplica a todas las terceras partes implicadas en el tratamiento de los datos así transferidos, con independencia de su ubicación (en los EE. UU. u otro tercer país), así como cuando el tercero receptor original transfiera los datos a otro tercero receptor, por ejemplo, para fines de subtratamiento. En todos los casos, el contrato celebrado con el tercero receptor debe prever que este último notificará a la organización del Escudo de la privacidad si toma una determinación que ya no pueda cumplir esta obligación. Cuando se tome tal determinación, el tratamiento por el tercero

([25]) Véase también el principio complementario «Resolución de litigios y ejecución» (anexo II, Sec. III.11).
([26]) Véase también el principio complementario «Autocertificación» (anexo II, Sec. III.6).
([27]) Véase también el principio complementario «Verificación» (anexo II, Sec. III.7).
([28]) Véase también el principio complementario «Contratos obligatorios para las transferencias ulteriores» (anexo II, Sec. III.10).
([29]) Véase también el principio complementario «Contratos obligatorios para las transferencias ulteriores» (anexo II, Sec. III.10.b). Si bien este principio permite transferencias basadas también en instrumentos no contractuales (por ejemplo, programas intragrupo de cumplimiento y control), el texto deja claro que estos instrumentos deben «garantizar la continuidad de la protección de los datos personales de conformidad con los principios». Además, dado que la entidad autocertificada de los EE. UU. seguirá siendo responsable del cumplimiento de los principios, tendrá un fuerte incentivo para utilizar instrumentos que sean realmente eficaces en la práctica.
([30]) Véase el anexo II, Sec. I.5.
([31]) Las personas físicas no tendrán derecho de exclusión voluntaria cuando los datos personales se transfieran a un tercero que actúe como agente para desempeñar tareas en nombre y bajo las instrucciones de la organización estadounidense. Sin embargo, esto requiere un contrato con el agente, y la organización de los EE. UU. asumirá la responsabilidad de garantizar la protección prevista en virtud de los principios, mediante el ejercicio de sus competencias de instrucción.

deberá terminar o deberán tomarse otras medidas razonables y adecuadas para poner remedio a la situación ([32]). Cuando surgen problemas de cumplimiento en la cadena de tratamiento (o subtratamiento), la entidad que actúe como responsable del tratamiento de los datos personales tendrá que demostrar que no se le puede imputar el hecho que ha provocado el daño o, de lo contrario, deberá asumir la responsabilidad del mismo, tal como se especifica en el *principio de recurso, aplicación y responsabilidad*. Se aplican protecciones adicionales en caso de transferencia ulterior a un tercero ([33]).

2.2. *Transparencia, administración y supervisión del Escudo de la privacidad UE-EE. UU.*

(30) El Escudo de la privacidad UE-EE. UU. prevé mecanismos de supervisión y aplicación para verificar y garantizar que las empresas estadounidenses autocertificadas cumplen los principios y que se aborda cualquier eventual incumplimiento. Estos mecanismos se establecen en los principios (anexo II) y los compromisos asumidos por el Departamento de Comercio (anexo I), la FTC (anexo IV) y el Departamento de Transporte (anexo V).

(31) Con miras a garantizar la correcta aplicación del Escudo de la privacidad UE-EE. UU., las partes interesadas, entre ellas las personas a las que se refieren los datos, los exportadores de datos y las autoridades de protección de datos («APD») deben poder identificar a las entidades que suscriban los principios. A tal efecto, el Departamento de Comercio (o su representante) se ha comprometido a mantener y poner a disposición del público una lista de las entidades que han autocertificado su adhesión a los principios de privacidad y están sujetas a la jurisdicción de, como mínimo, una de las autoridades mencionadas en los anexos I y II de la presente Decisión (en lo sucesivo, «lista del Escudo de la privacidad») ([34]). El Departamento de Comercio actualizará dicha lista en función de las renovaciones anuales de las autocertificaciones de las entidades que se presenten y cada vez que una entidad se retire o sea eliminada del Escudo de la privacidad UE-EE. UU. También mantendrá y pondrá a disposición del público un registro autorizado de las entidades que hayan sido eliminadas de la lista, identificando en cada caso el motivo de dicha eliminación. Por último, proporcionará un enlace a la lista de expedientes de ejecución de la FTC relacionados con el Escudo de la privacidad que puede consultarse en el sitio web de la citada institución.

(32) El Departamento de Comercio publicará tanto la lista del Escudo de la privacidad como las renovaciones de las autocertificaciones en un sitio web específico. Las entidades autocertificadas deberán a su vez facilitar la dirección web de la lista del Escudo de la privacidad. Además, si la política de privacidad de la entidad se encuentra publicada en Internet, deberá incluir un hipervínculo al sitio web del Escudo de la privacidad y otro al sitio web o al formulario de presentación de reclamaciones de la instancia independiente de recurso que se ocupará de investigar las reclamaciones pendientes de resolución. El Departamento de Comercio verificará sistemáticamente, en el marco de la certificación y recertificación de una entidad, que sus políticas en materia de privacidad se ajusten a los principios.

(33) Las entidades que incumplan de forma sistemática los principios serán eliminadas de la lista del Escudo de la privacidad y deberán devolver o suprimir los datos personales que hayan obtenido en el marco de dicho régimen. En los demás casos de eliminación de la lista, como la retirada voluntaria de la participación o la falta de recertificación, la entidad podrá conservar tales datos si reafirma cada año ante el Departamento de Comercio su compromiso de continuar aplicando los principios o brinda una protección adecuada de los datos personales por otros medios autorizados (por ejemplo, mediante un contrato que refleje fielmente las disposiciones de las cláusulas contractuales tipo pertinentes aprobadas por la Comisión). En este caso, la entidad tendrá que designar un punto de contacto en su seno para todas las cuestiones relacionadas con el Escudo de la privacidad.

(34) El Departamento de Comercio seguirá de cerca a las entidades que hayan dejado de ser miembro del Escudo de la privacidad UE-EE. UU., bien por haberse retirado voluntariamente o porque ha expirado su certificación, para verificar si van a devolver, borrar o conservar ([35]) los datos personales recibidos anteriormente en virtud del

([32]) La situación es diferente según se trate de un responsable o un encargado del tratamiento (agente). En la primera hipótesis, el contrato celebrado con el tercero debe disponer que este detenga el tratamiento o tome otras medidas razonables y adecuadas para poner remedio a la situación. En la segunda hipótesis, corresponde a la organización del Escudo de la privacidad —como responsable del tratamiento bajo cuyas instrucciones opera el agente— tomar estas medidas.

([33]) En tal caso, la organización estadounidense también deberá tomar medidas adecuadas y razonables i) para garantizar que el agente efectivamente trate los datos personales transferidos de manera coherente con las obligaciones de la organización con arreglo a los principios, y ii) para detener y remediar el tratamiento no autorizado, previa notificación.

([34]) Puede consultarse información sobre la gestión de la lista del Escudo de la privacidad en los anexos I y II (Sec. I.3, Sec. I.4, III.6.d, y Sec. III.11.g).

([35]) Véase, por ejemplo, anexo II, Sec. I.3, Sec. III.6.f y Sec. III.11.g.i.

marco. Si conservan estos datos, las entidades están obligadas a seguirles aplicando los principios. En los casos en que el Departamento de Comercio haya eliminado del marco a entidades debido a un persistente incumplimiento de los principios, se asegurará de que estas entidades devuelvan o supriman los datos personales recibidos con arreglo al marco.

(35) Cuando una entidad abandona el Escudo de la privacidad UE-EE. UU. por cualquier motivo, debe retirar todas las declaraciones públicas que den a entender que sigue participando en el Escudo o que disfruta de las ventajas que este ofrece, y, en particular, toda referencia a dicho Escudo que aparezca en su política de privacidad publicada. El Departamento de Comercio buscará y perseguirá las falsas declaraciones de participación en el marco, en particular por antiguos miembros ([36]). Cualquier deficiencia de la información dada a conocer al público por una entidad en lo referente a su adhesión a los principios en forma de declaraciones o prácticas engañosas podrá denunciarse ante la FTC, el Departamento de Transporte u otras autoridades estadounidenses competentes con funciones coercitivas; las deficiencias de la información proporcionada al Departamento de Comercio serán perseguibles en virtud de la False Statements Act (Ley de Declaraciones Falsas), codificada en el título 18, artículo 1001, del United States Code (Código de los Estados Unidos; en lo sucesivo, «USC») ([37]).

(36) El Departamento de Comercio supervisará de oficio cualquier afirmación fraudulenta de participación en el Escudo de la privacidad o el uso indebido de la marca de certificación del Escudo, y las APD podrán solicitar el examen de las entidades en un punto de contacto designado a tal efecto en el Departamento. Cuando una entidad se haya retirado del Escudo, no renueve su autocertificación o sea eliminada de la lista del Escudo, el Departamento de Comercio comprobará constantemente que dicha entidad haya suprimido de su política de privacidad toda referencia al Escudo que dé a entender que sigue adherida al mismo y, en caso de persistir en las afirmaciones fraudulentas, remitirá el asunto a la FTC, al Departamento de Transporte o a cualquier otra instancia competente con vistas a la posible adopción de medidas coercitivas. Asimismo, enviará cuestionarios a las entidades cuyas autocertificaciones caduquen y a aquellas que se hayan retirado voluntariamente del Escudo, a fin de confirmar si la entidad devolverá o suprimirá los datos personales que recibió durante su participación en el Escudo o si seguirá aplicando los principios de privacidad a dichos datos y, en este último supuesto, averiguar qué miembro de la entidad servirá de punto de contacto permanente para atender las preguntas relacionadas con el Escudo.

(37) De manera permanente, el Departamento de Comercio llevará a cabo de oficio revisiones ([38]) del cumplimiento de las entidades autocertificadas, en particular mediante el envío de cuestionarios detallados. También llevará a cabo de forma sistemática revisiones cuando haya recibido una denuncia específica (no frívola), cuando una organización no responda satisfactoriamente a sus solicitudes de información, o cuando existan pruebas creíbles que sugieran que una organización puede no estar cumpliendo los principios. En su caso, el Departamento de Comercio también consultará con las APD sobre dichas revisiones del cumplimiento.

2.3. *Mecanismos de recurso y tramitación y ejecución de reclamaciones*

(38) El Escudo de la privacidad UE-EE. UU., a través del *principio de recurso, aplicación y responsabilidad*, obliga a las entidades a prever mecanismos de recurso a los particulares afectados por el incumplimiento y, por tanto, la posibilidad para los interesados de la UE de presentar reclamaciones en relación con el incumplimiento por parte de entidades autocertificadas de EE. UU. y que se resuelvan estas reclamaciones, en su caso mediante una resolución que conceda un recurso efectivo.

(39) Como parte de su autocertificación, las entidades deberán cumplir los requisitos del principio de recurso, aplicación y responsabilidad facilitando mecanismos de recurso independientes, eficaces y disponibles rápidamente, mediante los cuales puedan investigarse y resolverse rápidamente las reclamaciones y controversias sin coste alguno para el interesado.

(40) Las entidades podrán recurrir a mecanismos independientes en la Unión o en los Estados Unidos. Esto incluye la posibilidad de comprometerse voluntariamente a cooperar con las autoridades de protección de datos de la UE. No obstante, no existe dicha opción si las organizaciones tratan datos sobre recursos humanos, dado que la

([36]) Véase el anexo I, sección «Buscar y abordar las falsas afirmaciones de participación».
([37]) Véase el anexo II, Sec. III.6.h y Sec. III.11.f.
([38]) Véase el anexo I.

cooperación con las APD es en estos casos obligatoria. Otras opciones son la resolución alternativa de litigios (RAL) independiente o *programas de privacidad* desarrollados por el sector privado que incorporen los principios en sus normas. Estos últimos deberán incluir mecanismos de ejecución eficaces de conformidad con los requisitos del principio de recurso, aplicación y responsabilidad. Las entidades están obligadas a subsanar los problemas de incumplimiento. También deberán especificar que están sujetas a los poderes de investigación y ejecución de la FTC, el Departamento de Transporte o cualquier otro organismo oficial autorizado de los Estados Unidos.

(41) Por consiguiente, el marco del Escudo de la privacidad facilita a los interesados una serie de posibilidades para hacer valer sus derechos, presentar reclamaciones en relación con el incumplimiento por parte de entidades autocertificadas de los Estados Unidos, y que se resuelvan sus reclamaciones, en su caso mediante una decisión que conceda la tutela judicial efectiva. Los particulares pueden presentar una reclamación directamente a una organización, a un órgano de resolución de litigios independiente designado por la organización, a las autoridades nacionales de protección de datos o a la FTC.

(42) En caso de que sus reclamaciones no sean resueltas por alguno de estos mecanismos de recurso o de ejecución, los particulares tienen derecho a invocar el arbitraje vinculante en el marco del panel del Escudo de la privacidad (anexo 1 del anexo II de la presente Decisión). Excepto por lo que se refiere al panel arbitral, que exige que se agoten ciertos recursos antes de que pueda recurrirse a él, los particulares tienen la posibilidad de ejercer alguna o todas las vías de recurso de su elección, y no están obligados a elegir un mecanismo antes que otro ni a seguir una secuencia específica. Sin embargo, hay un cierto orden lógico que es aconsejable seguir, como se indica a continuación.

(43) En primer lugar, los interesados de la UE podrán perseguir los casos de incumplimiento de los principios de privacidad a través de contactos directos con la *empresa estadounidense autocertificada*. Al objeto de facilitar la resolución, la entidad deberá establecer un mecanismo de recurso eficaz para tramitar las reclamaciones presentadas. La política de privacidad de una entidad ha de indicar por tanto claramente un punto de contacto, ya sea interno o externo, que se encargue de tramitar las reclamaciones (incluida cualquier instancia pertinente de la Unión que pueda atender las consultas o reclamaciones) e informar asimismo de los mecanismos independientes de tramitación de reclamaciones.

(44) Cuando reciba una reclamación de un individuo, directamente de este o a través del Departamento de Comercio tras haber sido remitida por una APD, la entidad deberá responder al interesado de la UE en un plazo de 45 días. En su respuesta deberá incluir una apreciación del fondo de la reclamación e información sobre el modo en que la entidad subsanará el problema. Asimismo, las entidades tienen la obligación de responder sin demora a las consultas y demás solicitudes de información del Departamento de Comercio o de una APD ([39]) (en el supuesto de que la entidad se haya comprometido a cooperar con la APD), con respecto a su adhesión a los principios. Las entidades deben conservar registros sobre la aplicación de sus políticas de privacidad y ponerlos a disposición cuando se soliciten ante una instancia independiente de recurso o la FTC (u otra autoridad estadounidense competente en materia de investigación de prácticas desleales y fraudulentas) en el marco de investigaciones o reclamaciones por incumplimiento.

(45) En segundo lugar, las personas también pueden reclamar directamente a un *organismo independiente de solución de conflictos* (en los Estados Unidos o en la Unión) designado por una entidad que se encargue de investigar y resolver las reclamaciones individuales (salvo que carezcan manifiestamente de fundamento o propósito) y ofrecer a la persona una vía de recurso adecuada y gratuita. Las sanciones y medidas correctoras impuestas por dicho organismo han de ser lo suficientemente rigurosas para garantizar el cumplimiento de los principios por parte de las entidades, y deben prever la anulación o corrección por estas últimas de los efectos del incumplimiento y, según el caso, la suspensión del tratamiento de los datos personales en cuestión o la supresión de estos, así como la publicidad de los casos de incumplimiento detectados. Los organismos independientes de solución de conflictos designados por una entidad tendrán que incluir en sus sitios web públicos información pertinente sobre el Escudo de la privacidad UE-EE. UU. y los servicios que prestan en este sentido. Deberán publicar un informe anual que contenga estadísticas agregadas sobre estos servicios ([40]).

([39]) Es la autoridad encargada de la tramitación que haya sido designada por el panel de APD previsto en el principio complementario sobre «la función de las autoridades de protección de datos» (anexo II, Sec. III.5).

([40]) Dicho informe anual expondrá: 1) el número total de reclamaciones relacionadas con el Escudo de la privacidad que se hayan recibido durante el año a que se refiere el informe; 2) la naturaleza de las reclamaciones recibidas; 3) medidas de la calidad de la solución de conflictos, como, por ejemplo, la duración de la tramitación de las reclamaciones; y 4) los resultados de las reclamaciones recibidas, a saber, el número y tipo de medidas correctoras o sanciones impuestas.

(46) Como parte de sus procedimientos de revisión del cumplimiento, el Departamento de Comercio comprobará que las empresas estadounidenses autocertificadas se hayan registrado efectivamente en las instancias independientes de recurso en las que afirman haberlo hecho. Tanto las entidades como las instancias independientes de recurso competentes deben responder sin demora a las consultas y solicitudes de información formuladas por el Departamento de Comercio con respecto al Escudo de la privacidad.

(47) Cuando una entidad incumpla la decisión de un organismo de solución de conflictos o de autorregulación, este último deberá notificar dicho incumplimiento al Departamento de Comercio y a la FTC (o a otra autoridad estadounidense competente en materia de investigación de prácticas desleales y fraudulentas), o a un órgano jurisdiccional competente ([41]). Si una organización se niega a cumplir una decisión definitiva de un organismo de autorregulación, un organismo independiente de solución de conflictos o un organismo público competente en materia de privacidad, o cuando dicho organismo determine que una organización a menudo no cumple los principios, esto se considerará como un incumplimiento sistemático con el resultado de que el Departamento de Comercio, tras dar a la organización que haya incumplido un preaviso de 30 días y una oportunidad para responder, eliminará a dicha organización de la lista ([42]). Si, una vez suprimida de la lista, la organización sigue alegando su certificación al Escudo de la privacidad, el Departamento la remitirá a la FTC u otro organismo con funciones coercitivas ([43]).

(48) En tercer lugar, las personas también pueden presentar sus reclamaciones a una *autoridad nacional de protección de datos*. Las entidades están obligadas a cooperar en la investigación y la resolución de una reclamación por una APD por lo que respecta al tratamiento de datos de recursos humanos recogidos en el contexto de una relación laboral o cuando la entidad respectiva se haya sometido voluntariamente a la supervisión por parte de las APD. En concreto, las entidades deben responder a las solicitudes de información, adecuarse a las recomendaciones proporcionadas por la APD, inclusive sobre medidas correctoras o medidas compensatorias, y aportar a la APD la confirmación por escrito de que se han adoptado dichas medidas.

(49) Las APD proporcionarán asesoramiento a través de un panel informal de APD a escala de la Unión ([44]), que permitirá seguir un enfoque armonizado y coherente por lo que respecta a una reclamación concreta. El asesoramiento se proporcionará una vez que las partes en litigio hayan tenido una oportunidad razonable de formular las observaciones y aportar las pruebas que deseen. El panel prestará asesoramiento tan pronto como lo permita el respeto de las garantías procesales y, por regla general, en los sesenta días siguientes a la recepción de la reclamación. Si una entidad no ha acatado las recomendaciones de la APD en un plazo de veinticinco días desde la prestación de asesoramiento, y no ha dado una explicación satisfactoria de la demora, el panel notificará su intención, o bien de trasladar el asunto a la FTC (o a otro servicio estadounidense competente con funciones coercitivas), o bien de resolver que se ha vulnerado gravemente el compromiso de cooperación. El primer supuesto podría dar lugar a la adopción de medidas coercitivas en virtud del artículo 5 de la FTC Act (o de otro acto legislativo similar). En el segundo supuesto, el panel informará al Departamento de Comercio, que considerará que la negativa de la entidad constituye un incumplimiento sistemático del asesoramiento del panel de la APD y la eliminará de la lista del Escudo de la privacidad.

(50) Si la APD a la que se ha dirigido la reclamación no toma medidas al respecto o estas son insuficientes, el reclamante tendrá la posibilidad de impugnar esta falta de medidas ante los órganos jurisdiccionales nacionales del Estado miembro de que se trate.

(51) Los particulares también podrán presentar reclamaciones a las APD, incluso cuando el panel de la APD no haya sido designado como organismo de resolución de litigios de una entidad. En estos casos, la APD podrá remitir dichas reclamaciones al Departamento de Comercio o a la FTC. Con el fin de facilitar y aumentar la cooperación en asuntos relativos a reclamaciones individuales e incumplimiento por parte de las organizaciones del Escudo de la privacidad, el Departamento de Comercio establecerá un punto de contacto específico que servirá de enlace y ayudará a las ADP con las indagaciones sobre el cumplimiento de los principios por parte de una entidad ([45]). Asimismo, la FTC se ha comprometido a establecer un punto de contacto específico ([46]) y a prestar asistencia en las investigaciones de las APD, en virtud de la US SAFE WEB Act (Ley estadounidense de seguridad en internet) ([47]).

([41]) Véase el anexo II, Sec. III.11.e.
([42]) Véase el anexo II, Sec. III.11.g, en particular los puntos ii) y iii).
([43]) Véase el anexo I, sección «Buscar y abordar las falsas afirmaciones de participación».
([44]) El reglamento interno del panel informal de la APD debe establecerse por las APD basándose en su competencia para organizar su trabajo y cooperar entre sí.
([45]) Véase el anexo I, secciones sobre «Aumentar la cooperación con las APD» y «Facilitar la resolución de reclamaciones por incumplimiento» y el anexo II, Sec. II.7.e.
([46]) Véase el anexo IV, p. 6.
([47]) *Ibídem*.

(52) En cuarto lugar, el Departamento de Comercio se ha comprometido a recibir, examinar y hacer todo lo posible por resolver las reclamaciones relativas al incumplimiento de los principios. A tal efecto, facilita a las APD procedimientos especiales para remitir las reclamaciones a un punto de contacto específico, realizar un seguimiento de las mismas y colaborar con las empresas interesadas para facilitar su resolución. Con objeto de agilizar la tramitación de las reclamaciones individuales, el punto de contacto tratará directamente con la APD pertinente las cuestiones relacionadas con el cumplimiento y, en particular, la pondrá al tanto del estado de las reclamaciones en un plazo no superior a los noventa días siguientes a la remisión de estas. Esto permitirá a los interesados presentar las reclamaciones por incumplimiento de empresas estadounidenses autocertificadas directamente ante su APD nacional y que esta las remita al Departamento de Comercio, autoridad estadounidense encargada de la administración del Escudo de la privacidad UE-EE. UU. Dicho Departamento se ha comprometido asimismo a presentar, en el marco de la revisión anual del funcionamiento del Escudo, un informe que analice de forma agregada las reclamaciones que recibe cada año ([48]).

(53) Cuando, a partir de sus verificaciones de oficio, de las reclamaciones recibidas o de cualquier otra información, el Departamento de Comercio concluya que una entidad ha incumplido de forma sistemática los principios, procederá a eliminarla de la lista del Escudo de la privacidad. Se considerará incumplimiento sistemático la negativa a cumplir las decisiones definitivas de un organismo de autorregulación, un organismo independiente de solución de conflictos o un organismo público competente en materia de privacidad, incluidas las APD.

(54) En quinto lugar, una entidad del Escudo de la privacidad debe estar sujeta a los poderes de investigación y ejecución de las autoridades estadounidenses, en particular la *Comisión Federal de Comercio* ([49]), que garantizará de manera eficaz el respeto de los principios. La Comisión Federal de Comercio examinará con carácter prioritario los casos de incumplimiento de los principios remitidos por organismos independientes de solución de conflictos o de autorregulación, el Departamento de Comercio y las APD (de oficio, o previa reclamación) al objeto de determinar si se ha vulnerado el artículo 5 de la FTC Act (Ley de la Comisión Federal de Comercio) ([50]). La FTC se ha comprometido a crear un procedimiento normalizado de remisión, a designar un punto de contacto en su seno al que las APD puedan remitir los asuntos pertinentes y a intercambiar información sobre las remisiones. Asimismo, admitirá reclamaciones directamente de particulares y emprenderá investigaciones de oficio en el marco del Escudo de la privacidad, en particular como parte de sus investigaciones más amplias de cuestiones relacionadas con la privacidad.

(55) La FTC puede exigir el cumplimiento mediante órdenes administrativas («autos de avenencia») y supervisar de manera sistemática el acatamiento de las mismas. Si las entidades incumplen sus obligaciones, la FTC podrá remitir el asunto al órgano jurisdiccional competente con el fin de solicitar multas administrativas y otras soluciones jurídicas, incluida la indemnización por cualquier perjuicio ocasionado por la conducta infractora. Por otra parte, la FTC podrá acudir directamente a un tribunal federal para solicitar medidas cautelares preliminares o permanentes u otro tipo de soluciones jurídicas. Los autos de avenencia (*consent orders*) dictados a una entidad perteneciente al Escudo de la privacidad contendrán disposiciones de autoinformación ([51]) y las entidades tendrán que hacer públicas todas las secciones pertinentes relacionadas con el Escudo de todo informe de cumplimiento o evaluación presentado a la FTC. Por último, la FTC mantendrá una lista en línea de las empresas que hayan sido objeto de una resolución de la FTC o de un órgano jurisdiccional en asuntos relativos al Escudo.

(56) En sexto lugar, como instancia de último recurso en el supuesto de que ninguna de las anteriores vías disponibles haya resuelto de manera satisfactoria la reclamación de un particular, el interesado de la UE podrá solicitar un procedimiento de arbitraje vinculante al «*panel del Escudo de la privacidad*». Las entidades deben informar a los particulares sobre la posibilidad, en ciertas condiciones, de invocar el arbitraje vinculante y están obligadas a responder cuando un particular haya recurrido a esta opción, notificándolo a la entidad de que se trate ([52]).

([48]) Véase el anexo I, sección «Facilitar la resolución de reclamaciones por incumplimiento».

([49]) Una entidad del Escudo de la privacidad tiene que declarar públicamente su compromiso de cumplir los principios, revelar públicamente sus políticas de protección de la privacidad de conformidad con estos principios, y aplicarlos plenamente. El incumplimiento podrá perseguirse conforme a la sección 5 de la Ley de la FTC que prohíbe actos desleales y engañosos en el comercio o que o afecten al comercio.

([50]) Según información de la FTC, no tiene competencias para llevar a cabo inspecciones sobre el terreno en el ámbito de la protección de la privacidad. No obstante, tiene la facultad de obligar a las entidades a presentar documentos y declaraciones de testigos (véase la sección 20 de la Ley de la FTC) y podrá utilizar el sistema judicial para hacer cumplir tales órdenes en caso de incumplimiento.

([51]) Las resoluciones de la FTC o de órganos jurisdiccionales pueden exigir a las empresas que introduzcan programas de protección de la vida privada y que presenten periódicamente a la FTC informes de cumplimiento o evaluaciones de terceros independientes sobre dichos programas.

([52]) Véase el anexo II, Sec. II.1.xi y III.7.c.

(57) Este panel arbitral estará integrado por un grupo mínimo de veinte árbitros designados por el Departamento de Comercio y la Comisión en función de su independencia, su integridad y su experiencia en el Derecho estadounidense en materia de privacidad y el Derecho de la Unión en materia de protección de datos. En cada litigio particular, las partes seleccionarán de este panel un grupo compuesto por uno o tres ([53]) árbitros. El procedimiento se regirá por un reglamento estándar de arbitraje acordado entre el Departamento de Comercio y la Comisión. Estas normas completarán el marco ya concluido que contiene varios elementos que refuerzan la accesibilidad de este mecanismo para los interesados de la UE: i) en la preparación de una alegación ante el panel, el interesado podrá ser asistido por su APD nacional; ii) si bien el arbitraje se celebrará en los Estados Unidos, los interesados de la UE podrán participar, si lo desean, por videoconferencia o conferencia telefónica sin coste alguno para ellos; iii) si bien el arbitraje se desarrollará en inglés, previa solicitud motivada, normalmente ([54]) se proporcionará un servicio de traducción e interpretación en las audiencias arbitrales sin coste para el interesado; iv) por último, si bien cada parte deberá pagar los honorarios de sus respectivos abogados, en caso de disponer de representación letrada ante el panel, el Departamento de Comercio creará un fondo financiado con cuotas anuales pagadas por las entidades pertenecientes al Escudo de la privacidad, que cubrirá los gastos subvencionables del procedimiento de arbitraje hasta los importes máximos que determinen las autoridades estadounidenses en consulta con la Comisión.

(58) El panel del Escudo de la privacidad estará facultado para imponer la «compensación equitativa individualizada de carácter no monetario» ([55]) necesaria para subsanar el incumplimiento de los principios. Si bien dicho panel tendrá en cuenta en su apreciación las soluciones jurídicas que ya se hayan obtenido por las demás vías de recurso del Escudo de la privacidad, las personas afectadas podrán recurrir de todos modos al arbitraje si consideran que tales soluciones son insuficientes. Esto permitirá a los interesados de la UE solicitar un procedimiento de arbitraje en todos aquellos casos en los que la actuación u omisión de las autoridades estadounidenses competentes (por ejemplo, la FTC) no haya resuelto de manera satisfactoria sus reclamaciones. No se podrá solicitar un procedimiento arbitraje en aquellos casos en que la APD esté facultada jurídicamente para resolver la reclamación en cuestión con respecto a la empresa estadounidense autocertificada, en particular cuando la entidad tenga la obligación de cooperar y de acatar las recomendaciones formuladas por la APD en relación con el tratamiento de los datos de recursos humanos recopilados en el ámbito laboral o se haya comprometido voluntariamente a hacerlo. En virtud de la Federal Arbitration Act (Ley Federal de Arbitraje), las personas físicas pueden ejecutar el laudo arbitral ante los órganos jurisdiccionales estadounidenses con el fin de garantizar una vía de recurso en caso de incumplimiento por parte de la empresa.

(59) En séptimo lugar, cuando una entidad no cumpla su compromiso de observar los principios y la política de privacidad publicada, el Derecho estadounidense podrá prever otras vías de recurso judicial que ofrezcan soluciones jurídicas en virtud del Derecho de la responsabilidad civil y en casos de falsedad u omisión dolosa, actos o prácticas desleales o fraudulentos, o incumplimiento de contrato.

(60) Además, cuando una APD, tras recibir una reclamación de un interesado de la UE, considere que la transferencia de datos personales a una entidad en los Estados Unidos se realiza violando la legislación de la UE sobre protección de datos, incluso cuando el exportador de datos de la UE tenga razones para creer que la entidad no se ajusta a los principios, también podrá ejercer sus competencias respecto del exportador de datos y, si es necesario, ordenar la suspensión de la transferencia.

(61) A la luz de la información expuesta en la presente sección, la Comisión considera que los principios establecidos por el Departamento de Comercio de los Estados Unidos proporcionan, como tales, un nivel de protección de los datos personales sustancialmente equivalente al brindado por los principios básicos fundamentales que establece la Directiva 95/46/CE.

(62) Además, las obligaciones en materia de transparencia y la administración y revisión del cumplimiento del Escudo de la privacidad por parte del Departamento de Comercio garantizan la aplicación efectiva de los principios.

(63) Por otra parte, la Comisión considera que, en su conjunto, los mecanismos de recurso, supervisión y ejecución previstos por el Escudo de la privacidad permiten identificar y sancionar en la práctica las vulneraciones de los principios cometidas por las organizaciones pertenecientes a dicho marco y ofrecen al interesado la posibilidad de ejercer acciones en Derecho para acceder a los datos personales que le conciernen y, en último término, obtener su rectificación o supresión.

([53]) El número de árbitros que integran el panel deberá ser acordado entre las partes.

([54]) No obstante, el panel podrá dictaminar que, dadas las circunstancias de un determinado arbitraje, la cobertura de estos servicios originaría unos costes injustificados o desproporcionados.

([55]) Las personas físicas no pueden reclamar daños y perjuicios en un procedimiento de arbitraje, pero el hecho de solicitar tal procedimiento no impide la posibilidad de reclamar la citada indemnización ante los órganos jurisdiccionales ordinarios de los Estados Unidos.

3. ACCESO A LOS DATOS PERSONALES TRANSFERIDOS EN EL MARCO DEL ESCUDO DE LA PRIVACIDAD UE-EE. UU. Y UTILIZACIÓN DE LOS MISMOS POR LOS PODERES PÚBLICOS ESTADOUNIDENSES

(64) Tal como se desprende del anexo II, sección I, apartado 5, la adhesión a los principios se limita a lo estrictamente necesario para satisfacer las exigencias de seguridad nacional, interés público o aplicación de la ley.

(65) La Comisión ha evaluado las limitaciones y salvaguardias existentes en el Derecho de los Estados Unidos con respecto al acceso a los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. y la utilización de los mismos por los poderes públicos estadounidenses a efectos de seguridad nacional, aplicación de la ley y otros fines de interés público. Asimismo, el Gobierno estadounidense, a través de su Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) ([56]), ha proporcionado a la Comisión una serie de declaraciones y compromisos detallados que se exponen en el anexo VI de la presente Decisión. Mediante carta firmada por el secretario de Estado y adjunta como anexo III a la presente Decisión, el Gobierno de los Estados Unidos se ha comprometido asimismo a crear un nuevo mecanismo de supervisión de las injerencias con fines de seguridad nacional, a saber, el Defensor del Pueblo en el ámbito del Escudo de la privacidad, que será independiente de los servicios de inteligencia. Por último, la declaración del Departamento de Justicia de los Estados Unidos contenida en el anexo VII de la presente Decisión describe las limitaciones y salvaguardias aplicables al acceso a los datos y a su utilización por parte de los poderes públicos a efectos de aplicación de la ley y otros fines de interés público. Con vistas a mejorar la transparencia y reflejar la naturaleza jurídica de estos compromisos, cada uno de los documentos enumerados y adjuntos a la presente Decisión se publicará en el Registro Federal de los Estados Unidos.

(66) A continuación se desarrollan las constataciones de la Comisión con respecto a las limitaciones del acceso a los datos transferidos desde la Unión Europea a los Estados Unidos y su utilización por parte de los poderes públicos de dicho país, así como sobre la existencia de una tutela judicial efectiva.

3.1. *Acceso y utilización por parte de los poderes públicos estadounidenses a efectos de seguridad nacional*

(67) Del análisis de la Comisión se desprende que el Derecho estadounidense establece varias limitaciones al acceso a los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. y su utilización a efectos de seguridad nacional, así como mecanismos de supervisión y recurso que ofrecen salvaguardias suficientes que permiten proteger de manera eficaz dichos datos contra injerencias ilícitas y los riesgos de abuso ([57]). Este marco jurídico se ha reforzado considerablemente desde 2013, cuando la Comisión publicó sus dos Comunicaciones (véase el considerando 7), como se describe a continuación.

3.1.1. Limitaciones

(68) De conformidad con la Constitución de los Estados Unidos, corresponde al presidente, en su calidad de jefe de Estado y de Gobierno y capitán general de las Fuerzas Armadas, garantizar la seguridad nacional y, por lo que respecta a la inteligencia exterior, administrar los asuntos exteriores del país ([58]). Si bien el Congreso está facultado para imponer limitaciones, y así lo ha hecho en diversos aspectos, el presidente podrá dirigir dentro de estos límites las actividades de los servicios de inteligencia estadounidenses, en particular mediante *executive orders* (decretos) o *presidential directives* (directivas presidenciales). Naturalmente, esto también es aplicable a los ámbitos en los que no existen orientaciones del Congreso. En la actualidad, los dos principales instrumentos jurídicos en este sentido son el Executive Order 12333 (en lo sucesivo, «EO 12333») ([59]) y la Presidential Policy Directive 28 (en lo sucesivo, «PPD-28»).

([56]) El Director de Inteligencia Nacional («DNI», por sus siglas en inglés) es el órgano responsable de los servicios de inteligencia y el principal asesor del presidente de los Estados Unidos y del Consejo de Seguridad Nacional. Véase la Intelligence Reform and Terrorism Prevention Act (Ley de reforma de los servicios de inteligencia y de prevención del terrorismo) de 2004, Pub. L. (Ley de Derecho Público) 108-458 de 17.12.2004. Entre otras cosas, la ODNI gestionará y dirigirá la asignación de selectores, la recopilación, el análisis, la elaboración y la difusión de inteligencia nacional por parte de los servicios de inteligencia y determinará los requisitos aplicables al respecto, inclusive mediante la formulación de directrices sobre el acceso a dicha información, su utilización e intercambio. Véase el artículo 1.3, letras a) y b), del EO 12333.

([57]) Véase Schrems, apartado 91.

([58]) Artículo II de la Constitución de los Estados Unidos. Véase también la introducción de la PPD-28.

([59]) EO 12333: *United States Intelligence Activities* (Actividades de los servicios de inteligencia de los Estados Unidos), Registro Federal vol. 40, n.º 235 (8 de diciembre de 1981). En la medida en que este acto es accesible al público, define los objetivos, las orientaciones, las obligaciones y las responsabilidades de las misiones estadounidenses de inteligencia (incluido el cometido de los distintos servicios de inteligencia) y establece los parámetros generales para llevar a cabo actividades de inteligencia (concretamente, la necesidad de promulgar normas de procedimiento específicas). En virtud del artículo 3.2 del EO 12333, el presidente, respaldado por el Consejo Nacional de Seguridad y por el director de Inteligencia Nacional, adoptará las directivas, procedimientos y orientaciones pertinentes y necesarios para la aplicación de este acto.

(69) La PPD-28, adoptada el 17 de enero de 2014, impone una serie de limitaciones a las operaciones de «inteligencia de señales» ([60]). Esta directiva presidencial es vinculante para los servicios de inteligencia de los Estados Unidos ([61]) y permanece en vigor aunque se produzcan cambios en el Gobierno estadounidense ([62]). La PPD-28 reviste especial importancia para los ciudadanos no estadounidenses, entre ellos los interesados de la UE. Entre otras cosas, estipula lo siguiente:

a) la recopilación de inteligencia de señales se basará en un acto legislativo o en una autorización presidencial y deberá llevarse a cabo de conformidad con la Constitución de los Estados Unidos (en particular, con su Enmienda IV) y el Derecho estadounidense;

b) todas las personas deben ser tratadas con dignidad y respeto, con independencia de su nacionalidad o de su lugar de residencia;

c) todas las personas tienen intereses legítimos de privacidad en el tratamiento de su información personal;

d) la privacidad y las libertades civiles se tendrán plenamente en cuenta en la planificación de las actividades de inteligencia de señales de los Estados Unidos;

e) las actividades de inteligencia de señales de los Estados Unidos deberán, por tanto, incluir salvaguardias adecuadas con respecto a la información personal de todas las personas físicas, con independencia de su nacionalidad o su lugar de residencia.

(70) La PPD-28 dispone que la inteligencia de señales se podrá recabar exclusivamente a efectos de inteligencia exterior o contrainteligencia para apoyar misiones nacionales y ministeriales, y no para otros fines (por ejemplo, para proporcionar una ventaja competitiva a empresas estadounidenses). En este sentido, la ODNI explica que los servicios de inteligencia deberían exigir que, siempre que sea posible, la recopilación se centre en objetivos o temas específicos de inteligencia exterior mediante el empleo de discriminantes (por ejemplo, recursos específicos, términos de selección e identificadores) ([63]). Asimismo, las declaraciones aseguran que las decisiones acerca de la recogida de información no constituyen una facultad discrecional de cada agente de inteligencia, sino que han de basarse en las políticas y procedimientos que los servicios de inteligencia estadounidenses deben adoptar para aplicar la PPD-28 ([64]). Por tanto, el estudio y la determinación de los selectores adecuados se desarrolla dentro del marco global denominado National Intelligence Priorities Framework (Marco de Prioridades de Inteligencia Nacional; en lo sucesivo, «NIPF»), que garantiza que las prioridades de inteligencia sean fijadas por responsables políticos de alto nivel y revisadas periódicamente para que puedan seguir respondiendo a las amenazas reales a la seguridad nacional y tener en cuenta los posibles riesgos, inclusive en materia de privacidad ([65]). Sobre esta base, el personal de los servicios de inteligencia estudia e identifica términos de selección específicos que permitan recabar inteligencia exterior en función de las prioridades establecidas ([66]). Los términos de selección o «selectores» deben revisarse periódicamente para comprobar si siguen proporcionando inteligencia valiosa con arreglo a las prioridades ([67]).

([60]) De conformidad con el EO 12333, el director de la Agencia de Seguridad Nacional (en lo sucesivo «NSA», por sus siglas en inglés) es el responsable funcional de la inteligencia de señales y ha de dirigir una organización unificada de las actividades en dicho ámbito.

([61]) Por «servicios de inteligencia» (en inglés, *Intelligence Community*) se entenderán los detallados en el artículo 3.5.h), del EO 12333, tal como se indica en la nota 1 de la PPD-28.

([62]) Véase el Memorando de la Oficina del Asesor Jurídico del Departamento de Justicia de los Estados Unidos, dirigido al presidente Clinton, de 29 de enero de 2000. Con arreglo a este dictamen jurídico, las directivas presidenciales surten los mismos efectos jurídicos sustantivos que los decretos.

([63]) Declaraciones de la ODNI (anexo VI), p. 3.

([64]) Véase el artículo 4.b) y c), de la PPD-28. Según datos publicados, la revisión de 2015 confirmó los seis fines existentes. Véase ODNI: *Signals Intelligence Reform: 2016 Progress Report* (Informe de 2016 sobre los avances de la reforma de la inteligencia de señales).

([65]) Declaraciones de la ODNI (anexo VI), p. 6 [con referencia a la Intelligence Community Directive 204 (Directiva de los Servicios de Inteligencia 204)]. Véase también el artículo 3 de la PPD-28.

([66]) Declaraciones de la ODNI (anexo VI), p. 6. Véase, por ejemplo, NSA Civil Liberties and Privacy Office (Oficina de Libertades Civiles y Privacidad de la NSA; en lo sucesivo, «NSA CLPO»): *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333* (Medidas de la NSA para la protección de las libertades civiles y la privacidad en las actividades de recopilación selectiva de inteligencia de señales en virtud del Decreto 12333), 7 de octubre de 2014. Véase también el informe de situación de 2014 de la ODNI. Por lo que respecta a las solicitudes de acceso en virtud del artículo 702 de la FISA, las consultas se rigen por los procedimientos de minimización aprobados por el FISC. Véase NSA CLPO: *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Aplicación del artículo 702 de la Ley de Vigilancia de Inteligencia Exterior por la NSA), 16 de abril de 2014.

([67]) Véase ODNI: *Signals Intelligence Reform: 2015 Anniversary Report* (Informe de 2015 sobre el aniversario de la reforma de la inteligencia de señales). Véanse también las declaraciones de la ODNI (anexo VI), pp. 6, 8, 9 y 11.

(71) Además, los requisitos que se precisan en la PPD-28 de que la recopilación de información será siempre ([68])«lo más adaptada posible», y que los servicios de inteligencia darán prioridad a la disponibilidad de otra información y de alternativas adecuadas y factibles ([69]), refleja una regla general de priorización de la recopilación selectiva frente a la recopilación indiscriminada. Según la declaración de la ODNI, garantizan, en particular, que la recopilación en bloque no es «masiva» ni «indiscriminada», y que la excepción no sustituye a la norma ([70]).

(72) Aunque la PPD-28 estipula que, en determinadas circunstancias, los servicios de inteligencia se ven obligados a recabar inteligencia de señales de manera indiscriminada (por ejemplo, con objeto de identificar amenazas nuevas o emergentes), les exige que concedan prioridad a las alternativas que permitan llevar a cabo actividades de inteligencia de señales selectivas ([71]). Así pues, la recopilación indiscriminada se autorizará únicamente cuando la recopilación selectiva mediante el empleo de discriminantes -es decir, identificadores asociados a un objetivo específico, como el correo electrónico o número de teléfono del objetivo- no pueda llevarse a cabo por motivos técnicos u operativos ([72]). Esto es aplicable tanto al modo en que se recaba la inteligencia de señales como al contenido propiamente dicho de la información recopilada ([72]).

(73) Según las declaraciones de la ODNI, incluso cuando los servicios de inteligencia no puedan utilizar identificadores específicos para especificar la recopilación, intentarán reducir la recopilación «en la mayor medida posible». Para garantizar esto, «aplicarán filtros y otras herramientas técnicas para centrar la recopilación en las instalaciones que puedan contener comunicaciones de valor para la inteligencia extranjera» (y, por tanto, darán respuesta a las exigencias de los responsables políticos de EE. UU. con arreglo al procedimiento descrito en el punto 70). Como consecuencia de ello, la recopilación indiscriminada se centrará de al menos dos maneras: En primer lugar, siempre se referirá a objetivos específicos de inteligencia extranjera (por ejemplo, adquirir inteligencia de señales sobre las actividades de un grupo terrorista que opera en una región en particular) y centrar la recopilación en las comunicaciones que posean tal nexo. Según la declaración de la ODNI, esto se refleja en el hecho de que las actividades de inteligencia de señales de Estados Unidos atañen solo a una fracción de las comunicaciones a través de Internet ([73]). En segundo lugar, las declaraciones de la ODNI explican que los filtros y otros instrumentos técnicos utilizados estarán concebidos para centrar la recopilación «de la forma más precisa posible» con el fin de garantizar que la cantidad de «información no pertinente» recogida sea mínima.

(74) Por último, aun cuando los Estados Unidos consideren necesaria la recopilación indiscriminada de inteligencia de señales, en las circunstancias previstas en los considerandos 70 a 73, la PPD-28 limita el uso de dicha información a una lista específica de seis fines de seguridad nacional destinados a proteger la privacidad y las libertades civiles de todas las personas, con independencia de su nacionalidad o su lugar de residencia ([74]). Estos fines admisibles comprenden medidas para detectar y neutralizar las amenazas que plantean el espionaje, el

([68]) Véanse las declaraciones de la ODNI (anexo VI), p. 3.

([69]) También procede observar que, en virtud del artículo 2.4 del EO 12333, los servicios de inteligencia deberán utilizar las técnicas de recopilación lo menos intrusivas posible dentro de los Estados Unidos. Por lo que se refiere a las limitaciones de sustituir todas las recopilaciones indiscriminadas por recopilaciones selectivas, véanse los resultados de una evaluación por el Consejo Nacional de Investigación, tal como ha informado la Agencia de los Derechos Fundamentales de la Unión Europea, Vigilancia por los servicios de inteligencia: derechos fundamentales, salvaguardias y recursos en la UE (2015), p. 18.

([70]) Declaraciones de la ODNI (anexo VI), p. 4.

([71]) Véase también el artículo 5.d), de la PPD-28, que exige al director de Inteligencia Nacional que presente al presidente de los Estados Unidos, en coordinación con los jefes de los servicios de inteligencia correspondientes y la Oficina de Política Científica y Tecnológica, un informe que evalúe la viabilidad de crear un programa informático que facilite a los servicios de inteligencia recabar información de manera más selectiva que indiscriminada. Según datos publicados, el resultado de este informe fue que no hay ninguna alternativa informática que sirva para sustituir por completo la recopilación indiscriminada a efectos de la detección de determinadas amenazas a la seguridad nacional. Véase ODNI: *Signals Intelligence Reform: 2015 Anniversary Report* (Informe de 2015 sobre el aniversario de la reforma de la inteligencia de señales).

([72]) Véase la nota 68 a pie de página.

([73]) Declaraciones de la ODNI (anexo VI). Esto aborda específicamente la preocupación expresada por las autoridades nacionales de protección de datos en su dictamen sobre el proyecto de Decisión de adecuación. Véase el dictamen n.º 1/2016 del Grupo de Trabajo del artículo 29, sobre el proyecto de decisión de adecuación sobre el Escudo de la privacidad UE-EE. UU. (adoptado el 13 de abril de 2016), p. 38, n. 47.

([74]) Véase el artículo 2 de la PPD-28.

terrorismo, las armas de destrucción masiva y las amenazas de ciberseguridad para las Fuerzas Armadas o el personal militar, así como las amenazas delictivas transnacionales relacionadas con los otros cinco fines, y se revisarán con una periodicidad mínima anual. De las declaraciones del Gobierno estadounidense se desprende que los servicios de inteligencia han reforzado sus prácticas analíticas y sus normas para consultar la inteligencia de señales no evaluada con arreglo a estos requisitos; el empleo de consultas específicas garantiza que únicamente se presenten a los analistas, para su examen, los elementos que se considera que podrían aportar información valiosa ([75]).

(75) Estas limitaciones resultan de especial importancia en relación con los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU., en particular cuando la recopilación de tales datos deba tener lugar fuera de los Estados Unidos, incluso durante su tránsito por los cables transatlánticos desde la Unión a Estados Unidos. Tal como han confirmado las autoridades estadounidenses en declaraciones de la ODNI, esta recopilación está sujeta a las limitaciones y salvaguardias establecidas en el marco, que incluyen las previstas en la PPD-28 ([76]).

(76) Aunque no se formule en tales términos jurídicos, estos principios captan la esencia de los principios de necesidad y proporcionalidad. Se concede una clara prioridad a la recopilación selectiva, mientras que la recopilación indiscriminada se limita a situaciones (excepcionales) en las que no es posible llevar a cabo una selectiva por motivos técnicos u operativos. Aun cuando no pueda evitarse la *recopilación indiscriminada*, el acceso a tales datos y su posterior utilización se *limita estrictamente* a fines legítimos y específicos de seguridad nacional ([77]).

(77) Al estar contenidos en una directiva adoptada por el presidente en calidad de Jefe de Gobierno, estos requisitos vinculan a la totalidad de los servicios de inteligencia y se han aplicado asimismo a través de una serie de normas y procedimientos institucionales que incorporan los principios generales a las instrucciones específicas aplicables a sus operaciones cotidianas. Por otro lado, aunque el Congreso no está directamente vinculado por la PPD-28, también ha adoptado medidas para garantizar que la recopilación de datos personales y el acceso a los mismos en los Estados Unidos sean de carácter selectivo en lugar de «generalizados».

(78) De la información disponible, incluidas las declaraciones recibidas del Gobierno estadounidense, se desprende que, una vez que los datos se hayan transferido a entidades ubicadas en los Estados Unidos y autocertificadas en el marco del Escudo de la privacidad UE-EE. UU., los servicios de inteligencia estadounidenses solo ([78]) podrán recabar datos personales si su petición cumple la Foreign Intelligence Surveillance Act (Ley de Vigilancia de Inteligencia Exterior; en lo sucesivo, «FISA») o procede del Federal Bureau of Investigation (en lo sucesivo, «FBI»), sobre la base de una denominada National Security Letter (carta de seguridad nacional; en lo sucesivo, «NSL») ([79]). Existen diversas bases jurídicas en virtud de la FISA que pueden utilizarse para recopilar (y posteriormente tratar)

([75]) Declaraciones de la ODNI (anexo VI), p. 4. Véase también la *Intelligence Community Directive 203* (Directiva de los Servicios de Inteligencia 203).

([76]) Declaraciones de la ODNI (anexo VI), p. 2. También se aplican las limitaciones estipuladas en el EO 12333 (por ejemplo, la necesidad de que la información recabada responda a las prioridades de inteligencia fijadas por el presidente de los Estados Unidos).

([77]) Véase Schrems, apartado 93.

([78]) La recopilación de datos por parte del FBI podrá basarse asimismo en autorizaciones con fines coercitivos (véase el apartado 3.2 de la presente Decisión).

([79]) Para más información sobre la utilización de NSL, véanse las declaraciones de la ODNI (anexo VI), pp. 13 y 14 y nota 38. Tal como se indica en dicho documento, el FBI solo podrá recurrir a las NSL para solicitar información sin contenido, siempre que esta sea pertinente a efectos de una investigación autorizada de seguridad nacional destinada a brindar protección contra el terrorismo internacional o actividades de inteligencia clandestinas. En cuanto a las transferencias de datos en el marco del Escudo de la privacidad UE-EE. UU., el principal fundamento jurídico existente parece ser la Electronic Communications Privacy Act (Ley de Privacidad de las Comunicaciones Electrónicas, codificada en el título 18, artículo 2709, del USC), que dispone que toda solicitud de información sobre los abonados o registros de operaciones utilice un término que identifique específicamente a una persona, una entidad, un número de teléfono o una cuenta.

los datos personales de interesados de la UE que han sido transferidos en el marco del Escudo de la privacidad UE-EE. UU. Los dos instrumentos fundamentales, aparte del artículo 104 de la FISA ([80]) que cubre la vigilancia electrónica individualizada convencional y el artículo 402 de la FISA ([81]) sobre la instalación de dispositivos de identificación y registro de llamadas entrantes (*trap and trace devices*) o salientes (*pen registers*), son el artículo 501 [antiguo artículo 215 de la *USA Patriot Act* (Ley Patriótica de los Estados Unidos)] y el artículo 702 de la FISA ([82]).

(79) A este respecto, la USA Freedom Act (Ley de Libertad de los Estados Unidos), adoptada el 2 de junio de 2015, prohíbe la recopilación indiscriminada de documentos en virtud del artículo 402 de la FISA (dispositivos de identificación y registro de llamadas entrantes y salientes), del artículo 501 de la FISA (antiguo artículo 215 de la USA Patriot Act) ([83]) y mediante la utilización de NSL y, en su lugar, exige el empleo de «términos de selección» específicos ([84]).

(80) Aunque la FISA contiene otras base jurídicas que permiten emprender actividades de inteligencia nacional, incluida la inteligencia de señales, de la evaluación de la Comisión se desprende que, en lo concerniente a los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU., tales bases limitan igualmente las injerencias de las autoridades públicas a una recopilación y un acceso selectivos.

(81) Ello es evidente en el caso de la vigilancia electrónica individualizada convencional en virtud del artículo 104 de la FISA ([85]). En cuanto al artículo 702 de la FISA, que sirve de base para dos importantes programas de inteligencia gestionados por los servicios de inteligencia estadounidenses (a saber, PRISM y Upstream), establece que las búsquedas se lleven a cabo de manera selectiva mediante la utilización de selectores individuales que identifiquen recursos de comunicaciones específicos, como la dirección de correo electrónico o el número de teléfono del objetivo, pero no palabras clave ni los nombres de personas seleccionadas ([86]). Por tanto, tal como señala el Privacy and Civil Liberties Oversight Board (Consejo de Supervisión de la Privacidad y de las Libertades Civiles de los Estados Unidos (en lo sucesivo «PCLOB»), la vigilancia en virtud del artículo 702 se centra

([80]) USC, título 50, artículo 1804. Aunque esta base jurídica exige una exposición de los hechos y circunstancias en que se basa el solicitante para justificar su creencia de que el objetivo de la vigilancia electrónica es una potencia extranjera o un agente de una potencia extranjera, este último puede ser un ciudadano no estadounidense implicado en actos de terrorismo internacional o en la proliferación internacional de armas de destrucción masiva (incluidas las actividades preparatorias) [USC, título 50, artículo 1801, letra b), punto 1]. Sin embargo, solo existe una conexión teórica con los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU., ya que la exposición de los hechos también debe justificar la creencia de que cada uno de los recursos o lugares a los que se dirige la vigilancia electrónica está siendo utilizado, o va a ser utilizado en breve, por una potencia extranjera o un agente de una potencia extranjera. En cualquier caso, para poder ejercer esta facultad, es necesario presentar una solicitud previa al FISC, que determinará, entre otras cosas, si los hechos expuestos acreditan que existen indicios razonables al respecto.

([81]) USC, título 50, artículo 1842 en relación con el artículo 1841, punto 2, del mismo título y con el artículo 3127 del título 18. Esta facultad no se refiere a los contenidos de las comunicaciones, sino que se centra en la información relativa al cliente o abonado que utiliza el servicio (como su nombre, dirección, número de abonado, duración o naturaleza del servicio recibido y fuente o modalidad de pago). Es preciso solicitar un mandamiento del FISC (o de un juez estadounidense de primera instancia e instrucción) y utilizar un término de selección específico a tenor de lo dispuesto en el artículo 1841, punto 4 (a saber, un término que identifique de manera específica a una persona, una cuenta, etc., y que se emplee para delimitar, en la medida de lo razonablemente posible, el ámbito de la información buscada).

([82]) Mientras que el artículo 501 de la FISA (antiguo artículo 215 de la USA Patriot Act) autoriza al FBI a solicitar un mandamiento judicial para presentar «elementos tangibles» (sobre todo metadatos telefónicos, pero también documentos profesionales) como prueba con fines de inteligencia exterior, el artículo 702 de la FISA permite a los servicios de inteligencia estadounidenses demandar acceso a información, incluido el contenido de comunicaciones por Internet, procedente de los Estados Unidos, pero acerca de determinados ciudadanos no estadounidenses que se encuentran fuera del país.

([83]) En virtud de esta disposición, el FBI puede solicitar «elementos tangibles» (por ejemplo, registros, escritos y documentos) al objeto de demostrar ante el Foreign Intelligence Surveillance Court (Tribunal de Vigilancia de Inteligencia Exterior; en lo sucesivo, «FISC») que existen motivos fundados para pensar que resultan pertinentes para una determinada investigación del FBI. A la hora de efectuar su búsqueda, el FBI debe utilizar términos de selección aprobados por el FISC cuando exista una «sospecha clara y fundada» de que tales términos están asociados a la participación de una o varias potencias extranjeras o sus agentes en actos de terrorismo internacional o en actividades preparatorias relacionadas con estos. Véase el informe del PCLOB sobre el artículo 215, p. 59; NSA CLPO, *Transparency Report: The USA Freedom Act Business Records FISA Implementation* (Informe de transparencia sobre la aplicación de la FISA modificada por la disposición sobre documentos profesionales de la USA Freedom Act), 15 de enero de 2016, pp. 4 a 6.

([84]) Declaraciones de la ODNI (anexo VI), p. 13 (nota 38).

([85]) Véase la nota 81.

([86]) Informe del PCLOB sobre el artículo 702, pp. 32 y 33, y las referencias allí citadas. Con arreglo a su oficina de privacidad, la NSA deberá comprobar que existe una conexión entre el objetivo y el selector y documentar la información de inteligencia exterior que se prevé recabar; esta información deberá ser revisada y aprobada por dos analistas superiores de la NSA y se monitorizará todo el proceso a efectos de las posteriores verificaciones del cumplimiento efectuadas por la ODNI y el Departamento de Justicia. Véase NSA CLPO: *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Aplicación del artículo 702 de la Ley de Vigilancia de Inteligencia Exterior por la NSA), 16 de abril de 2014.

íntegramente en ciudadanos no estadounidenses específicos sobre los que se han efectuado determinaciones individualizadas ([87]). Debido a una cláusula de extinción, el artículo 702 de la FISA deberá someterse a revisión en 2017, momento en el que la Comisión tendrá que evaluar de nuevo las salvaguardias de que disponen los interesados de la UE.

(82) Por otro lado, el Gobierno de los Estados Unidos ha asegurado de forma explícita a la Comisión Europea que los servicios de inteligencia estadounidenses no desarrollan actividades de vigilancia indiscriminada de los ciudadanos europeos de a pie ni de ninguna otra persona ([88]). Por lo que respecta a los datos personales recopilados dentro de los Estados Unidos, dicha afirmación se apoya en pruebas empíricas que demuestran que las *solicitudes de acceso* presentadas a través de NSL y en virtud de la FISA, tanto a título individual como colectivo, solo se refieren a un número relativamente reducido de objetivos en comparación con el flujo total de datos en Internet ([89]).

(83) En lo concerniente al *acceso* a los datos recopilados y a la *seguridad de los datos*, la PPD-28 dispone que el acceso se limitará al personal autorizado que necesite conocer esa información para desempeñar sus funciones y que la información personal deberá tratarse y almacenarse en condiciones que permitan una adecuada protección e impidan el acceso de personas no autorizadas, de conformidad con las salvaguardias aplicables a la información delicada. El personal de los servicios de inteligencia recibe una formación pertinente y adecuada en relación con los principios establecidos en la PPD-28 ([90]).

(84) Por último, en lo referente al *almacenamiento* y a la *difusión* ulterior de los datos personales de interesados de la UE recopilados por los servicios de inteligencia de los Estados Unidos, la PPD-28 establece que todas las personas (incluidos los ciudadanos no estadounidenses) deberían ser tratados con dignidad y respeto, que todas las personas tienen intereses legítimos de privacidad en el tratamiento de su información personal y que, por tanto, los servicios de inteligencia han de elaborar políticas que ofrezcan unas salvaguardias adecuadas respecto de tales datos y hayan sido razonablemente concebidas para minimizar su difusión y conservación ([91]).

([87]) Informe del PCLOB sobre el artículo 702, p. 111. Véanse también las declaraciones de la ODNI (anexo VI), p. 9, según las cuales la recopilación en virtud del artículo 702 de la [FISA] no es «masiva e indiscriminada», sino que se centra estrictamente en la recopilación de inteligencia exterior de objetivos legítimos identificados de manera individual, y en la p. 13, nota 36 (con referencia a un dictamen del FISC de 2014), así como el informe de la NSA CLPO *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Aplicación del artículo 702 de la Ley de Vigilancia de Inteligencia Exterior por la NSA), 16 de abril de 2014. Incluso en el caso del programa Upstream, la NSA podrá únicamente solicitar la interceptación de comunicaciones electrónicas dirigidas a los selectores asignados, procedentes de ellos o sobre estos.

([88]) Declaraciones de la ODNI (anexo VI), p. 18. Véase también la página 6, según la cual los procedimientos aplicables «demuestran un claro compromiso para prevenir la recopilación arbitraria e indiscriminada de información de inteligencia de señales y aplicar el principio de razonabilidad desde las más altas esferas del Gobierno de los Estados Unidos».

([89]) Véase el *Statistical Transparency Report Regarding Use of National Security Authorities* (Informe estadístico de transparencia sobre la utilización de las autorizaciones de seguridad nacional), 22 de abril de 2015. Con respecto al flujo total de datos en Internet, véase, por ejemplo, Agencia de los Derechos Fundamentales de la Unión Europea: *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU* (Vigilancia de los servicios de inteligencia: salvaguardias y recursos en materia de derechos humanos en la UE), 2015, pp. 15 y 16. En cuanto al programa Upstream, con arreglo a un dictamen desclasificado del FISC de 2011, más del 90 % de las comunicaciones electrónicas recabadas en virtud del artículo 702 de la FISA procedían del programa PRISM, mientras que menos del 10 % provenían del programa Upstream. Véase FISC: Dictamen 2011 WL 10945618 (FISA Ct. [Tribunal de la FISA], 3.10.2011), nota 21 (disponible en el siguiente enlace: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Véase el artículo 4, letra a), inciso ii), de la PPD-28. Véase también el informe de la ODNI *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28* (Salvaguardar la información personal de todas las personas: un informe de situación sobre el desarrollo y la aplicación de los procedimientos previstos en la PPD-28), julio de 2014, p. 5, según el cual las políticas de los servicios de inteligencia deberían reforzar las normas y prácticas analíticas existentes con el fin de que los analistas traten de estructurar las consultas y los demás términos y técnicas de búsqueda de modo que identifiquen la información de inteligencia pertinente para llevar a cabo una misión legítima de inteligencia o de aplicación de la ley; centren las consultas relativas a personas en categorías de información que respondan a un requisito de inteligencia o de aplicación de la ley; y reduzcan al mínimo el examen de información personal no relevante a efectos del cumplimiento de los requisitos de inteligencia o de aplicación de la ley. Véanse, por ejemplo, CIA: *Signals Intelligence Activities* (Actividades de inteligencia de señales), p. 5, y FBI: *Presidential Policy Directive 28 Policies and Procedures* (Políticas y procedimientos en virtud de la Directiva de Política Presidencial 28), p. 3. Con arreglo al informe de situación de 2016 sobre la reforma de la inteligencia de señales, los servicios de inteligencia (incluidos el FBI, la CIA y la NSA) han tomado medidas para sensibilizar a su personal sobre las exigencias de la PPD-28 mediante nuevas políticas de formación o la modificación de las existentes.

([91]) Según las declaraciones de la ODNI, estas restricciones se aplican con independencia de si la información se recopiló indiscriminadamente o de forma selectiva, y de la nacionalidad del individuo.

(85) El Gobierno de los Estados Unidos ha explicado que este requisito de razonabilidad implica que los servicios de inteligencia no tendrán que adoptar «cualquier medida teóricamente posible», sino que deberán encontrar el equilibrio entre sus esfuerzos para proteger los intereses legítimos en materia de privacidad y libertades civiles, por un lado, y las necesidades prácticas de las actividades de inteligencia de señales, por otro ([92]). En este sentido, los ciudadanos no estadounidenses recibirán el mismo trato que los ciudadanos estadounidenses, de conformidad con los procedimientos aprobados por el fiscal general ([93]).

(86) Con arreglo a estas normas, la conservación se limita, por lo general, a un máximo de cinco años, salvo que exista una determinación específica en la legislación o que el director de Inteligencia Nacional adopte una determinación expresa, previa evaluación minuciosa de los problemas de privacidad —teniendo en cuenta los puntos de vista del responsable de Protección de las Libertades Civiles de la ODNI, así como de los funcionarios competentes en materia de privacidad y libertades civiles de los distintos servicios—, de que la continuación de la conservación redunda en interés de la seguridad nacional ([94]). La difusión se limita a aquellos casos en que la información sea pertinente a efectos del objetivo fundamental de la recopilación y responda, por tanto, a un requisito autorizado de inteligencia exterior o de aplicación de la ley ([95]).

(87) El Gobierno de los Estados Unidos garantiza que no podrá difundirse información personal por la única razón de que la persona interesada no sea de nacionalidad estadounidense y, en este sentido, señala que «no procederá considerar la inteligencia de señales sobre las actividades cotidianas de una persona extranjera inteligencia exterior que pueda difundirse o conservarse de forma permanente por ese mero hecho, a menos que responda de otro modo a un requisito de inteligencia exterior autorizado» ([96]).

(88) Por todo lo anterior, la Comisión concluye que en los Estados Unidos existen normas destinadas a garantizar que las posibles injerencias cometidas a efectos de seguridad nacional en los derechos fundamentales de las personas cuyos datos personales se transfieran desde la Unión a los Estados Unidos en el marco del Escudo de la privacidad UE-EE. UU. se limiten a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido.

(89) Según ha puesto de manifiesto el análisis precedente, la normativa estadounidense garantiza que las medidas de vigilancia solo podrán emplearse para obtener información de inteligencia exterior, lo que es un objetivo legítimo ([97]), y ser lo más adaptadas posible. En particular, la recopilación indiscriminada solo podrá autorizarse

([92]) Véanse las declaraciones de la ODNI (anexo VI).

([93]) Véase el artículo 4, letra a), inciso i), de la PPD-28 en relación con el artículo 2.3 del EO 12333.

([94]) Véanse el artículo 4, letra a), inciso i), de la PPD-28, y las declaraciones de la ODNI (anexo VI), p. 7. Por ejemplo, con respecto a la información personal recopilada en virtud del artículo 702 de la FISA, los procedimientos de minimización de la NSA aprobados por el FISC prevén como norma que los metadatos y los contenidos no evaluados del programa PRISM no puedan conservarse más de cinco años y, en el caso de los datos de Upstream, no más de dos años. La NSA respeta estos límites de almacenamiento a través de un proceso automatizado que suprime los datos recopilados al vencer el correspondiente plazo de conservación. Véanse los Procedimientos de minimización de la NSA con respecto al artículo 702 de la FISA, artículo 7 en relación con el artículo 6, letra a), punto 1, y NSA CLPO: *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Aplicación del artículo 702 de la Ley de Vigilancia de Inteligencia Exterior por la NSA), 16 de abril de 2014. Asimismo, el plazo de conservación dispuesto en el artículo 501 de la FISA (antiguo artículo 215 de la USA Patriot Act) se limita a cinco años, a menos que los datos personales sean objeto de una difusión debidamente autorizada de información de inteligencia exterior, o que el Departamento de Justicia notifique a la NSA por escrito la obligación de conservar determinada documentación en algún litigio pendiente o previsto. Véase NSA CLPO: *Transparency Report: The USA Freedom Act Business Records FISA Implementation* (Informe de transparencia sobre la aplicación de la FISA modificada por la disposición sobre documentos profesionales de la *USA Freedom Act*), 15 de enero de 2016.

([95]) En particular, en virtud del artículo 501 de la FISA (antiguo artículo 215 de la USA Patriot Act), la información personal solo puede difundirse a efectos de lucha contra el terrorismo o como prueba de un delito, mientras que el artículo 702 de la citada ley permite la difusión únicamente cuando exista un objetivo legítimo de inteligencia exterior o de aplicación de la ley. Véanse los informes de la NSA CLPO *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Aplicación del artículo 702 de la Ley de Vigilancia de Inteligencia Exterior por la NSA), 16 de abril de 2014; *Transparency Report: The USA Freedom Act Business Records FISA Implementation* (Informe de transparencia sobre la aplicación de la FISA modificada por la disposición sobre documentos profesionales de la USA Freedom Act), 15 de enero de 2016; *y NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333* (Medidas de la NSA para la protección de las libertades civiles y la privacidad en las actividades de recopilación selectiva de inteligencia de señales en virtud del Decreto 12333), 7 de octubre de 2014.

([96]) Declaraciones de la ODNI (anexo VI), p. 7 (con referencia a la *Intelligence Community Directive 203* [Directiva de los Servicios de Inteligencia 203]).

([97]) El Tribunal de Justicia ha aclarado que la seguridad nacional constituye un objetivo político legítimo. Véase Schrems, apartado 88. Véase también la sentencia Digital Rights Ireland y otros, antes citada, apartados 42 a 44 y 51, en la que el Tribunal consideró que la lucha contra las formas graves de delincuencia, en particular la delincuencia organizada y el terrorismo, puede depender en gran medida de la utilización de técnicas modernas de investigación. Por otra parte, a diferencia de lo que ocurre en las investigaciones penales que suelen referirse a la determinación retroactiva de la responsabilidad y culpa por conductas pasadas, las actividades de inteligencia suelen centrarse en la prevención de amenazas a la seguridad nacional antes de que se hayan producido daños. Por tanto, dicha investigación puede a menudo tener que cubrir una gama más amplia de posibles actores («objetivos») y un área geográfica más amplia. Véase TEDH, sentencia Weber y Saravia/Alemania de 29 de junio de 2006, demanda n.º 54934/00, apartados 118 a 105 (sobre el denominado «seguimiento estratégico»).

excepcionalmente cuando la recogida selectiva no sea viable, e irá acompañada de salvaguardias adicionales para reducir al mínimo la cantidad de datos recogidos y en su ulterior acceso (que deberá ser selectivo y permitirse únicamente para fines específicos).

(90) En la evaluación de la Comisión, esto es conforme con la norma establecida por el Tribunal de Justicia en la sentencia Schrems, según la cual una legislación que implique una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe imponer unas «exigencias mínimas» ([98]) y «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» ([99]). Tampoco habrá una recopilación y almacenamiento de datos ilimitados de todas las personas sin ninguna limitación, ni acceso ilimitado. Por otra parte, las declaraciones facilitadas a la Comisión, incluida la garantía de que las actividades de inteligencia de señales de los Estados Unidos afectan solo a una fracción de las comunicaciones a través de Internet, excluye que se pueda acceder «de forma generalizada» ([100]) al contenido de las comunicaciones electrónicas.

3.1.2. Tutela judicial efectiva

(91) La Comisión ha evaluado tanto los mecanismos de supervisión existentes en los Estados Unidos con respecto a las posibles injerencias de los servicios de inteligencia estadounidenses en los datos personales transferidos a dicho país como las vías de recurso individual a disposición de los interesados de la UE.

Supervisión

(92) Los servicios de inteligencia de los Estados Unidos están sujetos a diversos mecanismos de revisión y supervisión que corresponden a los tres poderes del Estado. Aquí se incluyen los órganos internos y externos del poder ejecutivo, una serie de comisiones del Congreso, así como la supervisión judicial, esto último sobre todo en relación con las actividades en el marco de la Ley de Vigilancia de Inteligencia Exterior.

(93) En primer lugar, las actividades de inteligencia llevadas a cabo por las autoridades estadounidenses son objeto de una amplia supervisión por parte del poder ejecutivo.

(94) Con arreglo al artículo 4, letra a), inciso iv), de la PPD-28, las políticas y procedimientos de los servicios de inteligencia comprenderán las medidas oportunas —entre ellas, auditorías periódicas— para facilitar la supervisión de la aplicación de las salvaguardias que protegen la información personal ([101]).

([98]) Véase Schrems, apartado 91, y la jurisprudencia allí citada.
([99]) Schrems, apartado 93.
([100]) Véase Schrems, apartado 94.
([101]) ODNI: *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28* (Salvaguardar la información personal de todas las personas: un informe de situación sobre el desarrollo y la aplicación de los procedimientos previstos en la Directiva de Política Presidencial 28), p. 7. Véanse, por ejemplo, CIA: «Compliance» (Cumplimiento), *Signals Intelligence Activities* (Actividades de inteligencia de señales), p. 6; FBI: *Presidential Policy Directive 28 Policies and Procedures* (Políticas y procedimientos en virtud de la Directiva de Política Presidencial 28), apartado III, letra A, punto 4, y letra B, punto 4; y NSA: *PPD-28 Section 4 Procedures* (Procedimientos en virtud del artículo 4 de la PPD-28), 12 de enero de 2015, apartados 8.1 y 8.6, letra c).

(95) Se han establecido múltiples niveles de supervisión en este ámbito, entre los que figuran los funcionarios de libertades civiles o de privacidad, los inspectores generales, la Oficina de Libertades Civiles y Privacidad de la ODNI, el PCLOB y la Junta de Supervisión de Inteligencia del Presidente. Estos mecanismos de supervisión reciben el apoyo del personal especializado presente en todas las agencias ([102]).

(96) Tal como expone el Gobierno de los Estados Unidos ([103]), existen *funcionarios de libertades civiles o de privacidad* con responsabilidades de supervisión en diversos servicios de inteligencia y departamentos que desempeñan labores de inteligencia ([104]). Aunque las facultades específicas de estos funcionarios pueden variar ligeramente en función del acto de autorización correspondiente, suelen incluir la supervisión de procedimientos para garantizar que el respectivo departamento o servicio tenga debidamente en cuenta las cuestiones relacionadas con la privacidad y las libertades civiles y haya instaurado los procedimientos adecuados para atender las reclamaciones de las personas que consideren que se han vulnerado su privacidad o sus libertades civiles (y, en ocasiones, como en el caso de la ODNI, pueden estar facultados para investigar reclamaciones ([105])). Por su parte, el jefe del departamento o servicio ha de procurar que el funcionario reciba toda la información y tenga acceso a todo el material necesario para el ejercicio de sus funciones. Los funcionarios de libertades civiles y privacidad presentan informes periódicos al Congreso y al PCLOB, entre otros acerca del número y la naturaleza de las reclamaciones recibidas por el departamento o servicio, así como un resumen del curso dado a las mismas, los controles e investigaciones llevados a cabo y las repercusiones de las actividades desarrolladas por el funcionario ([106]). De acuerdo con la evaluación realizada por las autoridades nacionales de protección de datos, el control interno que ejercen los funcionarios de libertades civiles o de privacidad puede considerarse «fuerte», aunque en su opinión no cumplen el grado necesario de independencia ([107]).

(97) Además, cada servicio de inteligencia dispone de su propio *inspector general*, que se encarga, entre otras cosas, de supervisar las actividades de inteligencia exterior ([108]). En el caso de la ODNI, existe una Oficina del Inspector General con amplias competencias sobre el conjunto de servicios de inteligencia y facultada para investigar reclamaciones o información relativa a presuntas conductas ilícitas o abusos de autoridad, en relación con los programas y actividades de la ODNI o de los servicios de inteligencia ([109]). Los inspectores generales son figuras jurídicamente independientes ([110]) que se encargan de efectuar auditorías e investigaciones con respecto a los programas y operaciones emprendidos por el servicio correspondiente con fines de inteligencia nacional, incluidos el abuso o incumplimiento de la ley ([111]). Disponen de acceso autorizado a todos los registros, informes,

([102]) Por ejemplo, la NSA cuenta con más de trescientos empleados especializados en dicho ámbito en su Dirección de Cumplimiento. Véanse las declaraciones de la ODNI (anexo VI), p. 7.

([103]) Véase el documento sobre la figura del Defensor del Pueblo (anexo III), apartado 6, letra b), incisos i) a iii).

([104]) Véase el título 42, artículo 2000ee-1, del USC. Entre ellos figuran, por ejemplo, el Departamento de Estado, el Departamento de Justicia (incluido el FBI), el Departamento de Seguridad del Territorio Nacional, el Departamento de Defensa, la NSA, la CIA y la ODNI.

([105]) Según afirma el Gobierno de los Estados Unidos, si la Oficina de Privacidad y Libertades Civiles de la ODNI recibe una reclamación, se coordinará asimismo con otros servicios de inteligencia para determinar el curso que debe darse a la reclamación en tales servicios. Véase el documento sobre la figura del Defensor del Pueblo (anexo III), apartado 6, letra b), inciso ii).

([106]) Véase el título 42, artículo 2000ee-1, letra f), puntos 1 y 2, del USC.

([107]) Véase el dictamen n.º 1/2016 del Grupo de Trabajo del artículo 29, sobre el proyecto de decisión de adecuación sobre el Escudo de la privacidad UE-EE. UU. (adoptado el 13 de abril de 2016), p. 41.

([108]) Declaraciones de la ODNI (anexo VI), p. 7. Véanse, por ejemplo, NSA: *PPD-28 Section 4 Procedures* (Procedimientos en virtud del artículo 4 de la PPD-28), 12 de enero de 2015, apartado 8.1, y CIA: «Responsibilities» (Responsabilidades), *Signals Intelligence Activities* (Actividades de inteligencia de señales), p. 7.

([109]) Este inspector general (cuya figura fue creada en octubre de 2010) es nombrado por el presidente de los Estados Unidos, con el respaldo del Senado, y únicamente puede ser destituido por el presidente, nunca por el director de Inteligencia Nacional.

([110]) Estos inspectores generales gozan de garantías en el desempeño de sus funciones y solo pueden ser destituidos por el presidente, que deberá comunicar al Congreso por escrito los motivos de tal destitución. Ello no significa necesariamente que no puedan recibir ningún tipo de instrucciones. En algunos casos, el jefe del departamento podrá prohibir al inspector general que inicie, lleve a cabo o finalice una auditoría o investigación cuando se considere necesario en aras de importantes intereses nacionales (de seguridad). No obstante, el Congreso deberá ser informado del ejercicio de esta facultad y podrá exigir responsabilidades a este respecto al director correspondiente. Véanse, por ejemplo, la Inspector General Act (Ley de Inspectores Generales) de 1978, artículos 8 (Inspector General del Departamento de Defensa); 8E (Inspector General del Departamento de Justicia); 8G, letra d), punto 2, letras A y B (Inspector General de la NSA); así como el título 50, artículo 403q, letra b), del USC (Inspector General de la CIA), y la *Intelligence Authorization Act For Fiscal Year 2010* (Ley de Autorización de Actividades Inteligencia para el Ejercicio 2010), artículo 405, letra f) (Inspector General de los Servicios de Inteligencia). De acuerdo con la evaluación realizada por las autoridades nacionales de protección de datos, es probable que los inspectores generales cumplan el criterio de independencia organizativa según lo definido por el Tribunal de Justicia y el Tribunal Europeo de Derechos Humanos (TEDH), al menos a partir del momento en que el nuevo proceso de designación se aplique a todos. Véase el dictamen n.º 1/2016 del Grupo de Trabajo del artículo 29, sobre el proyecto de decisión de adecuación sobre el Escudo de la privacidad UE-EE. UU. (adoptado el 13 de abril de 2016), p. 40.

([111]) Véanse las declaraciones de la ODNI (anexo VI), p. 7. Véase también la *Inspector General Act* de 1978, en su versión modificada, Pub. L. (Ley de Derecho Público) 113-126 de 7 de julio de 2014.

auditorías, exámenes, documentos, escritos, recomendaciones u otro material pertinente, previa citación si es preciso, y pueden tomar declaración ([112]). Aunque los inspectores generales solo pueden formular recomendaciones no vinculantes de medidas correctoras, sus informes, incluidos los relativos al seguimiento (o a su ausencia), se ponen a disposición del público y se transmiten asimismo al Congreso, que puede ejercer su función de supervisión a este respecto ([113]).

(98) Por otro lado, el Privacy and Civil Liberties Oversight Board (Consejo de Supervisión de la Privacidad y de las Libertades Civiles), un órgano independiente ([114]) dentro del poder ejecutivo e integrado por un consejo bipartidista de cinco miembros ([115]) nombrados por el presidente con la aprobación del Senado, asume responsabilidades en el ámbito de la elaboración y aplicación de las políticas de lucha contra el terrorismo con miras a proteger la privacidad y las libertades civiles. En su control de la actividad de los servicios de inteligencia, podrá tener acceso a todos los registros, informes, auditorías, exámenes, documentos, escritos y recomendaciones, incluso a la información clasificada, así como realizar interrogatorios y tomar declaración. También recibe informes de los funcionarios de libertades civiles y privacidad de diversos departamentos y servicios federales ([116]), a los que puede formular recomendaciones, e informa periódicamente a las comisiones del Congreso y al presidente ([117]). El PCLOB se encarga asimismo de elaborar, dentro de los límites de su mandato, un informe de evaluación de la aplicación de la PPD-28.

(99) Por último, los mecanismos de supervisión anteriormente mencionados se complementan con la Intelligence Oversight Board (Junta de Supervisión de Inteligencia) del presidente, constituida en el seno de la Junta Asesora de Inteligencia del presidente, que supervisa el cumplimiento de la Constitución y de las demás normas pertinentes por parte de los servicios de inteligencia de los Estados Unidos.

(100) A fin de facilitar la supervisión, se insta a los servicios de inteligencia a que diseñen sistemas de información que permitan el seguimiento, el registro y la inspección de las consultas u otras búsquedas de información personal ([118]). Los organismos de supervisión y cumplimiento efectuarán controles periódicos de las prácticas de los servicios de inteligencia para proteger la información personal contenida en la inteligencia de señales y del cumplimiento de tales procedimientos de dichos servicios ([119]).

(101) Estas funciones de supervisión se encuentran asimismo respaldadas por amplios requisitos de notificación con respecto a los posibles incumplimientos. En particular, los procedimientos de los servicios de inteligencia deben garantizar que, cuando surja un problema importante de cumplimiento que afecte a información personal recabada mediante inteligencia de señales acerca de cualquier ciudadano, con independencia de su nacionalidad, deberá ser notificado cuanto antes al jefe del servicio en cuestión, que, a su vez, informará al director de Inteligencia Nacional con el fin de que este último, en virtud de la PPD-28, determine si es necesario adoptar medidas correctoras al respecto ([120]). Además, en virtud del EO 12333, todos los servicios de inteligencia tienen la obligación de comunicar los incumplimientos detectados a la Intelligence Oversight Board ([121]). Estos

([112]) Véase la Inspector General Act de 1978, artículo 6.

([113]) Véanse las declaraciones de la ODNI (anexo VI), p. 7. Véase la Inspector General Act de 1978, artículo 4, letra a), punto 5, y artículo 5. Con arreglo al artículo 405, letra b), puntos 3 y 4, de la Intelligence Authorization Act For Fiscal Year 2010 (Pub. L. 111-259 de 7 de octubre de 2010), el inspector general de los servicios de inteligencia mantendrá al director de Inteligencia Nacional y al Congreso informados acerca de la necesidad de emprender medidas correctoras y de la evolución de estas.

([114]) De acuerdo con la evaluación realizada por las autoridades nacionales de protección de datos, el PCLOB ha demostrado en el pasado sus «poderes independientes». Véase el dictamen n.º 1/2016 del Grupo de Trabajo del artículo 29, sobre el proyecto de decisión de adecuación sobre el Escudo de la privacidad UE-EE. UU., (adoptado el 13 de abril de 2016), p. 42.

([115]) Además, el PCLOB dispone de una plantilla fija de cerca de veinte empleados. Véase https://www.pclob.gov/about-us/staff.html

([116]) Entre ellos figuran, como mínimo, el Departamento de Justicia, el Departamento de Defensa, el Departamento de Seguridad del Territorio Nacional, el director de Inteligencia Nacional y la Agencia Central de Inteligencia, así como cualquier otro departamento, organismo o servicio del poder ejecutivo que el PCLOB considere pertinente.

([117]) Véase el título 42, artículo 2000ee, del USC. Véase el documento sobre la figura del Defensor del Pueblo (anexo III), apartado 6, letra b), inciso iv). Entre otras cosas, el PCLOB deberá informar cuando una agencia del ejecutivo se niegue a seguir su consejo.

([118]) ODNI: *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28* (Salvaguardar la información personal de todas las personas: un informe de situación sobre el desarrollo y la aplicación de los procedimientos previstos en la Directiva de Política Presidencial 28), pp. 7 y 8.

([119]) Véase la nota anterior, p. 8. Véanse también las declaraciones de la ODNI (anexo VI), p. 9.

([120]) ODNI: *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28* (Salvaguardar la información personal de todas las personas: un informe de situación sobre el desarrollo y la aplicación de los procedimientos previstos en la Directiva de Política Presidencial 28), p. 7. Véanse, por ejemplo, NSA: *PPD-28 Section 4 Procedures* (Procedimientos en virtud del artículo 4 de la PPD-28), 12 de enero de 2015, apartados 7.3 y 8.7, letras c) y d); FBI: *Presidential Policy Directive 28 Policies and Procedures* (Políticas y procedimientos en virtud de la PPD-28), apartado III, letra A, punto 4, y letra B, punto 4; y CIA: *Signals Intelligence Activities* (Actividades de inteligencia de señales), p. 6, «Compliance» (Cumplimiento), y p. 8, «Responsibilities» (Responsabilidades).

([121]) Véase el EO 12333, artículo 1.6, letra c).

mecanismos garantizan que el problema se aborde al más alto nivel en el ámbito de los servicios de inteligencia. Cuando el problema afecta a un ciudadano no estadounidense, el director de Inteligencia Nacional, en consulta con el secretario de Estado y el jefe del departamento o servicio notificante, determinará las medidas que deben adoptarse para informar al Gobierno extranjero pertinente, sin perjuicio de la protección de las fuentes y métodos y del personal de los Estados Unidos ([122]).

(102) En segundo lugar, aparte de estos mecanismos de supervisión dentro del poder ejecutivo, el Congreso de los Estados Unidos y, en particular, las *comisiones judiciales y de inteligencia de la Cámara de Representantes y del Senado,* poseen competencias de supervisión sobre todas las actividades de inteligencia exterior del país, incluidas las relacionadas con la inteligencia de señales. En virtud de la Ley de Seguridad Nacional, el presidente garantizará que las comisiones de inteligencia del Congreso reciban constantemente información completa y actualizada sobre las actividades de inteligencia de los Estados Unidos, incluida toda actividad significativa prevista con arreglo a lo dispuesto en el subcapítulo correspondiente ([123]). Asimismo, la citada ley dispone que el presidente velará por que se notifique cuanto antes a las comisiones de inteligencia del Congreso toda actividad de inteligencia ilegal, así como toda medida correctora que se haya adoptado o se prevea adoptar con respecto a dicha actividad ilegal ([124]). Los miembros de dichas comisiones disponen de acceso a información clasificada, así como a los métodos y programas de inteligencia ([125]).

(103) Posteriormente, se ha ido ampliando la legislación y se han perfeccionado los requisitos de notificación, tanto en lo concerniente a los servicios de inteligencia, como a los inspectores generales pertinentes y al fiscal general. Por ejemplo, la FISA exige al fiscal general que «informe plenamente» a las comisiones judiciales y de inteligencia del Senado y de la Cámara de Representantes acerca de las actividades llevadas a cabo por el Gobierno en virtud de determinados artículos de la FISA ([126]). Por otro lado, dispone que el Gobierno proporcione a las comisiones del Congreso copias de todas las resoluciones, autos o dictámenes del Foreign Intelligence Surveillance Court o del Foreign Intelligence Surveillance Court of Review que contengan interpretaciones significativas de las disposiciones de la FISA. En particular, por lo que respecta a la vigilancia en virtud del artículo 702 de la FISA, la supervisión se ejerce mediante la presentación de los informes prescritos por la legislación a las comisiones judiciales y de inteligencia, así como mediante la celebración de frecuentes reuniones informativas y audiencias. Entre los documentos presentados figuran un informe semestral del fiscal general en el que se describe la aplicación del artículo 702 de la FISA, acompañado de documentos justificativos, que incluyen, en particular, los informes de cumplimiento del Departamento de Justicia y de la ODNI y una descripción de los incumplimientos detectados ([127]), así como una evaluación semestral elaborada aparte por el fiscal general y el director de Inteligencia Nacional para documentar el cumplimiento de los procedimientos de fijación de objetivos y de minimización, incluida la observancia de los procedimientos concebidos para garantizar que la recopilación responda a una finalidad legítima de inteligencia exterior ([128]). El Congreso recibe también informes de los inspectores generales facultados para evaluar el cumplimiento de los servicios con los procedimientos de fijación de objetivos y de minimización y con las directrices del fiscal general.

(104) De conformidad con la USA Freedom Act de 2015, el Gobierno de los Estados Unidos debe facilitar cada año al Congreso (y al público) el número de mandamientos y directivas solicitados o recibidos en virtud de la FISA, así como estimaciones del número de ciudadanos estadounidenses y no estadounidenses sometidos a vigilancia, entre otros datos ([129]). La citada ley impone asimismo la obligación de divulgar el número de NSL emitidas tanto con

([122]) PPD-28, artículo 4, letra a), inciso iv).
([123]) Véase el artículo 501, letra a), punto 1 [USC, título 50, artículo 413, letra a), punto 1]. Esta disposición expone los requisitos generales aplicables a la supervisión por parte del Congreso en el ámbito de la seguridad nacional.
([124]) Véase el artículo 501, letra b) [USC, título 50, artículo 413, letra b)].
([125]) Véase el artículo 501, letra d) [USC, título 50, artículo 413, letra d)].
([126]) Véase el título 50, artículos 1808, 1846, 1862, 1871 y 1881f, del USC.
([127]) Véase el título 50, artículo 1881f, del USC.
([128]) Véase el título 50, artículo 1881a, letra l), punto 1, del USC.
([129]) Véase la USA Freedom Act de 2015, Pub. L. 114-23, artículo 602, letra a). Por otra parte, el artículo 402 dispone que el director de Inteligencia Nacional, en consulta con el fiscal general, llevará a cabo un examen desclasificatorio de todas las resoluciones, mandamientos o dictámenes dictados por el FISC o por el Foreign Intelligence Surveillance Court of Review (Tribunal de Apelación de Vigilancia de Inteligencia Exterior), tal como se define en el artículo 601, letra e), que contengan alguna interpretación significativa de cualquier disposición legal, incluida toda interpretación nueva o significativa de la expresión «término de selección específico», y, en función de dicho examen, poner a disposición del público en la medida de lo posible tales resoluciones, mandamientos o dictámenes.

respecto a ciudadanos estadounidenses como no estadounidenses (si bien, al mismo tiempo, permite a los destinatarios de mandamientos y certificaciones en virtud de la FISA y de solicitudes en forma de NSL presentar informes de transparencia en determinadas circunstancias) ([130]).

(105) En tercer lugar, las actividades de inteligencia desarrolladas por los poderes públicos de los Estados Unidos en virtud de la FISA pueden ser objeto de examen y, en algunos casos, estar sujetas a la autorización previa del FISA Court (Tribunal de la FISA; en lo sucesivo, «FISC») ([131]), un órgano jurisdiccional independiente ([132]) cuyas resoluciones pueden recurrirse ante el Foreign Intelligence Surveillance Court of Review (Tribunal de Apelación de Vigilancia de Inteligencia Exterior; en lo sucesivo, «FISCR») ([133]) y, en última instancia, ante el Tribunal Supremo de los Estados Unidos ([134]). En el supuesto de autorización previa, los servicios solicitantes (FBI, NSA, CIA, etc.) tendrán que presentar un proyecto de solicitud a los juristas de la División de Seguridad Nacional del Departamento de Justicia, que lo estudiarán y, cuando proceda, solicitarán información complementaria ([135]). Una vez finalizada la solicitud, habrá que obtener el visto bueno del fiscal general, el vicefiscal general o el fiscal general adjunto de Seguridad Nacional ([136]). A continuación, el Departamento de Justicia presentará la solicitud ante el FISC, que la evaluará y determinará de manera preliminar el modo de proceder ([137]). En caso de celebrarse una vista, el FISC está facultado para tomar declaración, incluso a expertos en la materia ([138]).

(106) El FISC (y el FISCR) cuenta con el apoyo de un grupo permanente de cinco expertos en materia de seguridad nacional y libertades civiles ([139]). El tribunal designará a uno de estos expertos como *amicus curiae* para que asista en el examen de cualquier solicitud de mandamiento o revisión que, a juicio del tribunal, presente una interpretación nueva o significativa del Derecho, salvo que el tribunal resuelva que no procede tal designación ([140]). Ello garantizará, en particular, que la apreciación del tribunal tenga debidamente en cuenta todas las consideraciones relativas a la privacidad. El tribunal también podrá designar *amicus curiae*, incluso para la prestación de asesoramiento técnico, a otras personas o entidades cuando lo estime oportuno, o autorizar, previa solicitud, la presentación de un escrito en calidad de *amicus curiae* por parte de cualquier persona o entidad ([141]).

([130]) USA Freedom Act, artículo 602, letra a), y artículo 603, letra a).

([131]) Para determinados tipos de vigilancia, el presidente del Tribunal Supremo de los Estados Unidos podrá designar públicamente un *magistrate judge* (juez de primera instancia e instrucción) con competencias para atender solicitudes y dictar mandamientos.

([132]) El FISC consta de once jueces nombrados por el presidente del Tribunal Supremo de los Estados Unidos de entre los jueces que integran los tribunales federales de distrito, que previamente han sido designados por el presidente de los Estados Unidos y confirmados por el Senado. Los jueces, que tienen cargos vitalicios y solo pueden ser destituidos en casos debidamente justificados, prestan servicio en el FISC por períodos escalonados de siete años. La FISA estipula que los jueces deben proceder de un mínimo de siete distritos judiciales federales distintos. Véanse el artículo 103 de la FISA [título 50, artículo 1803, letra a), del USC], así como el informe del PCLOB sobre el artículo 15, pp. 174-187. Los jueces son asistidos por letrados experimentados que integran el personal jurídico del tribunal y elaboran un análisis jurídico de las peticiones de recopilación. Véanse el informe del PCLOB sobre el artículo 215, p. 178, y la carta de Reggie B. Walton, presidente del Foreign Intelligence Surveillance Court, a Patrick J. Leahy, presidente de la Comisión Judicial del Senado de los Estados Unidos, de 29 de julio de 2013 (en lo sucesivo, «carta Walton»), pp. 2-3.

([133]) El FISCR está integrado por tres jueces nombrados por el presidente del Tribunal Supremo de los Estados Unidos de entre los jueces de tribunales federales de distrito o de apelación y prestan servicio por períodos escalonados de siete años. Véase el artículo 103 de la FISA [USC, título 50, artículo 1803, letra b)].

([134]) Véase el título 50, artículos 1803, letra b); 1861a, letra f); y 1881a, letras h) e i), punto 4, del USC.

([135]) Por ejemplo, datos fácticos complementarios sobre el objetivo de la vigilancia, información técnica sobre los métodos de vigilancia o garantías acerca de la manera en que se utilizará y difundirá la información. Véase el informe del PCLOB sobre el artículo 215, p. 177.

([136]) USC, título 50, artículos 1804, letra a), y 1801, letra g).

([137]) El FISC podrá dar el visto bueno a la solicitud, demandar más información, determinar la necesidad de celebrar una vista o indicar una posible denegación de la solicitud. Sobre la base esta determinación preliminar, el Gobierno presentará su solicitud definitiva. Esta última podrá contener modificaciones sustanciales con respecto a la solicitud original, en consonancia con las observaciones preliminares del juez. Si bien un elevado porcentaje de las solicitudes definitivas reciben el visto bueno del FISC, una parte importante de estas presentan modificaciones sustanciales con respecto a la solicitud original (por ejemplo, el 24 % de las solicitudes aprobadas para el período comprendido entre julio y septiembre de 2013). Véanse el informe del PCLOB sobre el artículo 215, p. 179, y la carta Walton, p. 3.

([138]) Informe del PCLOB, sobre el artículo 215, p. 179, nota 619.

([139]) USC, título 50, artículo 1803, letra i), puntos 1 y 3, letra A. Esta nueva legislación incorporó las recomendaciones del PCLOB relativas a la confección de una lista de expertos en privacidad y libertades civiles que puedan intervenir en calidad de *amicus curiae*, con objeto de proporcionar al tribunal argumentos jurídicos en favor de la privacidad y las libertades civiles. Véase el informe del PCLOB sobre el artículo 215, pp. 183 a 187.

([140]) USC, título 50, artículo 1803, letra i), punto 2, letra A. Con arreglo a la información facilitada por la ODNI, ya han tenido lugar tales designaciones. Véase *Signals Intelligence Reform: 2016 Progress Report* (Informe de 2016 sobre los avances de la reforma de la inteligencia de señales).

([141]) USC, título 50, artículo 1803, letra i), punto 2, letra B.

(107) La supervisión del FISC con respecto a los dos fundamentos jurídicos de vigilancia en virtud de la FISA que revisten mayor importancia para las transferencias de datos efectuadas en el marco del Escudo de la privacidad UE-EE. UU. varía de uno a otro.

(108) En virtud del artículo 501 de la FISA ([142]), que autoriza la recopilación de cualesquiera elementos tangibles, entre ellos libros, registros, escritos, documentos y otros efectos, la solicitud presentada al FISC debe contener una exposición de los hechos que demuestren la existencia de motivos fundados para pensar que tales elementos resultan pertinentes en el contexto de una investigación autorizada (distinta de una evaluación de amenazas) llevada a cabo con el fin de recabar información de inteligencia exterior que no se refiera a un ciudadano estadounidense o brindar protección contra el terrorismo internacional o actividades de inteligencia clandestinas. Por otra parte, la solicitud ha de contener una lista de los procedimientos de minimización adoptados por el fiscal general en lo referente a la conservación y difusión de la inteligencia recabada ([143]).

(109) En cambio, con arreglo al artículo 702 de la FISA ([144]), el FISC no autoriza medidas de vigilancia individuales, sino programas de vigilancia (como PRISM o Upstream) sobre la base de certificaciones anuales elaboradas por el fiscal general y el director de Inteligencia Nacional. El artículo 702 de la FISA permite fijar como objetivos de la adquisición de información de inteligencia exterior a personas de las que se tengan motivos fundados para pensar que se encuentran ubicadas fuera de los Estados Unidos ([145]). Estos objetivos son fijados por la NSA en dos fases: en primer lugar, los analistas de la NSA identificarán a los ciudadanos no estadounidenses ubicados en el extranjero cuya vigilancia vaya a conducir, con arreglo a la valoración de los analistas, a la obtención de la inteligencia exterior pertinente especificada en la certificación; en segundo lugar, una vez que estas personas específicas han sido identificadas y aprobadas como objetivos a través de un amplio mecanismo de examen dentro de la NSA ([146]), se asignan (es decir, se desarrollan y aplican) una serie de selectores que identifican los recursos de comunicación (por ejemplo, direcciones de correo electrónico) utilizados por dichas personas ([147]). Según se indica, las certificaciones que han de recibir el visto bueno del FISC no contienen información sobre las personas objetivo propiamente dichas, sino que identifican categorías de información de inteligencia exterior ([148]). Aunque el FISC no valora —sobre la base de la existencia de indicios razonables o de cualquier otra norma— si los objetivos fijados son adecuados para recabar información de inteligencia exterior ([149]), su control abarca la condición de que uno de los principales fines de la recopilación de datos sea obtener ese tipo de información ([150]). De hecho, el artículo 702 de la FISA permite a la NSA recabar comunicaciones de ciudadanos no estadounidenses ubicados fuera de los Estados Unidos únicamente cuando existan motivos fundados para pensar que un determinado medio de comunicación está siendo utilizado para transmitir información de inteligencia exterior (por ejemplo, relacionada con el terrorismo internacional, la proliferación de armas nucleares o actividades informáticas hostiles). Las determinaciones a este respecto son susceptibles de control jurisdiccional ([151]). Las certificaciones deben contemplar asimismo los procedimientos de fijación de objetivos y de minimización ([152]). El fiscal general y el director de Inteligencia Nacional verifican el cumplimiento y los servicios

([142]) USC, título 50, artículo 1861.
([143]) USC, título 50, artículo 1861, letra b).
([144]) USC, título 50, artículo 1881.
([145]) USC, título 50, artículo 1881a, letra a).
([146]) Informe del PCLOB sobre el artículo 702, p. 46.
([147]) USC, título 50, artículo 1881a, letra h).
([148]) USC, título 50, artículo 1881a, letra g). Según el PCLOB, hasta la fecha, estas categorías se han centrado principalmente en el terrorismo internacional y en temas como la adquisición de armas de destrucción masiva. Véase el informe del PCLOB sobre el artículo 702, p. 25.
([149]) Informe del PCLOB sobre el artículo 702, p. 27.
([150]) USC, título 50, artículo 1881a.
([151]) *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (Libertad y seguridad en un mundo cambiante: Informe y recomendaciones del Grupo Consultivo del Presidente en materia de inteligencia y tecnologías de la comunicación), 12 de diciembre de 2013, p. 152.
([152]) USC, título 50, artículo 1881a, letra i).

tienen la obligación de notificar cualesquiera incumplimientos detectados al FISC ([153]) (así como al Congreso y la Junta de Supervisión de Inteligencia del Presidente), que podrá modificar la autorización en función de estos ([154]).

(110) Asimismo, con vistas a mejorar la eficacia de la supervisión llevada a cabo por el FISC, el Gobierno de los Estados Unidos ha accedido a poner en práctica la recomendación del PCLOB de proporcionar al FISC documentación sobre las decisiones de fijación de objetivos en virtud del artículo 702, incluida una muestra aleatoria de hojas de asignación de selectores, de modo que el FISC pueda evaluar el cumplimiento en la práctica de la finalidad de inteligencia exterior exigida ([155]). Al mismo tiempo, el Gobierno estadounidense accedió también a revisar los procedimientos de fijación de objetivos de la NSA al objeto de documentar mejor los motivos de inteligencia exterior en que se basan las decisiones de fijación de objetivos, y ha adoptado una serie de medidas a este respecto ([156]).

Recursos individuales

(111) El Derecho estadounidense pone una serie de vías de recurso a disposición de los interesados de la UE que alberguen dudas sobre si sus datos personales han sido tratados (entre otros, mediante su recopilación o el acceso a los mismos) por los servicios de inteligencia de los Estados Unidos y, de ser así, si se han respetado las limitaciones previstas en tal Derecho. Estas se refieren básicamente a tres ámbitos: las injerencias previstas en la FISA; el acceso intencionado y no autorizado a datos personales por funcionarios públicos; y el acceso a información en virtud de la Freedom of Information Act (Ley de Libertad de Información; en lo sucesivo, «FOIA») ([157]).

(112) En primer lugar, la FISA contempla una serie de recursos, también a disposición de los ciudadanos no estadounidenses, para impugnar la vigilancia electrónica ilegal ([158]). Esto incluye la posibilidad para las personas de interponer una demanda de indemnización por daños y perjuicios económicos contra los Estados Unidos cuando se haya utilizado o divulgado información sobre ellas de manera intencionada y no autorizada ([159]); de demandar a funcionarios públicos estadounidenses a título personal («con apariencia de legalidad») por daños y perjuicios económicos ([160]); y de impugnar la legalidad de la vigilancia (y solicitar la supresión de la información) en el supuesto de que el Gobierno de los Estados Unidos pretenda utilizar o divulgar cualquier información obtenida o derivada de la vigilancia electrónica en contra del interesado en diligencias judiciales o administrativas emprendidas en dicho país ([161]).

(113) En segundo lugar, el Gobierno estadounidense indicó a la Comisión una serie de vías adicionales que los interesados de la UE podían utilizar para presentar un recurso contra determinados funcionarios por el acceso no

([153]) El artículo 13, letra b), del Reglamento del FISC dispone que, cuando el Gobierno detecte que el ejercicio de alguna autorización o visto bueno otorgado por el Tribunal no cumple lo dictaminado por este o la legislación aplicable, deberá comunicarlo de inmediato al Tribunal por escrito. Asimismo, exige al Gobierno que notifique por escrito al Tribunal los hechos y circunstancias que determinan dicho incumplimiento. Por lo general, el Gobierno presentará una comunicación definitiva en virtud del artículo 13, letra a), cuando se conozcan los hechos pertinentes y se haya destruido la información recopilada de manera ilegítima. Véase la carta Walton, p. 10.

([154]) USC, título 50, artículo 1881, letra l). Véanse también el informe del PCLOB sobre el artículo 702, pp. 66 a 76, y el informe de la NSA CLPO *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Aplicación del artículo 702 de la Ley de Vigilancia de Inteligencia Exterior por la NSA), 16 de abril de 2014. La recopilación de datos personales a efectos de inteligencia en virtud del artículo 702 de la FISA está sujeta a supervisión interna y externa en el ámbito del poder ejecutivo. La supervisión interna comprende, entre otras cosas, programas de cumplimiento interno que tienen por objeto evaluar y supervisar el cumplimiento de los procedimientos de fijación de objetivos y de minimización; la notificación de los incumplimientos detectados, tanto a nivel interno como externo, a la ODNI, al Departamento de Justicia, al Congreso y al FISC; e inspecciones anuales remitidas a los mismos organismos. En cuanto a la supervisión externa, consiste principalmente en inspecciones de las actividades de fijación de objetivos y de minimización por parte de la ODNI, del Departamento de Justicia y de los inspectores generales, que, a su vez, informan al Congreso y al FISC, indicando los posibles incumplimientos. Los incumplimientos graves deben ser comunicados al FISC de inmediato y, el resto, en informes trimestrales. Véase el informe del PCLOB sobre el artículo 702, pp. 66 a 77.

([155]) PCLOB, *Recommendations Assessment Report* (Informe de evaluación de recomendaciones), 29 de enero de 2015, p. 20.

([156]) PCLOB, *Recommendations Assessment Report* (Informe de evaluación de recomendaciones), 29 de enero de 2015, p. 16.

([157]) Por otro lado, el artículo 10 de la Classified Information Procedures Act (Ley de Procedimientos de Información Clasificada) dispone que, en todo proceso en el que los Estados Unidos deban demostrar que un determinado material constituye información clasificada (por ejemplo, porque requiera protección contra su divulgación no autorizada por motivos de seguridad nacional), el país comunicará al acusado las partes del material en las que tenga razonablemente previsto basarse para demostrar el elemento de información clasificada del delito.

([158]) Véanse las siguientes declaraciones de la ODNI (anexo VI), p. 16.

([159]) USC, título 18, artículo 2712.

([160]) USC, título 50, artículo 1810.

([161]) USC, título 50, artículo 1806.

autorizado a datos personales y la utilización de estos por parte el Gobierno, incluso con presuntos fines de seguridad nacional [a saber, la Computer Fraud and Abuse Act (Ley de Abuso y Fraude Informático) ([162]); la Electronic Communications Privacy Act (Ley de Privacidad de las Comunicaciones Electrónicas) ([163]); y la Right to Financial Privacy Act (Ley del Derecho a la Confidencialidad Financiera) ([164])]. Todos estos fundamentos jurídicos para incoar un procedimiento se refieren a datos, objetivos o tipos de acceso específicos (por ejemplo, el acceso remoto a un ordenador a través de Internet) y pueden invocarse en determinadas circunstancias (tales como la comisión de actos intencionados o premeditados, o actos al margen de las propias funciones, así como el padecimiento de daños) ([165]). La Administrative Procedure Act (Ley de procedimiento administrativo) ofrece una posibilidad de recurso más general (título 5, artículo 702 del USC) según la cual toda persona que sufra un perjuicio a causa de actuaciones de una agencia o que se haya visto adversamente afectada o perjudicada por la acción de una agencia, tiene derecho a interponer un recurso judicial. Esto incluye la posibilidad de solicitar al órgano jurisdiccional que declare ilegales y anule la actuación, los resultados y las conclusiones de la agencia que hayan resultado ser arbitrarios, caprichosos, un abuso de la facultad de apreciación, o de otro modo no conformes a Derecho ([166]).

(114) Por último, el Gobierno de los Estados Unidos ha señalado la FOIA como instrumento a disposición de los ciudadanos no estadounidenses para solicitar acceso a los registros que obran en poder de los servicios federales, en particular cuando estos contengan datos personales del interesado ([167]). Tal como está planteada, la FOIA no ofrece una vía de recurso individual propiamente dicha contra las injerencias en los datos personales, si bien podría, en principio, permitir a los interesados obtener acceso a la información pertinente que poseen los servicios de inteligencia nacional. Incluso en este sentido, las posibilidades parecen limitadas, ya que dichos servicios pueden retener la información comprendida en determinadas excepciones previstas, entre ellas el acceso a información de seguridad nacional clasificada y a información relativa a investigaciones policiales ([168]). Con todo, las personas pueden impugnar el recurso a tales excepciones por parte de los servicios de inteligencia nacional y solicitar procedimientos tanto de control administrativo como de control jurisdiccional.

(115) Si bien las personas, incluidos los interesados de la UE, disponen, por tanto, de una serie de vías de recurso cuando han sido objeto de vigilancia (electrónica) no autorizada a efectos de seguridad nacional, también es evidente que no están cubiertas todas las bases jurídicas que pueden invocar los servicios de inteligencia estadounidenses (por ejemplo, el EO 12333). Además, aunque los ciudadanos no estadounidenses dispongan, en principio, de la posibilidad de recurso jurisdiccional, como en el caso de la vigilancia en virtud de la FISA, los medios de acción previstos son limitados ([169]) y las demandas interpuestas por personas físicas (incluidos los ciudadanos estadounidenses) se declararán improcedentes cuando estas no puedan demostrar su legitimación ([170]), lo que restringe el acceso a los órganos jurisdiccionales ordinarios ([171]).

(116) Con miras a proporcionar una vía complementaria de recurso accesible a todos los interesados de la UE, el Gobierno de los Estados Unidos ha decidido crear una nueva figura, a saber, el Defensor del Pueblo, tal como se describe en la carta del Secretario de Estado a la Comisión, contenida en el anexo III de la presente Decisión. Dicha figura se basa en la designación, en virtud de la PPD-28, de un coordinador superior (con la categoría de subsecretario) en el seno del Departamento de Estado como punto de contacto para los gobiernos extranjeros que planteen cuestiones con respecto a las actividades de inteligencia de señales de los Estados Unidos, pero su cometido es mucho más amplio que el concepto original.

([162]) USC, título 18, artículo 1030.
([163]) USC, título 18, artículos 2701 a 2712.
([164]) USC, título 12, artículo 3417.
([165]) Declaraciones de la ODNI (anexo VI), p. 17.
([166]) USC, título 5, artículo 706, apartado 2, letra A).
([167]) USC, título 5, artículo 552. Existen leyes similares de ámbito estatal.
([168]) De ser así, lo normal es que la persona solo obtenga una respuesta tipo por la que el servicio se niegue a confirmar o desmentir la existencia de ningún tipo de registros. Véase ACLU/CIA, 710 F.3d 422 (D.C. Cir. [Tribunal de Apelación del Distrito de Columbia] 2014).
([169]) Véanse las declaraciones de la ODNI (anexo VI), p. 16. Con arreglo a las explicaciones facilitadas, las causas de acción previstas exigen, bien la existencia de *daños* (USC, título 18, artículo 2712; USC, título 50 artículo 1810), bien la demostración de que el *Gobierno pretende utilizar o divulgar información* obtenida o derivada de la vigilancia electrónica de la persona interesada contra dicha persona en *diligencias judiciales o administrativas* emprendidas en los Estados Unidos (USC, título 50, artículo 1806). No obstante, como ya ha señalado el Tribunal de Justicia en reiteradas ocasiones, para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada carece de relevancia que el interesado haya sufrido o no inconvenientes en razón de tal injerencia. Véase Schrems, apartado 89, y la jurisprudencia allí citada.
([170]) Dicho criterio de admisibilidad se desprende del requisito de «caso o controversia» establecido en el artículo III de la Constitución de los Estados Unidos.
([171]) Véase Clapper/Amnesty International USA, 133 S. Ct. [Tribunal Supremo] 1138, 1144 (2013). Por lo que respecta a la utilización de NSL, la USA Freedom Act [artículos 502, letra f), a 503] estipula que los requisitos de confidencialidad se deberán revisar periódicamente y que los *destinatarios* de NSL deberán ser informados cuando los hechos dejen de justificar la aplicación de alguno de estos requisitos [véanse las declaraciones de la ODNI (anexo VI), p. 13]. Sin embargo, esto no garantiza que se vaya a comunicar al interesado de la UE que ha sido objeto de una investigación.

(117) En particular, con arreglo a los compromisos contraídos por el Gobierno de los Estados Unidos, la figura del Defensor del Pueblo velará por que todas las reclamaciones individuales se investiguen y aborden adecuadamente y que todas las personas reciban una confirmación independiente del cumplimiento de la legislación estadounidense o, en caso de incumplimiento, de la subsanación consiguiente ([172]). Esta figura incluye el «Defensor del Pueblo en el ámbito del Escudo de la privacidad», es decir, el Subsecretario y otro personal, así como otros órganos de supervisión competentes para controlar los distintos elementos de los servicios de inteligencia en cuya cooperación se basará el Defensor del Pueblo en el ámbito del Escudo de la privacidad para tramitar las reclamaciones. En particular, cuando la solicitud de una persona se refiera a la compatibilidad de la vigilancia con la legislación estadounidense, el Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá confiar en organismos de supervisión independientes con competencias de investigación (como los inspectores generales o el PCLOB). En cada caso, el Secretario de Estado garantizará que el Defensor del Pueblo disponga de los medios para velar por que su respuesta a las peticiones individuales se base en toda la información necesaria.

(118) A través de esta «estructura compuesta», la figura del Defensor del Pueblo garantiza la supervisión independiente y la reparación individual. Además, la cooperación con otros organismos de supervisión garantiza el acceso a los conocimientos especializados necesarios. Por último, al imponer al Defensor del Pueblo en el ámbito del Escudo de la privacidad la obligación de confirmar el cumplimiento o subsanar cualquier incumplimiento, esta figura refleja el compromiso del Gobierno de los EE. UU. en su conjunto para abordar y resolver las reclamaciones de los ciudadanos de la UE.

(119) En primer lugar, a diferencia de un mero mecanismo intergubernamental, el Defensor del Pueblo en el ámbito del Escudo de la privacidad recibirá y responderá a reclamaciones individuales. Tales reclamaciones podrán dirigirse a las autoridades de supervisión de los Estados miembros competentes en materia de supervisión de los servicios de seguridad nacional y/o del tratamiento de los datos personales por las autoridades públicas, que las dirigirán a un organismo centralizado a escala de la UE que las remitirá al Defensor del Pueblo en el ámbito del Escudo de la privacidad ([173]). De hecho, esto beneficiará a los ciudadanos de la UE, que podrán acudir a una autoridad nacional cerca de su lugar de residencia y en su propia lengua. Corresponderá a dicha autoridad ayudar al reclamante a presentar una instancia al Defensor del Pueblo en el ámbito del Escudo que contenga la información esencial, de modo que pueda considerarse «completa». El reclamante no tendrá que demostrar que el Gobierno estadounidense ha accedido, de hecho, a sus datos personales mediante actividades de inteligencia de señales.

(120) En segundo lugar, el Gobierno de los EE. UU., se compromete a garantizar que, en el ejercicio de sus funciones, el Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá apoyarse en la cooperación de otros mecanismos de verificación del cumplimiento y de supervisión previstos en el Derecho estadounidense. Esto implicará a veces a las autoridades nacionales de inteligencia, en particular si la petición debe interpretarse como de acceso a los documentos con arreglo a la Ley de libertad de información. En otros casos, en particular cuando las peticiones se refieran a la compatibilidad de la vigilancia con la legislación estadounidense, tal cooperación implicará a organismos de supervisión independientes (por ejemplo, inspectores generales) con responsabilidad y competencia para llevar a cabo una investigación en profundidad (en particular mediante el acceso a todos los documentos pertinentes) y para solicitar información y declaraciones y abordar los casos de incumplimiento ([174]). Además, el Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá transmitir asuntos al PCLOB para su examen ([175]). En los casos en que se haya detectado algún incumplimiento por parte de uno de estos organismos de supervisión, el servicio de inteligencia en cuestión (por ejemplo, una agencia de inteligencia) deberá corregir el incumplimiento, ya que solo de este modo podrá el Defensor del Pueblo garantizar una respuesta «positiva» a la persona (es decir, que se ha subsanado el incumplimiento), con arreglo al compromiso

([172]) En caso de que el denunciante solicite acceso a documentos que obren en poder de las autoridades de los Estados Unidos, se aplicarán las normas y los procedimientos establecidos en la Freedom of Information Act (Ley de la libertad de información). Esto incluye la posibilidad de buscar reparación judicial (en lugar de una supervisión independiente) en caso de que la solicitud sea rechazada, de conformidad con las condiciones establecidas en dicha Ley.

([173]) Con arreglo al apartado 4, letra f), del documento sobre la figura del Defensor del Pueblo (anexo III), el Defensor del Pueblo en el ámbito del Escudo de la privacidad se comunicará directamente con el organismo de la UE encargado de la tramitación de reclamaciones individuales, que se ocupará, a su vez, de entablar comunicación con el reclamante. Aunque las comunicaciones directas forman parte de los «procesos subyacentes» que permiten obtener la reparación solicitada (por ejemplo, una petición de acceso en virtud de la FOIA; véase el apartado 5 del documento anteriormente citado), dichas comunicaciones deberán llevarse a cabo de conformidad con los procedimientos aplicables.

([174]) Véase el documento sobre la figura del Defensor del Pueblo [anexo III, apartado 2, letra a)]. Véanse también los considerandos 96 y 97.

([175]) Véase el documento sobre la figura del Defensor del Pueblo [anexo III, apartado 2, letra c)]. De las explicaciones proporcionadas por el Gobierno de los Estados Unidos se desprende que el PCLOB someterá a constantes revisiones tanto las políticas y procedimientos de las autoridades estadounidenses competentes en materia de lucha contra el terrorismo como la aplicación de los mismos, a fin de determinar si las actividades de dichas autoridades «ofrecen una protección adecuada de la privacidad y las libertades civiles y si son conformes con las disposiciones legislativas, reglamentarias y normativas aplicables en tales ámbitos». Asimismo, «recibirá y examinará informes y otra información de los funcionarios de privacidad y de libertades civiles y, cuando proceda, les formulará recomendaciones sobre sus actividades».

del Gobierno de los EE. UU. Asimismo, en el marco de la cooperación, el Defensor del Pueblo en el ámbito del Escudo de la privacidad será informado de los resultados de la investigación, y el Defensor del Pueblo dispondrá de medios para garantizar que recibe toda la información necesaria para preparar su respuesta.

(121) Por último, el Defensor del Pueblo en el ámbito del Escudo de la privacidad será un órgano independiente de los servicios de inteligencia de los Estados Unidos y, por tanto, no recibirá ningún tipo de instrucciones de estos ([176]). Este punto reviste suma importancia, ya que el Defensor del Pueblo tendrá que «confirmar» que: i) la reclamación se ha investigado correctamente, y que ii) se ha observado el Derecho estadounidense pertinente, incluidas en particular las limitaciones y salvaguardias previstas en el anexo VI o, en caso de incumplimiento, que este se ha subsanado. A efectos de poder emitir esa confirmación independiente, el Defensor del Pueblo en el ámbito del Escudo de la privacidad tendrá que recibir la información necesaria en relación con la investigación, a fin de evaluar la exactitud de la respuesta a la reclamación. Además, el Secretario de Estado se ha comprometido a garantizar que el Subsecretario lleve cabo la función del Defensor del Pueblo en el ámbito del Escudo de la privacidad con objetividad y libre de cualquier influencia indebida que pueda afectar a la respuesta que vaya a darse.

(122) En general, este mecanismo garantiza que las reclamaciones individuales se investiguen minuciosamente y se resuelvan, y que al menos en el ámbito de la vigilancia, intervengan organismos de supervisión independientes con la experiencia y las facultades de investigación necesarias, así como un Defensor del Pueblo que pueda llevar a cabo sus funciones sin influencias inadecuadas, en particular políticas. Además, las personas podrán presentar reclamaciones sin tener que demostrar, ni proporcionar indicaciones, de que han sido objeto de vigilancia ([177]). A la luz de estos elementos, la Comisión considera que existen garantías adecuadas y eficaces contra el abuso.

(123) Sobre la base de todo lo expuesto, la Comisión concluye que los Estados Unidos garantizan una tutela judicial efectiva contra las injerencias de sus servicios de inteligencia en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a los Estados Unidos en el marco del Escudo de la privacidad UE-EE. UU.

(124) A este respecto, la Comisión toma nota de la sentencia del Tribunal de Justicia en el asunto Schrems, según la cual «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» ([178]). La evaluación de la Comisión ha confirmado que tales acciones están previstas en los Estados Unidos, en particular a través de la introducción de la figura del Defensor del Pueblo. Esta figura dispone de poderes de supervisión independiente con competencias de investigación. En el marco de su supervisión continua del Escudo de la privacidad, en particular a través de la revisión conjunta anual en la que también participará el Defensor del Pueblo, la Comisión revisará la eficacia de este mecanismo.

3.2. *Acceso y utilización por parte de los poderes públicos estadounidenses a efectos de aplicación de la ley y de otros fines de interés público*

(125) Por lo que respecta a las injerencias en los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. a efectos de aplicación de la ley, el Gobierno de los Estados Unidos (a través del Departamento de Justicia) ha ofrecido garantías en cuanto a las limitaciones y salvaguardias aplicables, que, a juicio de la Comisión, ponen de manifiesto un nivel de protección adecuado.

([176]) Véase *Roman Zakharov v. Russia*, sentencia de 4 de diciembre de 2015 (Gran Sala), demanda n.º 47143/06, apartado 275 (si bien en principio es conveniente confiar el control de supervisión a un juez, la supervisión por órganos no judiciales puede considerarse compatible con el Convenio, siempre que el organismo de supervisión sea independiente de las autoridades encargadas de la vigilancia y tenga poderes de supervisión suficientes y eficaces).

([177]) Véase Kennedy c. the United Kingdom, sentencia de 18 de mayo de 2010, demanda n.º 26839/05, apartado 167.

([178]) Schrems, apartado 95. Como se desprende de los apartados 91 y 96 de la sentencia, el apartado 95 hace referencia al nivel de protección garantizado en el ordenamiento jurídico de la Unión, al que el nivel de protección en el tercer país debe ser «esencialmente equivalente». Según los apartados 73 y 74 de la sentencia, ello no supone que el nivel de protección o los medios para que el tercer país recurra deberán ser idénticos, a pesar de que los medios utilizados deberán demostrar, en la práctica, ser eficaces.

(126) Con arreglo a esta información, la Enmienda IV a la Constitución de los Estados Unidos ([179]) dispone que los registros e incautaciones por parte de las fuerzas y cuerpos de seguridad ([180]) requieren un mandamiento judicial por indicios razonables. En las contadas excepciones específicas previstas en las que no es necesario obtener dicho mandamiento ([181]), la adopción de medidas coercitivas queda supeditada a una prueba de «razonabilidad» ([182]). La razonabilidad de un registro o incautación se determina mediante la apreciación, por un lado, de la medida en que supone una invasión de la intimidad de una persona y, por otro, de la medida en que es necesario en aras de intereses gubernamentales legítimos ([183]). En un sentido más amplio, la Enmienda IV garantiza la privacidad y la dignidad y brinda protección frente a actos arbitrarios e invasivos de funcionarios públicos ([184]). Estos conceptos plasman la idea de necesidad y proporcionalidad del Derecho de la Unión. En cuanto las fuerzas y cuerpos de seguridad ya no necesiten los elementos incautados como pruebas, deberán ser devueltos ([185]).

(127) Aunque el derecho de la Enmienda IV no se extiende a los ciudadanos no estadounidenses que no residan en los Estados Unidos, estos se benefician de manera indirecta de su protección, dado que los datos personales obran en poder de empresas estadounidenses con el efecto de que las fuerzas y cuerpos de seguridad deben contar con autorización judicial o, al menos, respetar el requisito de razonabilidad ([186]). Se prevén garantías adicionales en actos legislativos específicos, así como en las directrices del Departamento de Justicia, que limitan el acceso de las fuerzas y cuerpos de seguridad a los datos por razones similares a los principios de necesidad y proporcionalidad (por ejemplo, al exigir al FBI el empleo de métodos de investigación lo menos intrusivos posible, teniendo en cuenta su repercusión en la privacidad y las libertades civiles) ([187]). Según declara el Gobierno estadounidense, en el caso de las investigaciones policiales de ámbito estatal se aplican, como mínimo, las mismas garantías (con respecto a las investigaciones llevadas a cabo al amparo del Derecho estatal) ([188]).

(128) Aunque no es necesario obtener una autorización judicial previa de un tribunal o un gran jurado (sección del tribunal encargada de la instrucción y constituida por un juez o magistrado) en todos los casos ([189]), los requerimientos administrativos se limitan a casos concretos y se someterán a un control jurisdiccional independiente, como mínimo, cuando el Gobierno solicite su ejecución ante los tribunales ([190]).

([179]) Según la Enmienda IV, el derecho de los ciudadanos a la seguridad de sus personas, hogares, documentos y efectos frente a registros e incautaciones no razonables no podrá vulnerarse, y solo podrán emitirse órdenes con causa probable, apoyadas por juramento o promesa, y que describan en particular el lugar que deba registrarse y las personas o cosas que deban incautarse. Solo los jueces podrán emitir órdenes de registro. Las órdenes federales para la copia de información almacenada de forma electrónica se rigen por la norma 41 de las normas federales de enjuiciamiento criminal.

([180]) El Tribunal Supremo se ha referido en numerosas ocasiones a los registros sin órdenes como «excepcionales». Véase, por ejemplo, Johnson v. United States, 333 U.S. 14, 10 (1948); McDonald v. United States, 335 U.S. 453, 451 (1948); Camara V. Municipal Court, 387 US 523, 528-29 (1967); G.M. Leasing Corp. v. United States, 429 U.S. 355, 338-352, 53 (1977). Del mismo modo, el Tribunal Supremo subraya regularmente que la norma constitucional más básica en este ámbito es que los registros efectuados al margen del proceso judicial, la aprobación previa de un juez o magistrado, son per se abusivos con arreglo a la Enmienda IV, y solo se justifican por algunas excepciones específicas y bien delimitadas. Véase por ejemplo Coolidge v. New Hampshire, 403 US 443, 454-55 (1971); G.M. Leasing Corp. v. United States, 429 U.S. 358, 338-352, 53 (1977).

([181]) City of Ontario, California v. Quon, 130 S. Ct. [Tribunal Supremo] 2619, 2630 (2010).

([182]) Informe del PCLOB sobre el artículo 215, p. 107, en relación con la sentencia Maryland v. King, 133 S. Ct. 1958, 1970 (2013).

([183]) Informe del PCLOB sobre el artículo 215, p. 107, en relación con la sentencia Samson v. California, 547 S. Ct. 843, 848 (2006).

([184]) City of Ontario, California v. Quon, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Véase, por ejemplo, United Sates v. Wilson, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Véase Roman Zakharov v. Russia, sentencia de 4.12.2015 (Gran Sala), demanda n.º 47143/06, apartado 269, según la cual la obligación de mostrar una autorización de interceptación al proveedor de servicios de comunicaciones antes de obtener acceso a las comunicaciones de una persona es una de las salvaguardias importantes contra los abusos por parte de las fuerzas y cuerpos de seguridad, al garantizar que se obtiene la debida autorización en todos los casos de interceptación.

([187]) Declaraciones del Departamento de Justicia (anexo VII), p. 4, y las referencias allí citadas.

([188]) Declaraciones del Departamento de Justicia (anexo VII), nota 2.

([189]) Con arreglo a la información proporcionada a la Comisión y exceptuando algunos ámbitos específicos que es poco probable que incidan en las transferencias de datos efectuadas en el marco del Escudo de la privacidad UE-EE. UU. (por ejemplo, investigaciones de casos de fraude sanitario, maltrato infantil o sustancias controladas), este requisito es aplicable principalmente a determinadas facultades en virtud de la Electronic Communications Privacy Act (Ley de Privacidad de las Comunicaciones Electrónicas), concretamente a las peticiones de información básica sobre los abonados, sesiones y facturación [USC, título 18, artículo 2703, letra c), puntos 1 y 2, por ejemplo dirección, tipo y duración del servicios] y al contenido de los correos electrónicos con más de 180 días de antigüedad [USC, título 18, artículo 2703, letras a) y b)]. No obstante, en este último caso se tendrá que enviar una notificación al interesado, de modo que este tenga la oportunidad de impugnar la petición ante los órganos jurisdiccionales competentes. Véase también el resumen en DOJ *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (Registro e incautación de ordenadores, y obtención de pruebas electrónicas en las investigaciones penales), capítulo 3: The Stored Communications Act (Ley sobre comunicaciones almacenadas) pp. 115-138.

([190]) De conformidad con las declaraciones del Gobierno de los Estados Unidos, los destinatarios de requerimientos administrativos tendrán derecho a recurrirlos ante los órganos jurisdiccionales si consideran que son abusivos, es decir, desmesurados, opresivos o gravosos. Véanse las declaraciones del Departamento de Justicia (anexo VII), p. 2.

(129) Ocurre lo mismo en el caso de los requerimientos administrativos con fines de interés público. Además, de acuerdo con las declaraciones del Gobierno estadounidense, se aplican limitaciones sustantivas similares en el sentido de que los servicios de inteligencia solo podrán solicitar acceso a los datos que resulten pertinentes en relación con asuntos que sean de su competencia y deben atenerse al criterio de razonabilidad.

(130) Por otra parte, la legislación estadounidense establece una serie de vías de recurso judicial para personas contra una autoridad pública o uno de sus funcionarios, cuando dichas autoridades traten datos personales. Estas vías, que incluyen, en particular, la Administrative Procedure Act (Ley de procedimiento administrativo) (APA), la Freedom of Information Act (Ley de libertad de información) (FOIA), y la Electronic Communications Privacy Act (Ley de protección de la intimidad de las comunicaciones electrónicas) (ECPA) están abiertas a todas las personas, con independencia de su nacionalidad, siempre que se cumplan los requisitos aplicables.

(131) En general, en virtud de las disposiciones sobre revisión judicial de la Ley de procedimiento administrativo ([191]), toda persona que sufra un perjuicio a causa de actuaciones de una agencia, o que se haya visto adversamente afectada o perjudicada por la acción de una agencia, tiene derecho a interponer un recurso judicial ([192]). Esto incluye la posibilidad de solicitar al órgano jurisdiccional que declare ilegales y anule la actuación, los resultados y las conclusiones de la agencia que hayan resultado ser arbitrarios, caprichosos, un abuso de la facultad de apreciación, o de otro modo no conformes a Derecho ([193]).

(132) Más concretamente, el título II de la Ley de protección de la intimidad de las comunicaciones electrónicas ([194]) establece un régimen legal de derechos de privacidad y, como tal, regula el acceso de los cuerpos y fuerzas de seguridad a los contenidos de las comunicaciones telefónicas, verbales o electrónicas, almacenados por proveedores de servicios terceros ([195]). Esta norma tipifica el acceso ilegal (es decir, no autorizado por un tribunal o admisible de otro modo) a estas comunicaciones y prevé el derecho de las personas afectadas a interponer una acción civil ante un Tribunal federal de los Estados Unidos por daños reales e indemnizaciones, así como demandas de resoluciones declarativas o equitativas contra un funcionario gubernamental que haya cometido deliberadamente tales actos ilícitos, o contra los Estados Unidos.

(133) Asimismo, con arreglo a la Ley de libertad de información (FOIA, por sus siglas en inglés, título 5 del USC, apartado 552), cualquier persona tiene derecho a obtener acceso a los registros de las agencias federales y, en caso de agotamiento de las vías de recurso administrativo, ejercer tal derecho ante los tribunales, salvo en la medida en que dichos registros estén protegidos frente a la divulgación por una exención o exclusión policial especial ([196]).

([191]) USC, título 5, artículo 702.

([192]) Por lo general, solo las actuaciones «definitivas» de las agencias, en lugar de las actuaciones «preliminares, procesales, o intermedias», están sujetas a control judicial. Véase USC, título 5, artículo 704.

([193]) USC, título 5, artículo 706, apartado 2, letra A).

([194]) USC, título 18, artículos 2701 a 2712.

([195]) La ECPA protege las comunicaciones mantenidas por dos tipos de proveedores del servicio de red, a saber: prestadores de i) servicios de comunicaciones electrónicas, por ejemplo telefonía o correo electrónico; y ii) servicios informáticos remotos como servicios de tratamiento o almacenamiento informático.

([196]) No obstante, estas exclusiones están enmarcadas. Por ejemplo, según USC, título 5, artículo 552, letra b), inciso 7), los derechos de la FOIA se excluyen para los registros o información recogidos con fines policiales, pero únicamente en la medida en que la presentación de dicha información o registros policiales a) pueda esperarse razonablemente que interfiera con procedimientos de los cuerpos y fuerzas de seguridad; b) tenga el efecto de privar a una persona de su derecho a un juicio justo o una adjudicación imparcial; c) pueda pensarse razonablemente que constituye una intromisión injustificada en la vida privada; d) pueda esperarse razonablemente que revelaría la identidad de una fuente confidencial, en particular una autoridad o agencia estatal, local o extranjera o entidad privada que haya proporcionado información de forma confidencial y, en el caso de un registro o información recopilada por las autoridades policiales en el curso de una investigación penal o por una agencia que efectúe una investigación de seguridad nacional, la información facilitada por una fuente confidencial; e) revelaría técnicas y procedimientos de las investigaciones policiales o de los procesos penales, o revelaría directrices para las investigaciones policiales y enjuiciamientos, cuando pueda suponerse razonablemente que tal divulgación podría acarrear el riesgo de elusión de la ley; o f) pueda esperarse razonablemente que ponga en peligro la vida o la integridad física de alguna persona. Asimismo, cuando se presente una solicitud que implique el acceso a registros cuya obtención pueda razonablemente esperarse que interfiera con los procedimientos de ejecución, y a) la investigación o procedimiento se refiere a un posible delito penal, y b) haya razones para creer que: i) el sujeto de la investigación o procedimiento no tiene conocimiento del mismo, y que ii) la revelación de la existencia de los registros permita razonablemente pensar que interferirá con los procedimientos de ejecución, la agencia podrá, solo durante el tiempo en que se dé esta circunstancia, tratar los registros como si no estuviesen sujeto a los requisitos de este artículo [USC, título 18, artículo 552, letra c), inciso 1].

(134) Además, otros textos legislativos tales como la Wiretap Act (Ley de escuchas) ([197]), la Computer Fraud and Abuse Act (Ley de abuso y fraude informático) ([198]), la Federal Torts Claim Act (Ley federal de responsabilidad extracontractual) ([199]), la Right to Financial Privacy Act (Ley sobre el derecho a la privacidad financiera) ([200]), y la Fair Credit Reporting Act (Ley de informes de crédito justos) ([201]) confieren a los particulares el derecho a iniciar acciones contra una autoridad o funcionario público estadounidense con respecto al tratamiento de sus datos personales.

(135) Por consiguiente, la Comisión concluye que en los Estados Unidos existen normas destinadas a garantizar que las posibles injerencias cometidas a efectos de aplicación de la ley ([202]) y de otros fines de interés público en los derechos fundamentales de las personas cuyos datos personales se transfieran desde la Unión a los Estados Unidos en el marco del Escudo de la privacidad UE-EE. UU. se limiten a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que proporcionan una tutela judicial efectiva frente a tales injerencias.

4. NIVEL DE PROTECCIÓN ADECUADO EN EL MARCO DEL ESCUDO DE LA PRIVACIDAD UE-EE. UU.

(136) A la luz de las constataciones anteriormente expuestas, la Comisión considera que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades autocertificadas en el marco del Escudo de la privacidad UE-EE. UU.

(137) En particular, la Comisión estima que los principios de privacidad establecidos por el Departamento de Comercio de los Estados Unidos garantizan, en su conjunto, un nivel de protección de los datos personales sustancialmente equivalente al brindado por los principios básicos consagrados en la Directiva 95/46/CE.

(138) Además, las obligaciones en materia de transparencia y la administración del Escudo de la privacidad por parte del Departamento de Comercio garantizan la aplicación efectiva de los principios.

(139) Por otra parte, la Comisión considera que, en su conjunto, los mecanismos de recurso y supervisión previstos por el Escudo de la privacidad permiten identificar y sancionar en la práctica las vulneraciones de los principios de privacidad cometidas por las organizaciones pertenecientes a dicho marco y ofrecen al interesado la posibilidad de ejercer acciones en Derecho para acceder a los datos personales que le conciernen y, en último término, obtener su rectificación o supresión.

(140) Por último, sobre la base de la información disponible acerca del ordenamiento jurídico de los Estados Unidos, incluidas las declaraciones y compromisos prestados por el Gobierno estadounidense, la Comisión opina que las injerencias de los poderes públicos de los Estados Unidos en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a dicho país en el marco del Escudo de la privacidad a efectos de seguridad nacional, aplicación de la ley u otros fines de interés público, y las consiguientes restricciones impuestas a las entidades autocertificadas con respecto a su adhesión a los principios de privacidad, se limitarán a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que existe una tutela judicial efectiva frente a tales injerencias.

([197]) USC, título 18, artículo 2510 y ss. Con arreglo a la Ley de escuchas (USC, título 18, artículo 2520), una persona cuya comunicación por cable, oral o electrónica sea interceptada, divulgada o utilizada intencionadamente, podrá interponer una acción civil por violación de la Ley, incluso en determinadas circunstancias contra un funcionario concreto del Gobierno o los Estados Unidos. Por lo que respecta a la recopilación de direcciones y demás información sin contenido (por ejemplo, dirección IP, dirección de correo electrónico de envío o remitente), véase también el capítulo sobre *Pen Registers and Trap and Trace Devices* (Dispositivos de identificación y registro de llamadas entrantes y salientes) del título 18 (USC, título 18, artículos 3121-3127 y, respecto de la acción civil, el artículo 2707).

([198]) USC, título 18, artículo 1030. Con arreglo a la Ley de abuso y fraude informático, una persona podrá interponer una demanda contra cualquier persona por el acceso intencionado no autorizado (o que haya excedido el acceso autorizado) a fin de obtener información de una institución financiera, un sistema informático de la administración estadounidense u otro ordenador específico, y en particular, en determinadas circunstancias, contra un funcionario gubernamental concreto.

([199]) USC, título 28, artículo 2671 y ss. En virtud de la Ley federal de responsabilidad extracontractual, una persona podrá interponer una demanda, en determinadas circunstancias, contra los Estados Unidos por lo que se refiere a un acto u omisión negligente o ilegal de cualquier empleado de las administraciones públicas que actúe en el ámbito de su cargo o empleo.

([200]) USC, título 12, artículo 3401 y ss. En virtud de la Ley sobre el derecho a la privacidad financiera, una persona podrá interponer una demanda, en determinadas circunstancias, contra los Estados Unidos por lo que respecta a la obtención o divulgación de documentos financieros protegidos, en violación de la ley. El acceso de las autoridades públicas a los documentos financieros protegidos está por lo general prohibido, salvo que el Gobierno presente la solicitud con sujeción a una citación o una orden de registro o, con ciertas limitaciones, una solicitud formal por escrito, y la persona cuya información se solicita reciba una notificación de tal solicitud.

([201]) USC, título 15, artículos 1681-1681X. En virtud de la Ley de informes de crédito justos, una persona podrá interponer una demanda contra toda persona que incumpla los requisitos (en particular la necesidad de una autorización legal) en relación con la recopilación, la difusión y el uso de informes de crédito al consumo, o en determinadas circunstancias, contra un organismo estatal.

([202]) El Tribunal de Justicia ha reconocido que la aplicación de la ley constituye un objetivo político legítimo. Véanse los asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y Otros, EU:C:2014:238, apartado 42. Véase asimismo el artículo 8, apartado 2, del CEDH y la sentencia del Tribunal Europeo de Derechos Humanos en Weber y Saravia v. Alemania, demanda n.º 54934/00, apartado 104.

(141) La Comisión concluye que la protección ofrecida se ajusta a las exigencias previstas en el artículo 25 de la Directiva 95/46/CE, interpretada a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, tal como expone el Tribunal de Justicia, en particular, en su sentencia Schrems.

5. ACTUACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS E INFORMACIÓN A LA COMISIÓN

(142) En la sentencia Schrems, el Tribunal de Justicia aclaró que la Comisión no tiene competencias para limitar las facultades que el artículo 28 de la Directiva 95/46/CE atribuye a las APD (incluida la facultad de suspender las transferencias de datos) en el supuesto de que, con ocasión de una reclamación basada en esa disposición, alguna persona cuestione la compatibilidad de una decisión de adecuación adoptada por la Comisión con el respeto del derecho fundamental a la intimidad y a la protección de datos ([203]).

(143) Con miras a controlar de manera eficaz el funcionamiento del Escudo de la privacidad, los Estados miembros deben informar a la Comisión de cualquier medida pertinente emprendida por las APD.

(144) Por otro lado, el Tribunal de Justicia observó que, de conformidad con el artículo 25, apartado 6, párrafo segundo, de la Directiva 95/46/CE, los Estados miembros y sus órganos deben adoptar las medidas necesarias para dar cumplimiento a los actos de las instituciones de la Unión, los cuales 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. Por consiguiente, toda decisión de adecuación adoptada por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE vincula a todos los órganos de los Estados miembros destinatarios, entre los que se incluyen las autoridades de control independientes ([204]). En el supuesto de que alguna de estas autoridades haya recibido una reclamación que cuestione la compatibilidad de una decisión de adecuación adoptada por la Comisión con el respeto del derecho fundamental a la intimidad y a la protección de datos y considere fundadas las alegaciones expuestas, el Derecho nacional deberá proporcionar a dicha autoridad una vía de recurso que le permita exponer tales alegaciones ante los órganos jurisdiccionales nacionales, los cuales, en caso de duda, estarán obligados a suspender el procedimiento y a plantear una cuestión prejudicial al Tribunal de Justicia ([205]).

6. REVISIÓN PERIÓDICA DE LA CONSTATACIÓN DE ADECUACIÓN

(145) Habida cuenta de que el nivel de protección brindado por el ordenamiento jurídico de los Estados Unidos podría experimentar modificaciones, la Comisión, a raíz de la adopción de la presente Decisión, comprobará periódicamente si siguen siendo fundadas en Derecho y de hecho las constataciones relativas a la adecuación del nivel de protección garantizado por los Estados Unidos en virtud del Escudo de la privacidad UE-EE. UU. En cualquier caso, esa comprobación será obligada cuando la Comisión tenga conocimiento de cualquier indicio que genere una duda razonable en ese sentido ([206]).

(146) Por consiguiente, la Comisión llevará a cabo un seguimiento continuo del marco general para la transferencia de datos personales creado mediante el Escudo de la privacidad UE-EE. UU., así como del cumplimiento por parte de las autoridades estadounidenses de las declaraciones y compromisos recogidos en los documentos adjuntos a la presente Decisión. Para facilitar este proceso, los Estados Unidos se han comprometido a informar a la Comisión de las novedades que se produzcan en la legislación estadounidense si resultan pertinentes para el Escudo de la privacidad en el ámbito de la protección de datos y las limitaciones y garantías aplicables al acceso a datos personales por parte de las autoridades públicas. Asimismo, la presente Decisión se someterá a una revisión conjunta anual que abarcará todos los aspectos del funcionamiento del Escudo de la privacidad UE-EE. UU., incluida la aplicación de excepciones a los principios. Además, habida cuenta de que la constatación de adecuación también puede verse influida por cambios legislativos en el Derecho de la Unión, la Comisión evaluará el nivel de protección que ofrece el Escudo de la privacidad tras el comienzo de la aplicación del Reglamento general de protección de datos.

(147) Para llevar a cabo la revisión conjunta anual prevista en los anexos I, II y VI, la Comisión se reunirá con el Departamento de Comercio y la FTC, acompañados, si procede, por otros departamentos y servicios que intervengan en la aplicación del régimen del Escudo de la privacidad, así como, en asuntos relacionados con la seguridad nacional, representantes de la ODNI, otros servicios de inteligencia y el Defensor del Pueblo. Podrán asistir a esta reunión, si lo desean, las APD de la UE y representantes del Grupo de Trabajo del Artículo 29.

([203]) Schrems, apartados 40 y siguientes y 101 a 103.
([204]) Schrems, apartados 51, 52 y 62.
([205]) Schrems, apartado 65.
([206]) Schrems, apartado 76.

(148) En el marco de la revisión conjunta anual, la Comisión solicitará al Departamento de Comercio que proporcione información exhaustiva sobre todos los aspectos pertinentes del funcionamiento del Escudo de la privacidad UE-EE. UU., en la que se especifiquen también los asuntos remitidos al Departamento de Comercio por las APD y los resultados de las verificaciones del cumplimiento efectuadas de oficio. La Comisión recabará asimismo explicaciones acerca de cualesquiera dudas o problemas relacionados con el Escudo de la privacidad UE-EE. UU. y su funcionamiento que puedan surgir a partir de la información disponible, incluidos los informes de transparencia previstos en la USA Freedom Act; los informes públicos elaborados por los servicios estadounidenses de inteligencia nacional, las APD y los grupos especializados en materia de privacidad; y la información publicada en los medios de comunicación o cualquier otra posible fuente. Por otra parte, a fin de facilitar la labor de la Comisión a este respecto, los Estados miembros deben informar a la Comisión de aquellos casos en los que las medidas adoptadas por los organismos encargados de garantizar la observancia de los principios en los Estados Unidos no cumplan su cometido, así como de cualquier indicio de que la actuación de los poderes públicos estadounidenses competentes en materia de seguridad nacional o de prevención, investigación, detección o enjuiciamiento de infracciones penales no brinden el nivel de protección necesario.

(149) Sobre la base de la revisión conjunta anual, la Comisión elaborará un informe público que presentará al Parlamento Europeo y al Consejo.

7. SUSPENSIÓN DE LA DECISIÓN DE ADECUACIÓN

(150) En el supuesto de que, a partir de las comprobaciones efectuadas o de cualquier otra información disponible, la Comisión concluya que el nivel de protección que ofrece el Escudo de la privacidad ya no puede considerarse esencialmente equivalente al de la Unión o que existen indicios claros de que ya no puede garantizarse el cumplimiento efectivo de los principios en los Estados Unidos, o de que la actuación de los poderes públicos estadounidenses competentes en materia de seguridad nacional o de prevención, investigación, detección o enjuiciamiento de infracciones penales no brinda el nivel de protección necesario, informará de ello al Departamento de Comercio y solicitará la adopción de las medidas pertinentes para abordar con rapidez cualquier posible incumplimiento de tales principios en un plazo razonable especificado. Si, transcurrido dicho plazo, las autoridades estadounidenses no han podido demostrar de manera convincente que el Escudo de la privacidad UE-EE. UU. sigue garantizando un cumplimiento efectivo de las normas y un nivel de protección adecuado, la Comisión incoará el procedimiento conducente a la suspensión parcial o total o a la derogación de la presente Decisión ([207]). Por otra parte, la Comisión podría proponer modificar la presente Decisión, por ejemplo, mediante la limitación del ámbito de la constatación de adecuación únicamente a las transferencias de datos sujetas a determinadas condiciones.

(151) En particular, la Comisión incoará el procedimiento de suspensión o derogación en las siguientes circunstancias:

a) cuando haya indicios de que las autoridades estadounidenses no se atienen a las declaraciones y compromisos recogidos en los documentos adjuntos a la presente Decisión, en particular por lo que respecta a las condiciones y limitaciones del acceso por parte de los poderes públicos de los Estados Unidos a los datos personales transferidos en el marco del Escudo de la privacidad a efectos de aplicación de la ley, seguridad nacional y otros fines de interés público;

b) si no se atienden eficazmente las reclamaciones presentadas por los interesados de la UE; en este sentido, la Comisión tendrá en cuenta todas las circunstancias que influyan en la posibilidad de que los interesados de la UE hagan valer sus derechos, incluido, en particular, el compromiso voluntario contraído por las empresas estadounidenses autocertificadas de cooperar con las APD y acatar sus recomendaciones, o

c) en caso de que el Defensor del Pueblo en el ámbito del Escudo de la privacidad no responda de forma oportuna y adecuada a las peticiones de los interesados de la UE.

(152) La Comisión estudiará asimismo la posibilidad de incoar el procedimiento conducente a la modificación, suspensión o derogación de la presente Decisión si, en el curso de la revisión conjunta anual del funcionamiento del Escudo de la privacidad UE-EE. UU. o en otro contexto, el Departamento de Comercio u otros departamentos o servicios intervinientes en la aplicación del Escudo de la privacidad, o en asuntos relacionados con la seguridad nacional, los representantes de los servicios de inteligencia estadounidenses o el Defensor del Pueblo, no facilitasen la información o las aclaraciones precisas para evaluar el cumplimiento de los principios de privacidad, la eficacia de los procedimientos de tramitación de reclamaciones, o cualquier disminución del nivel necesario de

([207]) A partir de la fecha de aplicación del Reglamento general de protección de datos, la Comisión hará uso de sus facultades para adoptar, por razones imperiosas de urgencia debidamente justificadas, un acto de ejecución por el que se suspenda la presente Decisión, que será aplicable inmediatamente, sin previa presentación al comité de comitología competente, y permanecerá en vigor por un plazo no superior a seis meses.

protección como consecuencia de las actividades de los servicios de inteligencia nacional de los Estados Unidos, y en particular de un acceso a datos personales o una recopilación de estos que no se limite a lo estrictamente necesario y proporcionado. A este respecto, la Comisión tendrá en cuenta en qué medida puede obtenerse la información pertinente de otras fuentes, tales como los informes de las empresas estadounidenses autocertificadas de conformidad con lo dispuesto en la USA Freedom Act.

(153) El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales previsto en el artículo 29 de la Directiva 95/46/CE publicó su dictamen sobre el nivel de protección que brinda el Escudo de la privacidad UE-EE. UU. ([208]), que se ha tenido en cuenta en la elaboración de la presente Decisión.

(154) El Parlamento Europeo adoptó una Resolución sobre los flujos transatlánticos de datos ([209]).

(155) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité creado en virtud del artículo 31, apartado 1, de la Directiva 95/46/CE,

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

1. A los efectos del artículo 25, apartado 2, de la Directiva 95/46/CE, los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en los Estados Unidos en el marco del Escudo de la privacidad UE-EE. UU.

2. El Escudo de la privacidad UE-EE. UU. se compone de los principios establecidos por el Departamento de Comercio de los Estados Unidos el 7 de julio de 2016, tal como se exponen en el anexo II, y en los compromisos y declaraciones oficiales recogidos en los documentos enumerados en los anexos I y III a VII.

3. A los efectos del apartado 1, se considerarán datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. aquellos que hayan sido transferidos desde la Unión a entidades establecidas en los Estados Unidos que figuren en la denominada «lista del Escudo de la privacidad», mantenida y puesta a disposición del público por el Departamento de Comercio de los Estados Unidos, de conformidad con las secciones I a III de los principios expuestos en el anexo II.

Artículo 2

La presente Decisión no afecta a la aplicación de las demás disposiciones de la Directiva 95/46/CE distintas del artículo 25, apartado 1, que conciernen al tratamiento de datos personales en los Estados miembros, y en particular su artículo 4.

Artículo 3

Los Estados miembros informarán de inmediato a la Comisión cada vez que sus autoridades competentes ejerzan las facultades que les confiere el artículo 28, apartado 3, de la Directiva 95/46/CE para prohibir provisional o definitivamente los flujos de datos dirigidos a una entidad establecida en los Estados Unidos e incluida en la lista del Escudo de la privacidad con arreglo a lo dispuesto en las secciones I y III de los principios expuestos en el anexo II con el fin de proteger a las personas en lo que respecta al tratamiento de sus datos personales.

Artículo 4

1. La Comisión llevará a cabo un seguimiento continuo del funcionamiento del Escudo de la privacidad UE-EE. UU. con vistas a determinar si los Estados Unidos siguen garantizando un nivel adecuado de protección de los datos personales transferidos en el marco de dicho régimen desde la Unión a entidades establecidas en los Estados Unidos.

([208]) Dictamen n.º 1/2016 sobre el proyecto de decisión de adecuación sobre el Escudo de la privacidad UE-EE. UU., adoptado el 13 de abril de 2016.

([209]) Resolución del Parlamento Europeo, de 26 de mayo de 2016, sobre los flujos transatlánticos de datos [2016/2727(RSP)].

2. Los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en los que se tenga constancia de que organismos públicos de los Estados Unidos con facultades legales para exigir el cumplimiento de los principios expuesto en el anexo II no hayan dispuesto mecanismos eficaces de detección y control que permitan identificar y sancionar en la práctica las posibles vulneraciones de los principios.

3. Los Estados miembros y la Comisión se informarán recíprocamente cuando haya algún indicio de que las injerencias por parte de los poderes públicos estadounidenses competentes en materia de seguridad nacional, aplicación de la ley u otros intereses públicos en el derecho de las personas a la protección de sus datos de carácter personal transcienda de lo estrictamente necesario, o de que no exista una tutela judicial efectiva frente a tales injerencias.

4. En el plazo de un año a partir de la fecha de la notificación de la presente Decisión a los Estados miembros y posteriormente con carácter anual, la Comisión evaluará la constatación formulada en el artículo 1, apartado 1, sobre la base de toda la información de que disponga, incluida la información recibida como parte de la revisión conjunta anual a que se refieren los anexos I, II y VI.

5. La Comisión informará al Comité creado en virtud del artículo 31 de la Directiva 95/46/CE de toda constatación pertinente.

6. La Comisión presentará un proyecto de medidas con arreglo al procedimiento previsto en el artículo 31, apartado 2, de la Directiva 95/46/CE al objeto de suspender, modificar o derogar la presente Decisión o limitar su ámbito de aplicación, entre otros, cuando existan indicios:

— de que los poderes públicos estadounidenses no se atienen a las declaraciones y compromisos recogidos en los documentos adjuntos a la presente Decisión, en particular por lo que respecta a las condiciones y limitaciones del acceso por parte de los poderes públicos de los Estados Unidos, a efectos de la aplicación de la ley, la seguridad nacional y otros fines de interés público, a los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU.;

— de incumplimiento sistemático de la obligación de atender eficazmente las reclamaciones presentadas por los interesados de la UE, o

— de incumplimiento sistemático por parte del Defensor del Pueblo en el ámbito del Escudo de la privacidad de su obligación de responder de forma oportuna y adecuada a las peticiones de los interesados de la UE según lo exigido por el artículo 4, letra e), del anexo III.

La Comisión presentará asimismo dicho proyecto de medidas cuando la falta de cooperación de los organismos que deban garantizar el funcionamiento del Escudo de la privacidad UE-EE. UU. en los Estados Unidos le impida determinar si se ha producido algún cambio que afecte a la constatación formulada en el artículo 1, apartado 1.

Artículo 5

Los Estados miembros adoptarán todas las medidas necesarias para dar cumplimiento a lo dispuesto en la presente Decisión.

Artículo 6

Los destinatarios de la presente Decisión serán los Estados miembros.

Hecho en Bruselas, el 12 de julio de 2016.

Por la Comisión
Věra JOUROVÁ
Miembro de la Comisión

ANEXO I

Carta de la Secretaria de Comercio estadounidense, Penny Pritzker

7 de julio de 2016

Dña. Věra Jourová
Comisaria de Justicia, Consumidores e Igualdad de Género
Comisión Europea
Rue de la Loi/Westraat 200
1049 Bruselas
Bélgica

Estimada Comisaria Jourová:

En nombre de los Estados Unidos, me complace adjuntarle un paquete de material informativo relativo al Escudo de la privacidad UE-EE. UU., fruto de dos años de fructíferos debates entre nuestros equipos. Este paquete, junto con otros materiales de los que dispone la Comisión procedentes de fuentes públicas, ofrece una base muy sólida para un nueva constatación de adecuación de la Comisión Europea ([1]).

Ambos deberíamos estar orgullosos de las mejoras realizadas al marco. El Escudo de la privacidad se basa en principios que cuentan con un sólido apoyo consensuado en ambos lados del Atlántico, y hemos consolidado su funcionamiento. Gracias a nuestro trabajo conjunto, disponemos de una oportunidad única para mejorar la protección de la privacidad en todo el mundo.

El paquete del Escudo de la privacidad incluye los principios del Escudo de la privacidad, además de una carta, adjunta como anexo 1, de la Administración de Comercio Internacional (ITA) del Departamento de Comercio, que administra el programa, en la que se describen los compromisos adquiridos por nuestro Departamento para garantizar el funcionamiento eficaz del Escudo de la privacidad. El paquete incluye también el anexo 2, que contiene otros compromisos del Departamento de Comercio relacionados con el nuevo modelo de arbitraje disponible con arreglo al Escudo de la privacidad.

He dado órdenes a mi personal para que dediquen todos los recursos necesarios para la rápida y plena implantación del marco del Escudo de la privacidad y para garantizar el puntual cumplimiento de los compromisos estipulados en el anexo 1 y en el anexo 2.

El paquete del Escudo de la privacidad incluye también otros documentos procedentes de otros organismos estadounidenses, entre ellos:

— una carta de la Comisión Federal de Comercio (FTC, por sus siglas en inglés) que describe su cumplimiento del Escudo de la privacidad,

— una carta del Departamento de Transporte que describe su cumplimiento del Escudo de la privacidad,

— dos cartas redactadas por la Oficina del Director de Inteligencia Nacional (ODNI, por sus siglas en inglés) relacionadas con las protecciones y limitaciones aplicables a las autoridades de seguridad nacional estadounidenses,

— una carta del Departamento de Estado y el memorando que lo acompaña que describen el compromiso del Departamento de Estado de establecer un nuevo Defensor del Pueblo en el ámbito del Escudo de la privacidad al que se podrán enviar consultas relacionadas con las prácticas de inteligencia de señales de los Estados Unidos, y

— una carta redactada por el Departamento de Justicia relacionada con la protección y las limitaciones en el acceso del Gobierno de los Estados Unidos a efectos del cumplimiento de la ley y del interés público.

Puede estar segura de que los Estados Unidos asumen estos compromisos con la máxima seriedad.

([1]) DO L 281 de 23.11.1995, p. 31.

En el plazo de los 30 días siguientes a la aprobación final de la decisión sobre el carácter adecuado de la protección, se entregará el paquete del Escudo de la privacidad al Federal Register (Registro Federal) para su publicación.

Esperamos colaborar con usted cuando se produzca la implantación del Escudo de la privacidad y cuando nos embarquemos juntos en la siguiente fase de este proceso.

Atentamente,

Penny Pritzker

Anexo 1

Carta del Subsecretario de Comercio Internacional en funciones, Ken Hyatt

A la atención de Dña. Věra Jourová
Comisaria de Justicia, Consumidores e Igualdad de Género
Comisión Europea
Rue de la Loi/Westraat 200
1049 Bruselas
Bélgica

Estimada Comisaria Jourová:

En nombre de la Administración de Comercio Internacional, me complace describir la protección mejorada de los datos personales que ofrece el marco del Escudo de la privacidad UE-EE. UU. («Escudo de la privacidad» o «marco») y los compromisos que ha asumido el Departamento de Comercio («Departamento») para garantizar el eficaz funcionamiento del Escudo de la privacidad. La conclusión de este acuerdo histórico es un logro primordial para la privacidad y los negocios en ambos lados del Atlántico. Hace que los ciudadanos de la UE confíen en que sus datos estarán protegidos y que dispondrán de los recursos legales necesarios para abordar cualquier problema. Ofrece la certeza de que ayudará al crecimiento de la economía transatlántica gracias a la garantía de que miles de empresas europeas y estadounidenses podrán continuar invirtiendo y haciendo negocios a través de nuestras fronteras. El Escudo de la privacidad es el fruto de más de dos años de duro trabajo y colaboración con ustedes, nuestros colegas de la Comisión Europea («Comisión»). Esperamos poder seguir trabajando con la Comisión para garantizar que el Escudo de la privacidad funcione según lo previsto.

Hemos trabajado con la Comisión en el desarrollo del Escudo de la privacidad para permitir que las entidades establecidas en los Estados Unidos cumplan los requisitos de adecuación para la protección de datos previstos en la legislación de la UE. El nuevo marco supondrá varios e importantes beneficios, tanto para las personas como para las empresas. En primer lugar proporciona un destacado conjunto de protecciones para la privacidad de los datos de los ciudadanos de la UE. Requiere que las entidades estadounidenses participantes desarrollen una política de privacidad conforme, se comprometan públicamente a cumplir los principios del Escudo de la privacidad de manera que el compromiso sea ejecutable de conformidad con la legislación estadounidense, renueven anualmente la certificación de su cumplimiento ante el Departamento, proporcionen mecanismos de resolución de litigios independientes y gratuitos a los ciudadanos de la UE, y se sometan a la autoridad de la Comisión Federal de Comercio estadounidense («FTC», por sus siglas en inglés), el Departamento de Transporte («DOT», por sus siglas en inglés) u otro organismo de ejecución. En segundo lugar, el Escudo de la privacidad permitirá que miles de empresas de los Estados Unidos y filiales de empresas europeas radicadas en los Estados Unidos reciban datos personales de la Unión Europea para facilitar los flujos de datos que sostienen el comercio transatlántico. La relación económica transatlántica es actualmente la más importante del mundo; representa la mitad de la producción económica mundial y aproximadamente un billón USD en comercio de bienes y servicios, lo que supone millones de puestos de trabajo en ambos lados del Atlántico. Las empresas que se basan en los flujos de datos transatlánticos pertenecen a todos los sectores industriales e incluyen las principales empresas de la lista *Fortune 500*, así como muchas pequeñas y medianas empresas (pymes). Los flujos de datos transatlánticos permiten que las entidades estadounidenses puedan tratar los datos necesarios para ofertar productos, servicios y oportunidades laborales a ciudadanos europeos. El Escudo de la privacidad respalda los principios de privacidad compartidos, salvando las diferencias entre nuestros planteamiento jurídicos a la vez que fomenta los objetivos económicos y de comercio tanto de Europa como de los Estados Unidos.

Aunque la decisión de las empresas de autocertificar su adhesión a este nuevo marco será voluntaria, una vez que la empresa se comprometa públicamente a asumir el Escudo de la privacidad, tanto la Comisión Federal de Comercio como el Departamento de Transporte, dependiendo de la autoridad que tenga jurisdicción sobre la entidad adherida al Escudo de la privacidad, podrá exigir su compromiso en virtud de la legislación estadounidense.

Mejoras en virtud de los principios del Escudo de la privacidad

El Escudo de la privacidad resultante consolida la protección de la privacidad gracias a:

— la exigencia de proporcionar información adicional a las personas en el principio de notificación, en particular una declaración de la participación de la entidad en el Escudo de la privacidad, una declaración del derecho de las personas de acceder a los datos personales, y la identificación del correspondiente órgano de resolución de litigios independiente,

— la consolidación de la protección de los datos personales transferidos desde una entidad adherida al Escudo de la privacidad a un tercero responsable del tratamiento mediante la petición a las partes de que suscriban un contrato que garantice que solo se tratarán estos datos para fines limitados y especificados, coherentes con el consentimiento proporcionado por el particular,y que el destinatario ofrecerá el mismo nivel de protección que los principios,

— la consolidación de la protección de los datos personales transferidos desde una entidad adherida al Escudo de la privacidad a un tercer agente, en particular exigiendo a una entidad adherida al Escudo de la privacidad que tome medidas razonables y adecuadas para garantizar el tratamiento eficaz por parte del agente de la información personal transferida con arreglo a las obligaciones de la entidad en virtud de los principios; tras la recepción de la notificación, que tome medidas razonables y adecuadas para detener y reparar un tratamiento no autorizado; y que proporcione, a instancias del Departamento, un resumen o una copia representativa de las correspondientes disposiciones de privacidad de su contrato con este agente,

— siempre y cuando una entidad de Escudo de la privacidad sea responsable del tratamiento de la información personal que reciba en virtud del Escudo de la privacidad y seguidamente la transfiera a un tercero que actúe como agente en su nombre, esta entidad adherida al Escudo de la privacidad seguirá siendo responsable en virtud de los principios, si su agente trata dicha información personal contrariamente a lo establecido en los principios, salvo que la entidad demuestre que no es responsable del suceso que haya provocado el daño,

— la aclaración de que las entidades adheridas al Escudo de la privacidad deben limitar la información personal a la información pertinente a efectos del tratamiento;

— la exigencia a la entidad de que certifique anualmente ante el Departamento su compromiso de aplicar los principios a la información que recibió durante su participación en el Escudo de la privacidad, en caso de que abandone el mismo y decida conservar tales datos,

— la exigencia de proporcionar a los particulares unos mecanismos de recurso independientes y gratuitos,

— la exigencia a las entidades y a sus mecanismos de recurso independientes de que respondan rápidamente a las consultas y peticiones de información del Departamento relacionadas con el Escudo de la privacidad,

— la exigencia a las entidades de que respondan sin demora a las reclamaciones relacionadas con el cumplimiento de los principios, presentadas por las autoridades de los Estados miembros de la UE a través del Departamento, y

— la exigencia a las entidades adheridas al Escudo de la privacidad de hacer público cualquier apartado de los informes de cumplimiento o evaluación relacionado con el Escudo de la privacidad presentados a la FTC, si dicha entidad es objeto de una orden de la FTC o de una resolución judicial por incumplimiento.

Gestión y supervisión del programa del Escudo de la privacidad por parte del Departamento de Comercio

El Departamento reitera su compromiso de mantener y hacer pública una lista fidedigna de las entidades estadounidenses que se han autocertificado ante el Departamento y han declarado su compromiso de adhesión a los principios (la «lista del Escudo de la privacidad»). El Departamento mantendrá actualizada la lista del Escudo de la privacidad mediante la eliminación de las entidades que se retiren voluntariamente, que no presenten la certificación anual de conformidad con los procedimientos del Departamento, o que muestren un incumplimiento sistemático. El Departamento también mantendrá y hará público un registro fidedigno de las entidades estadounidenses que se hayan autocertificado previamente ante el Departamento pero que hayan sido eliminadas de la lista del Escudo de la privacidad, incluidas aquellas que hayan sido eliminadas por un incumplimiento sistemático de los principios. El Departamento identificará el motivo por el cual haya sido eliminada cada entidad.

Asimismo, el Departamento se compromete a reforzar la gestión y la supervisión del Escudo de la privacidad. Concretamente, el Departamento:

Ofrecerá información adicional sobre la web del Escudo de la privacidad

— mantendrá la lista del Escudo de la privacidad, así como un registro de aquellas entidades que previamente hayan autocertificado su adhesión a los principios, pero que hayan dejado de acogerse a los beneficios del Escudo de la privacidad,

— incluirá una explicación destacada que aclare que todas las entidades eliminadas de la lista del Escudo de la privacidad han dejado de acogerse a los beneficios del Escudo de la privacidad, pero no obstante deben continuar aplicando los principios a la información personal que recibieron durante su participación en el Escudo de la privacidad mientras mantengan dicha información, y

— proporcionará un enlace a la lista de casos de la FTC relacionados con el Escudo de la privacidad que figura en la web de la FTC.

Verificará los requisitos de autocertificación

— con anterioridad a la realización de la autocertificación de una entidad (o certificación anual) y a la inclusión de una entidad en la lista del Escudo de la privacidad, comprobará que la entidad:

  — haya proporcionado la información de contacto exigida,

  — haya descrito sus actividades con respecto a la información personal recibida de la UE,

  — haya indicado qué información personal está cubierta por su autocertificación,

  — si posee una web pública, haya facilitado la dirección de la web donde la que la política de privacidad esté disponible y accesible, o si no posee una web pública, haya facilitado la dirección donde su política de privacidad pueda ser consultada por el público,

  — haya incluido en su correspondiente política de privacidad la declaración de su adhesión a los principios, y si la política de privacidad se encuentra disponible en línea, un enlace a la web del Escudo de la privacidad del Departamento,

  — haya identificado el organismo oficial concreto con jurisdicción para entender de cualquier reclamación contra la entidad por posibles prácticas desleales o fraudulentas y vulneraciones de las leyes o normas sobre la vida privada (y que figure en los principios o en un futuro anexo a los principios),

  — en caso de que la entidad decida cumplir los requisitos establecidos en los puntos a) i) y a) iii), del principio de recurso, aplicación y responsabilidad mediante el compromiso de colaborar con las autoridades de protección de datos de la UE («APD»), haya indicado su intención de colaborar con las APD en la investigación y resolución de las reclamaciones relacionadas con el Escudo de la privacidad, y en particular de responder a sus consultas cuando los interesados de la UE hayan presentado sus reclamaciones directamente a sus APD nacionales,

  — haya identificado un programa de privacidad del que la entidad sea miembro,

  — haya identificado el método de verificación del cumplimiento de los principios (por ejemplo, interno, de un tercero),

  — haya identificado, tanto en la presentación de la autocertificación como en su política de privacidad, el mecanismo de recurso independiente disponible para investigar y resolver las reclamaciones,

  — haya incluido en su correspondiente política de privacidad, si la política se encuentra disponible en línea, un enlace a la web o al formulario de presentación de reclamaciones del mecanismo de recurso independiente disponible para la investigación de reclamaciones no resueltas, y

  — en caso de que la entidad haya indicado que pretende recibir información de recursos humanos transferida desde la UE para su uso en el contexto de la relación laboral, haya declarado su compromiso de colaborar y cumplir con las APD para resolver las reclamaciones relativas a sus actividades con relación a dichos datos, y haya proporcionado al Departamento una copia de su política de privacidad de recursos humanos y haya facilitado el lugar donde se encuentra disponible su política de privacidad para poder ser consultada por sus empleados afectados,

— trabajará con las instancias de recurso independientes para comprobar que las entidades estén realmente registradas en el mecanismo indicado en sus declaraciones de autocertificación, cuando se exija dicho registro.

Redoblará sus esfuerzos para realizar un seguimiento de las entidades que han sido eliminadas de la lista del Escudo de la privacidad.

— comunicará a las entidades que hayan sido eliminadas de la lista del Escudo de la privacidad por su «incumplimiento sistemático» que no están autorizadas a conservar información recopilada en virtud del Escudo de la privacidad, y

— enviará cuestionarios a las entidades cuyas autocertificaciones prescriban o que se hayan retirado voluntariamente del Escudo de la privacidad, con el fin de comprobar si la entidad devolverá o suprimirá la información personal recibida durante su participación en el Escudo de la privacidad, o si continuará aplicando los principios a dicha información, y si tal información personal se conserva, comprobará qué persona de la entidad actuará como punto de contacto continuo para las cuestiones relacionadas con el Escudo de la privacidad.

Buscará y abordará las declaraciones fraudulentas de participación

— revisará las políticas de privacidad de las entidades que hayan participado anteriormente en el programa del Escudo de la privacidad, pero que hayan sido eliminadas de la lista del Escudo de la privacidad, a fin de identificar las declaraciones fraudulentas de participación en el mismo,

— con carácter continuo, cuando una entidad: a) renuncie a su participación en el Escudo de la privacidad, b) no certifique nuevamente su adhesión a los principios, o c) sea eliminada como participante en el Escudo de la privacidad, en particular por su «incumplimiento sistemático», comprobará de oficio que la entidad haya eliminado de su política de privacidad publicada toda referencia al Escudo de la privacidad que implique que la entidad continua participando activamente en el mismo y que tiene derecho a sus beneficios. En caso de que el Departamento constate que estas referencias no han sido eliminadas, advertirá a la entidad de que, cuando proceda, remitirá las cuestiones al organismo pertinente para una posible medida coercitiva si este continúa alegando su certificación del Escudo de la privacidad. En caso de que la entidad no elimine las referencias ni autocertifique su adecuación al Escudo de la privacidad, el Departamento remitirá de oficio la cuestión al FTC, al DOT o a cualquier otro organismo competente, o bien cuando proceda adoptará las medidas necesarias para la aplicación de la marca de certificación del Escudo de la privacidad,

— acometerá otras acciones para la identificación de las declaraciones fraudulentas de participación en el Escudo de la privacidad y el uso indebido de la marca de certificación del Escudo de la privacidad, incluidas las búsquedas por Internet para identificar donde se muestran imágenes de la marca de certificación del Escudo de la privacidad y las referencias al Escudo de la privacidad en las políticas de privacidad de las entidades,

— abordará rápidamente cualquier cuestión que se identifique durante el seguimiento de oficio de las declaraciones fraudulentas de participación y de uso indebido de la marca de certificación, y en particular se cursará una advertencia a las entidades que tergiversen su participación en el programa del Escudo de la privacidad según lo antes descrito,

— adoptará otras medidas coercitivas adecuadas, incluidos los recursos legales que el Departamento está autorizado a incoar y la remisión de las cuestiones a la FTC, el DOT u otro órgano de aplicación pertinente, y

— revisará y resolverá rápidamente las reclamaciones sobre las declaraciones fraudulentas de participación que se reciban.

El Departamento procederá a la revisión de las políticas de privacidad de las entidades para identificar y abordar de una manera más eficaz las declaraciones fraudulentas de participación en el Escudo de la privacidad. Concretamente, el Departamento revisará las políticas de privacidad de las entidades cuya autocertificación haya prescrito debido a la no presentación de la nueva certificación de adhesión a los principios. El Departamento realizará este tipo de revisión para comprobar que estas entidades hayan eliminado de las políticas de privacidad publicadas cualquier referencia que implique que las entidades continúan participando activamente en el Escudo de la privacidad. Gracias a estos tipos de revisiones, se identificará a las entidades que no hayan eliminado estas referencias y se les enviará una carta de la Oficina del Consejo General del Departamento advirtiéndoles de la posible medida coercitiva a aplicar en caso de que no eliminen las referencias. El Departamento acometerá una acción de seguimiento para garantizar que las entidades suprimen las referencias inadecuadas, o bien vuelven a certificar su adhesión a los principios. De igual modo, el Departamento no regateará esfuerzos en la identificación de declaraciones fraudulentas de participación en el Escudo de la privacidad por parte de entidades que nunca han participado en el programa del Escudo de la privacidad, y acometerá acciones correctoras similares con respecto a estas entidades.

Realizará revisiones y evaluaciones periódicas de oficio del programa

— supervisará con carácter continuo el cumplimiento efectivo, incluso a través del envío de cuestionarios detallados a las entidades participantes, para la identificación de las cuestiones que puedan justificar un posterior seguimiento. En particular, estas revisiones del cumplimiento se llevarán a cabo cuando: a) el Departamento reciba denuncias serias y concretas sobre el cumplimiento de los principios por parte de una entidad, b) una entidad no responda satisfactoriamente a las solicitudes del Departamento de información relacionada con el Escudo de la privacidad, o c) existan pruebas de que una entidad no cumple con sus compromisos en el marco del Escudo de la privacidad. Cuando sea necesario, el Departamento consultará a las autoridades competentes de protección de datos sobre estas revisiones del cumplimiento, y

— evaluará periódicamente la gestión y supervisión del programa del Escudo de la privacidad con el objeto de garantizar la idoneidad de la supervisión para abordar los nuevos problemas que puedan surgir.

El Departamento ha incrementado los recursos destinados a la gestión y supervisión del programa del Escudo de la privacidad, e incluso ha duplicado el personal responsable de la gestión y supervisión del programa, y continuará dedicando los recursos necesarios para garantizar una supervisión y gestión eficaz del programa.

Adaptará la web del Escudo de la privacidad al público destinatario

El Departamento adaptará la web del Escudo de la privacidad para centrarse en tres públicos destinatarios: ciudadanos de la UE, empresas de la UE y empresas estadounidenses. La inclusión de material especialmente destinado a los ciudadanos de la UE y a las empresas estadounidenses facilitará la transparencia en muchos aspectos. Con respecto a los ciudadanos de la UE, explicará con toda claridad: 1) los derechos que otorga el Escudo de la privacidad a los ciudadanos de la UE; 2) los mecanismos de recurso disponibles para los ciudadanos de la UE cuando crean que una entidad infringe su compromiso de cumplir con los principios; y 3) cómo buscar información correspondiente a la autocertificación del Escudo de la privacidad de una entidad. Con respecto a las empresas estadounidenses, facilitará la comprobación de: 1) si una entidad cuenta con los beneficios del Escudo de la privacidad; 2) el tipo de información cubierta por la autocertificación del Escudo de la privacidad de una entidad; 3) la política de privacidad que se aplica a la información cubierta, y 4) el método que utiliza la entidad para verificar su adhesión a los principios.

Intensificará la colaboración con las APD

Para incrementar las oportunidades de colaboración con las APD, el Departamento establecerá un contacto nombrado por él mismo para actuar de enlace con las APD. En los casos en que una APD crea que una entidad no está cumpliendo con los principios, en particular a raíz de una reclamación de un ciudadano de la UE, la APD podrá acudir al contacto nombrado por el Departamento para solicitar una revisión más detallada de la entidad. El contacto también recibirá remisiones relativas a entidades que declaren fraudulentamente su participación en el Escudo de la privacidad a pesar de no haber autocertificado nunca su adhesión a los principios. El contacto colaborará con las APD en la búsqueda de información relacionada con la autocertificación de una entidad en concreto o con su anterior participación en el programa, y responderá a las preguntas de las APD relacionadas con la implantación de los requisitos específicos del Escudo de la privacidad. En segundo lugar, el Departamento proporcionará a las APD material relacionado con el Escudo de la privacidad para la inclusión en sus propias webs con el objeto de aumentar la transparencia para los ciudadanos de la UE y las empresas estadounidenses. Una mayor conciencia sobre el Escudo de la privacidad y los derechos y responsabilidades que comporta facilitaría la identificación de los problemas que puedan surgir, a fin de poder abordarlos adecuadamente.

Facilitará la resolución de las reclamaciones por incumplimiento

El Departamento, a través del contacto nombrado, recibirá las reclamaciones que le remita una APD relacionadas con el incumplimiento de los principios por parte de una entidad adherida al Escudo de la privacidad. El Departamento hará todo cuanto esté en su mano para facilitar la resolución de la reclamación con la entidad adherida al Escudo de la privacidad. En el plazo de 90 días siguientes a la recepción de la reclamación, el Departamento entregará una actualización a la APD. Para facilitar la presentación de estas reclamaciones, el Departamento elaborará un formulario estándar para que las APD lo presenten al contacto nombrado por el Departamento. El contacto nombrado llevará un registro de todos los casos remitidos por las APD al Departamento, y este incluirá, en la revisión anual que se describe a continuación, un informe en el que analizará el conjunto de las reclamaciones recibidas cada año.

Adoptará procedimientos de arbitraje y elegirá a los árbitros en consulta con la Comisión

El Departamento cumplirá sus compromisos previstos en el anexo I y publicará los procedimientos una vez alcanzado el acuerdo.

Mecanismo de revisión conjunta del funcionamiento del Escudo de la privacidad

El Departamento de Comercio, la FTC y otros organismos, cuando proceda, celebrarán reuniones anuales con la Comisión, las APD interesadas y los representantes del Grupo de Trabajo del Artículo 29, en las que el Departamento proporcionará actualizaciones del programa del Escudo de la privacidad. Las reuniones anuales incluirán un debate de las cuestiones actuales relacionadas con el funcionamiento, la implantación, la supervisión y la aplicación del Escudo de la privacidad, incluidas las remisiones recibidas por el Departamento de las APD, los resultados de las revisiones de oficio del cumplimiento, y también podrán incluir un debate sobre los cambios en la legislación. La primera revisión anual y, según proceda, las revisiones posteriores comprenderán un diálogo sobre otros temas, por ejemplo en el ámbito de la toma de decisiones automatizada, incluidos los aspectos relativos a las similitudes y diferencias de los enfoques de la UE y EE. UU.

Actualización de las leyes

El Departamento hará esfuerzos razonables para informar a la Comisión de los cambios legislativos importantes en los Estados Unidos en la medida en que sean pertinentes para el Escudo de la privacidad en el ámbito de la protección de la privacidad de los datos y de las limitaciones y garantías aplicables al acceso a datos personales por parte de las autoridades de EE. UU. y su posterior utilización.

Excepción de seguridad nacional

Por lo que respecta a las limitaciones para la adhesión a los principios del Escudo de la privacidad a efectos de la seguridad nacional, el Consejo General de la Oficina del Director de Inteligencia Nacional, Robert Litt, también ha enviado dos cartas dirigidas a Justin Antonipillai y Ted Dean del Departamento de Comercio, que le han sido remitidas a usted. Estas cartas tratan exhaustivamente, entre otras cosas, las políticas, salvaguardias y limitaciones que se aplican a las actividades de inteligencia de señales llevadas a cabo por los Estados Unidos. Asimismo, estas cartas describen la transparencia que ofrecen los servicios de inteligencia sobre estas cuestiones. Dado que la Comisión está evaluando el marco del Escudo de la privacidad, la información incluida en estas cartas ofrece la seguridad necesaria para concluir que el Escudo de la privacidad funcionará adecuadamente, de conformidad con los principios. Entendemos que usted podrá presentar en el futuro información publicada por los servicios de inteligencia, junto con otra información, para alimentar la revisión anual del marco del Escudo de la privacidad.

Sobre la base de los principios del Escudo de la privacidad y las cartas y materiales adjuntos, incluidos los compromisos del Departamento en lo que respecta a la gestión y supervisión del marco del Escudo de la privacidad, esperamos que la Comisión determine que el marco del Escudo de la privacidad UE-EE. UU. ofrece la protección adecuada a efectos de la legislación de la UE y que continúen las transferencias de datos de la Unión Europea a las entidades que participan en el Escudo de la privacidad.

Atentamente,

Ken Hyatt

Anexo 2

Modelo de arbitraje

Anexo I

Este anexo I comprende los términos en virtud de los cuales las entidades adheridas al Escudo de la privacidad están obligadas a arbitrar las reclamaciones, de conformidad con el principio de recurso, aplicación y responsabilidad. La opción del arbitraje vinculante descrita a continuación se aplica a determinadas reclamaciones «no resueltas» relativas a los datos cubiertos por el Escudo de la privacidad UE-EE. UU. El objetivo de esta opción es ofrecer un mecanismo rápido, independiente y equitativo, opcional para los ciudadanos, para la resolución de las infracciones denunciadas de los principios no resueltas por uno de los mecanismos del Escudo de la privacidad, si los hay.

A. **Ámbito de aplicación**

Los ciudadanos disponen de una opción de arbitraje para determinar, en el caso de las reclamaciones no resueltas, si una entidad adherida al Escudo de la privacidad ha infringido sus obligaciones previstas con relación al ciudadano en cuestión, y si dicha infracción sigue estando total o parcialmente sin resolver. Esta opción solamente está disponible para este propósito. Esta opción no está disponible, por ejemplo, por lo que respecta a las excepciones a los principios ([1]) ni con respecto a una denuncia sobre el carácter adecuado del Escudo de la privacidad.

B. **Recursos disponibles**

De conformidad con esta opción de arbitraje, el panel del Escudo de la privacidad (compuesto por de uno a tres árbitros, según el acuerdo entre las partes) posee la autoridad necesaria para imponer una reparación específica, equitativa y no monetaria (como el acceso, la corrección, la eliminación o la devolución de los datos de la persona en cuestión), necesaria para la reparación de la infracción de los principios en lo que se refiere exclusivamente a la persona. Estos son los únicos poderes del panel de arbitraje con respecto a los recursos. Al ponderar las reparaciones, el panel de arbitraje deberá considerar otras reparaciones previamente aplicadas por otros mecanismos en virtud del Escudo de la privacidad. No están disponibles las indemnizaciones, costes, honorarios u otras reparaciones. Cada parte asume los honorarios de sus abogados.

C. **Requisitos previos al arbitraje**

La persona que decida invocar esta opción de arbitraje deberá tomar las siguientes medidas antes de entablar una demanda de arbitraje: 1) plantear la infracción denunciada directamente a la entidad y ofrecerle la posibilidad de resolver la cuestión dentro del plazo establecido en el apartado III.11(d)(i) de los principios; 2) utilizar el mecanismo de recurso independiente contemplado en los principios, sin coste alguno para la persona, y 3) plantear la cuestión a través de su Autoridad de Protección de Datos al Departamento de Comercio y ofrecer al Departamento de Comercio la posibilidad de hacer todo cuanto pueda para resolver la cuestión en los plazos estipulados en la carta de la International Trade Administration (Administración de Comercio Internacional) del Departamento de Comercio, sin cargo alguno para la persona.

Esta opción de arbitraje no podrá ser invocada si esta misma infracción de los principios denunciada por la persona 1) estuvo anteriormente sujeta al arbitraje vinculante; 2) fue objeto de una sentencia firme dictada en un proceso judicial del que el particular fuera parte; o 3) fue anteriormente resuelta por las partes. Además, esta opción no podrá ser invocada si una Autoridad de Protección de Datos de la UE 1) tiene autoridad en virtud de los apartados III.5 o III.9 de los principios; o 2) tiene autoridad para resolver la infracción denunciada directamente con la entidad. La autoridad que tiene una APD para resolver la misma reclamación contra un responsable del tratamiento de la UE no impide la invocación de esta opción de arbitraje contra una entidad jurídica distinta no sujeta a la autoridad de la APD.

D. **Naturaleza vinculante de las decisiones**

La decisión de una persona de invocar esta opción de arbitraje vinculante es totalmente voluntaria. Las decisiones arbitrales serán vinculantes para todas las partes del arbitraje. Una vez invocada, la persona renuncia a la opción de solicitar reparación por la misma infracción denunciada en otro foro, con la excepción de que, en caso de que una medida no monetaria equitativa no resuelva totalmente la infracción denunciada, la invocación del arbitraje por parte de la persona no impedirá una reclamación por daños y perjuicios, recurriendo para ello a la justicia ordinaria.

([1]) Apartado I.5 de los principios.

E. **Control y ejecución**

Los particulares y las entidades adheridas al Escudo de la privacidad podrán solicitar el control judicial y la ejecución de las decisiones arbitrales de conformidad con la legislación estadounidense prevista en la Ley Federal de Arbitraje ([1]). Todos estos casos pueden ser llevados al tribunal de distrito federal cuya competencia territorial incluya el domicilio social principal de la entidad adherida al Escudo de la privacidad.

Esta opción de arbitraje pretende resolver las disputas individuales, y las sentencias arbitrales no pretenden funcionar como un precedente persuasivo o vinculante en cuestiones que impliquen a otras partes, inclusive en los futuros arbitrajes o en los tribunales de la UE o de EE. UU. o en los procedimientos de la FTC.

F. **Panel de arbitraje**

Las partes elegirán a los árbitros de la lista de árbitros mencionada a continuación.

De conformidad con la legislación aplicable, el Departamento de Comercio estadounidense y la Comisión Europea elaborarán una lista de como mínimo 20 árbitros, elegidos en función de su independencia, integridad y experiencia. Con relación a este proceso se aplicará cuanto sigue:

Árbitros:

1) se mantendrán en la lista durante un período de 3 años, a falta de circunstancias excepcionales o motivos justificados, renovable por un período adicional de 3 años;

2) no podrán recibir instrucciones ni estar asociados a ninguna de las partes, ninguna entidad adherida al Escudo de la privacidad, ni a ninguna otra autoridad gubernamental, autoridad pública u organismo de ejecución de EE. UU., de la UE o de un Estado miembro de la UE; y

3) deberán estar habilitados para ejercer la práctica jurídica en EE. UU. y ser expertos en legislación estadounidense en materia de privacidad, así como tener conocimientos en materia de legislación sobre protección de datos de la UE.

G. **Procedimientos de arbitraje**

De conformidad con la legislación aplicable, en el plazo de los 6 meses siguientes a la adopción de la decisión de adecuación, el Departamento de Comercio y la Comisión Europea acordarán adoptar un conjunto de procedimientos arbitrales estadounidenses existente y establecido (como AAA o JAMS) para regular los procedimientos ante el panel del Escudo de la privacidad, a reserva de las siguientes consideraciones:

1. Un particular podrá entablar un arbitraje vinculante sujeto a la disposición de los requisitos de pre-arbitraje antes mencionados, presentando una «notificación» a la entidad. La notificación deberá contener un resumen de los pasos acometidos en virtud del apartado C para resolver la reclamación, una descripción de la presunta infracción y, a discreción del particular, documentos y material justificativo o un análisis de la legislación aplicable a la reclamación en cuestión.

([1]) El capítulo 2 de la Ley Federal de Arbitraje («FAA», por sus siglas en inglés) establece que «un acuerdo de arbitraje o una sentencia arbitral que se derive de una relación jurídica, contractual o no, considerada comercial, incluida una transacción, contrato o acuerdo descrito en la [sección 2 de la FAA] corresponde a la Convención [sobre el reconocimiento y ejecución de las sentencias arbitrales extranjeras, de 10 de junio de 1958, 21 U.S.T. 2519, T.I.A.S. n.º 6997 ("Convención de Nueva York")]». 9 U.S.C. § 202. La FAA establece asimismo que «el acuerdo o la sentencia que se derive de dicha relación entre los ciudadanos de Estados se considerará que no corresponde a la Convención [de Nueva York] salvo que esa relación comporte una propiedad situada en el extranjero, contemple el cumplimiento o la ejecución en el extranjero o tenga alguna relación razonable de otro tipo con uno o más países extranjeros». *Íd.* De conformidad con el capítulo 2, «cualquier parte del arbitraje podrá recurrir a un tribunal que tenga jurisdicción en virtud de este capítulo para obtener una orden que confirme la sentencia contra cualquier otra parte del arbitraje. El tribunal confirmará la sentencia salvo que encuentre fundamentos para la denegación o el aplazamiento del reconocimiento o de la ejecución de la sentencia especificados en dicha Convención [de Nueva York]». *Id.* § 207. El capítulo 2 establece además que «los tribunales de distrito de los Estados Unidos... tendrán jurisdicción original sobre... una acción o procedimiento [en virtud de la Convención de Nueva York], independientemente del importe en cuestión». *Id.* § 203.
El capítulo 2 también establece que «se aplicará el capítulo 1 a las acciones y procedimientos contemplados en el presente capítulo, en la medida en que dicho capítulo no contravenga al presente capítulo o a la Convención» [de Nueva York], tal como fue ratificada por Estados Unidos. *Id.* § 208. A su vez, el capítulo 1 establece que «una disposición por escrito en... un contrato que evidencie una transacción comercial dirigida a resolver mediante arbitraje una controversia derivada de dicho contrato o transacción, o de la negativa a ejecutar la totalidad o parte del dicho contrato o transacción, o un acuerdo por escrito que comprometa a las partes a someter a arbitraje una controversia existente derivada de este contrato, transacción o negativa, será válido, irrevocable y ejecutable, salvo que existan motivos previstos por la ley o por el principio de equidad para la revocación de un contrato». *Id.* § 2. El capítulo 1 establece además que «cualquier parte del arbitraje podrá solicitar al tribunal especificado una orden que confirme la sentencia, y acto seguido el tribunal deberá conceder esta orden salvo que la sentencia haya sido anulada, modificada o corregida de conformidad con lo estipulado en las secciones 10 y 11 de [la FAA]». *Id.* § 9.

2. Se desarrollarán los procedimientos necesarios para garantizar que una misma infracción denunciada por una persona no sea objeto de recursos o procedimientos por duplicado.

3. La acción de la FTC podrá continuar en paralelo con el arbitraje.

4. Ningún representante de EE. UU., de la UE o de un Estado miembro de la UE ni ninguna autoridad gubernamental, autoridad pública u organismo de ejecución podrá participar en estos arbitrajes, si bien a petición de un particular de la UE, las APD de la UE podrán ofrecer asistencia para preparar la notificación únicamente, pero sin poder acceder a los contenidos ni a ningún otro material relacionado con estos arbitrajes.

5. La ubicación del arbitraje será los Estados Unidos, y la persona podrá elegir participar por videoconferencia o por teléfono, lo que se le facilitará sin coste alguno para la misma. No se exigirá la participación presencial.

6. El idioma del arbitraje será el inglés, salvo que las partes acuerden lo contrario. Tras una petición razonada, y teniendo en cuenta si la persona está representada por un abogado, se ofrecerá servicio de interpretación en la vista del arbitraje así como de traducción de los materiales del arbitraje, sin coste alguno para la persona, salvo que el panel decida que, en las circunstancias del arbitraje en concreto, esto supondría unos costes injustificados o desproporcionados.

7. Los materiales presentados a los árbitros serán tratados confidencialmente y solo se utilizarán con relación al arbitraje.

8. Si es necesario, podrá permitirse la revelación de contenidos específicos de la persona, y dicha revelación será tratada confidencialmente por las partes y solo se utilizará con relación al arbitraje.

9. Los arbitrajes deberán finalizarse en el plazo de los 90 días siguientes a la entrega de la notificación a la entidad en cuestión, salvo que las partes acuerden lo contrario.

H. **Costes**

Los árbitros deberán tomar medias razonables para minimizar los costes o gastos de los arbitrajes.

De conformidad con la legislación aplicable, el Departamento de Comercio facilitará el establecimiento de un fondo al que las entidades adheridas al Escudo de la privacidad deberán pagar una contribución anual, basada en parte en el tamaño de la entidad, que cubrirá el coste del arbitraje, incluidos los honorarios de los árbitros, hasta unas cantidades máximas («límites»), en consulta con la Comisión Europea. El fondo será gestionado por un tercero, el cual informará regularmente sobre las operaciones del fondo. En la revisión anual, el Departamento de Comercio y la Comisión Europea examinarán el funcionamiento del fondo, incluida la necesidad de ajustar el importe de las contribuciones o de los límites, y tendrán en cuenta, entre otras cosas, el número de arbitrajes, los costes y la duración de los arbitrajes, con el entendimiento mutuo de que no se impondrá una carga excesiva a las entidades adheridas al Escudo de la privacidad. Los honorarios de los abogados no están cubiertos por esta disposición ni por ningún fondo contemplado en esta disposición.

ANEXO II

PRINCIPIOS DEL MARCO DEL ESCUDO DE LA PRIVACIDAD UE-EE. UU. PUBLICADOS POR EL DEPARTAMENTO DE COMERCIO ESTADOUNIDENSE

I. SÍNTESIS

1. Aunque los Estados Unidos y la Unión Europea comparten el objetivo de aumentar la protección de la privacidad, los Estados Unidos adoptan un enfoque distinto de la privacidad al de la Unión Europea. Los Estados Unidos utilizan un enfoque sectorial que se basa en una mezcla de legislación, regulación y autorregulación. Dadas estas diferencias y para dotar a las entidades de los Estados Unidos de un mecanismo fiable para las transferencias de datos personales a los Estados Unidos procedentes de la Unión Europea y, a la vez, garantizar que los interesados de la UE continúen beneficiándose de protección y garantías eficaces, tal como exige la legislación europea con respecto al tratamiento de sus datos personales cuando son transferidos a países no pertenecientes a la UE, el Departamento de Comercio publica estos principios del Escudo de la privacidad, incluidos los principios complementarios (colectivamente «los principios»), en virtud de su competencia legal para impulsar, promocionar y desarrollar el comercio internacional (USC, título 15, artículo 1512). Los principios fueron desarrollados en colaboración con la Comisión Europea y con el sector y otras partes interesadas para facilitar el comercio y las relaciones de negocios entre los Estados Unidos y la Unión Europea. Están destinados a ser utilizados exclusivamente por las entidades de los Estados Unidos que reciben datos personales de la Unión Europea con el propósito de permitir a estas entidades cumplir las condiciones relativas al Escudo de la privacidad, y por lo tanto, beneficiarse de la decisión de adecuación de la Comisión Europea ([1]). Los principios no afectan a la aplicación de las disposiciones nacionales que implementan la Directiva 95/46/CE («la Directiva») que se aplica al tratamiento de los datos personales en los Estados miembros. Los principios tampoco limitan las obligaciones de privacidad, que por lo demás se aplican en virtud de la legislación estadounidense.

2. Para beneficiarse del Escudo de la privacidad para la realización de transferencias de datos personales desde la UE, las entidades deben autocertificar su adhesión a los principios ante el Departamento de Comercio (o su delegado) («el Departamento»). Aunque las decisiones de las entidades de adherirse al Escudo de la privacidad son totalmente voluntarias, el cumplimiento efectivo es obligatorio: las entidades que se autocertifiquen ante el Departamento y declaren públicamente su compromiso de adherirse a los principios deben cumplirlos íntegramente. Para adherirse al Escudo de la privacidad, las entidades deben: a) someterse a las competencias de investigación y ejecución de la Comisión Federal de Comercio («la FTC»), el Departamento de Transporte u otro organismo oficial que garantice eficazmente el cumplimiento de los principios *(en el futuro podrán incluirse como anexo otros órganos oficiales estadounidenses reconocidos por la UE)*; b) declarar públicamente su compromiso de cumplir los principios; c) hacer públicas sus políticas de privacidad acordes con estos principios; y d) aplicarlos en su totalidad. El incumplimiento por parte de una entidad puede ser objeto de medidas de ejecución en virtud del artículo 5 de la Ley de la Comisión Federal de Comercio que prohíbe actos desleales o fraudulentos en el comercio o que afecten al comercio [USC, título 15, artículo 45, letra a)] o en virtud de otras leyes o reglamentos que prohíban estos actos.

3. El Departamento de Comercio mantendrá y hará pública una lista fidedigna de las entidades estadounidenses que se hayan autocertificado ante el Departamento y hayan declarado su compromiso de adhesión a los principios (la «lista del Escudo de la privacidad»). Se garantizan los beneficios del Escudo de la privacidad a partir de la fecha en que el Departamento incluya a la entidad en la lista del Escudo de la privacidad. El Departamento eliminará a una entidad de dicha lista si esta se retira voluntariamente del Escudo de la privacidad o si no presenta su nueva certificación anual al Departamento. La eliminación de una entidad de la lista del Escudo de la privacidad significa que ya no podrá seguir beneficiándose de la decisión de adecuación de la Comisión Europea para recibir información personal de la UE. La entidad deberá continuar aplicando los principios a la información personal recibida durante su participación en el Escudo de la privacidad, y ratificar anualmente ante el Departamento su compromiso de hacerlo durante el tiempo en que siga conservando dicha información; de lo contrario, la entidad deberá devolver o borrar la información o proporcionar una protección «adecuada» a la información con otros medios autorizados. El Departamento también eliminará de la lista del Escudo de la privacidad a aquellas entidades que hayan incumplido repetidamente los principios; estas entidades no podrán acogerse a los beneficios del Escudo de la privacidad y deberán devolver o borrar la información personal que recibieron en virtud del mismo.

4. El Departamento también mantendrá y hará público un registro fidedigno de las entidades estadounidenses que se hayan autocertificado previamente ante el Departamento, pero que hayan sido eliminadas de la lista del Escudo de la privacidad. El Departamento advertirá claramente que estas entidades no participan en el Escudo de la privacidad; que la eliminación de la lista del Escudo de la privacidad significa que estas entidades no podrán reivindicar su cumplimiento del Escudo de la privacidad y deberán evitar cualquier declaración o práctica engañosa que implique su participación en el Escudo de la privacidad; y que estas entidades ya no tienen derecho a beneficiarse de la decisión de adecuación de la Comisión Europea que permitiría que estas entidades recibieran información personal procedente de la UE. La entidad que continúe reivindicando su participación en el Escudo de la privacidad o haga

([1]) Dado que la Decisión de la Comisión sobre la adecuación de la protección ofrecida por el Escudo de la privacidad UE-EE. UU. es aplicable a Islandia, Liechtenstein y Noruega, el paquete del Escudo de la privacidad cubrirá tanto a la Unión Europea como a estos tres países. En consecuencia, deberá interpretarse que las referencias a la UE y a sus Estados miembros incluyen a Islandia, Liechtenstein y Noruega.

otras declaraciones tergiversadas relacionadas con el Escudo de la privacidad después de haber sido eliminada de la lista podrá ser objeto de medidas coercitivas de la FTC, del Departamento de Transporte o de otros organismos de ejecución.

5. La adhesión a estos principios puede verse limitada por: a) exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que origine conflictos de obligaciones o prevea autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios está limitado en la medida necesaria para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; o 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 los Estados Unidos, se espera que las entidades opten por el mayor nivel de protección posible.

6. Las entidades están obligadas a aplicar los principios en todos los datos personales transferidos en virtud del Escudo de la privacidad una vez adheridas al mismo. La entidad que decida extender los beneficios del Escudo de la privacidad también a la información sobre recursos humanos transferida desde la Unión Europea para usarla en el contexto de una relación laboral, deberá indicarlo al Departamento y atenerse a los requisitos establecidos en el principio complementario sobre autocertificación.

7. La legislación estadounidense se aplicará a las cuestiones relativas a la interpretación y a las políticas de protección de la vida privada de las entidades adheridas al Escudo de la privacidad, excepto si estas se han comprometido a cooperar con las autoridades europeas de protección de datos («APD»). Salvo que se indique otra cosa, serán aplicables todas las disposiciones de los principios cuando sea pertinente.

8. Definiciones:

   a. «Datos personales» e «información personal» son datos referidos a una persona identificada o identificable, que entren en el ámbito de la Directiva y sean recibidos por entidades estadounidenses con procedencia de la Unión Europea, cualquiera que sea la forma en que se registren.

   b. «Tratamiento» de los datos personales es cualquier operación o conjunto de operaciones que se realice con los datos personales, tanto por medios automatizados como no automatizados, tales como la recopilación, la grabación, la organización, el almacenamiento, la adaptación o la modificación, la recuperación, la consulta, el uso, la divulgación o difusión, y la supresión o destrucción.

   c. «Responsable del tratamiento de datos» es una persona u entidad que, en solitario o conjuntamente con otros, establece las finalidades y los medios del tratamiento de los datos personales.

9. La fecha de entrada en vigor de los principios es la fecha de aprobación final de la decisión de adecuación de la Comisión.

II. PRINCIPIOS

1. **Notificación**

   a. Las entidades informarán a los particulares sobre:

      i. su participación en el Escudo de la privacidad, y proporcionarán un enlace a la lista del Escudo de la privacidad o la dirección web de la misma,

      ii. los tipos de datos personales recopilados y, cuando proceda, las entidades o filiales de la entidad adheridas también a los principios,

iii. su compromiso de someter a los principios todos los datos personales recibidos de la UE en virtud del Escudo de la privacidad,

iv. los fines para los que recogen y utilizan información sobre ellos,

v. la forma de contactar con ellas para cualquier pregunta o reclamación, incluido cualquier establecimiento de la UE que pueda responder a dichas preguntas o reclamaciones,

vi. el tipo o la identidad de los terceros a los que revelan la información personal, y los fines de tal revelación,

vii. el derecho de las personas a acceder a sus datos personales,

viii. las opciones y medios que la entidad ofrece a los particulares para limitar el uso y la divulgación de sus datos personales,

ix. el organismo de resolución de conflictos independiente designado para tramitar las reclamaciones y ofrecer un recurso gratuito para las personas, independientemente de que dicho organismo sea: 1) el panel designado por las APD, 2) un organismo de resolución alternativa de conflictos radicado en la UE, o 3) un organismo de resolución alternativa de conflictos radicado en los Estados Unidos,

x. el hecho de estar sometidas a las competencias de investigación y ejecución de la FTC, del Departamento de Transporte o de cualquier otro organismo oficial estadounidense autorizado,

xi. la posibilidad, en determinadas condiciones, de que la persona se acoja a un arbitraje vinculante,

xii. la obligación de comunicar datos personales en respuesta a peticiones legales de las autoridades públicas, en particular para responder a necesidades de seguridad nacional o de aplicación de la ley, y

xiii. su responsabilidad en los casos de transferencias ulteriores a terceros.

b. La notificación se hará en lenguaje claro y de forma visible la primera vez que se pida a los particulares que proporcionen información personal a la entidad o, posteriormente, tan pronto como sea posible, pero en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que haya efectuado la transferencia, o antes de que se divulgue por primera vez a un tercero.

2. **Opción**

a. Las entidades ofrecerán a los particulares la posibilidad de decidir (exclusión) si su información personal: i) puede divulgarse a un tercero, o ii) puede utilizarse para un propósito sustancialmente distinto del objetivo inicial para el que fue recogida o autorizada posteriormente por el particular. Se deben proporcionar a los particulares mecanismos claros, visibles y de fácil acceso para que ejerzan su derecho de opción.

b. No obstante lo establecido en el párrafo anterior, no es necesario ofrecer la posibilidad de optar cuando la divulgación se realice a un tercero que actúe como agente para realizar las tareas en nombre de la entidad y siguiendo sus indicaciones. Sin embargo, la entidad deberá suscribir siempre un contrato con el agente.

c. Si se trata de información sensible, como datos sobre el estado de salud, el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical o la orientación sexual de la persona, la opción de participar será afirmativa o expresa (aceptación) si la información: i) va a revelarse a un tercero, o ii) va a utilizarse para un fin distinto para el que se recogió inicialmente o se autorizó con posterioridad mediante la aceptación del interesado. En cualquier caso, una entidad debe tratar como sensible toda información recibida de un tercero cuando dicho tercero la identifique y la trate como información sensible.

3. **Responsabilidad por una transferencia ulterior**

a. Para transferir información personal a un tercero que actúe como responsable del tratamiento, las entidades deberán cumplir con los principios de notificación y opción. Las entidades deberán también suscribir un contrato con el tercero responsable del tratamiento que estipule que estos datos solo se podrán tratar para propósitos limitados y específicos que sean conformes al consentimiento proporcionado por la persona, y que el destinatario ofrecerá el mismo nivel de protección que los principios y comunicará a la entidad si decide que ya no puede cumplir esta obligación. El contrato establecerá que, en caso de que se tome tal decisión, el tercero responsable del tratamiento dejará de tratar los datos o tomará otras medidas de reparación razonables y apropiadas.

b. Para transferir datos personales a un tercero que actúe de agente, las entidades deberán: i) transferir estos datos única y exclusivamente para fines limitados y especificados; ii) cerciorarse de que el agente está obligado a proporcionar como mínimo el mismo nivel de protección de la privacidad exigido por los principios; iii) tomar medidas razonables y adecuadas para garantizar el tratamiento eficaz por parte del agente de la información personal transferida con arreglo a las obligaciones de la entidad en virtud de los principios; iv) requerir al agente que notifique a la entidad si decide que ya no puede cumplir su obligación de proporcionar el mismo nivel de protección exigido por los principios; v) tras la recepción de la notificación, en particular lo establecido en el inciso iv), tomar las medidas razonables y adecuadas para detener y reparar un tratamiento no autorizado, y vi) proporcionar, a instancias del Departamento, un resumen o una copia representativa de las correspondientes disposiciones de privacidad de su contrato con ese agente.

4. **Seguridad**

a. Las entidades que creen, mantengan, utilicen o difundan información personal deberán adoptar medidas razonables y apropiadas para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, su modificación y su destrucción, teniendo en cuenta los riesgos inherentes al tratamiento y la naturaleza de los datos personales.

5. **Integridad de los datos y limitación de la finalidad**

a. De acuerdo con los principios, la información personal debe limitarse a la información relevante a efectos del tratamiento ([1]). Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el particular. En la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos personales tengan fiabilidad para el uso previsto y sean exactos, completos y actuales. La entidad debe respetar los principios durante el tiempo que conserve dicha información.

b. La información podrá conservarse en una forma que identifique o haga identificable ([2]) a la persona únicamente mientras esta conservación sirva para alcanzar la finalidad del tratamiento con arreglo a lo dispuesto en el apartado 5a. Esta obligación no impide a las entidades tratar la información personal por períodos más largos, durante el tiempo y en la medida en que dicho tratamiento sirva razonablemente a fines de archivo en interés público, periodísticos, literarios y artísticos, de investigación científica o histórica y de análisis estadístico. En estos casos, el tratamiento estará sujeto a los demás principios y disposiciones del marco. Las entidades deben adoptar medidas razonables y apropiadas para cumplir esta disposición.

6. **Acceso**

a. Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, o haya sido tratada infringiendo los principios, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona, o cuando puedan vulnerarse los derechos de otras personas.

([1]) Dependiendo de las circunstancias, los ejemplos de finalidades de tratamiento compatibles pueden incluir aquellas que sirvan razonablemente a las relaciones con los clientes, el cumplimiento y los aspectos jurídicos, la auditoría, la seguridad y la prevención del fraude, la conservación o defensa los derechos legales de la entidad, así como otras finalidades compatibles con las expectativas razonables de una persona en el contexto de la recopilación.

([2]) En este contexto, si habida cuenta del medio de identificación que es razonablemente probable que se utilice (teniendo en cuenta, entre otras cosas, los costes y el tiempo necesarios para identificar a la persona, así como la tecnología disponible en el momento del tratamiento) y de la forma en que se conserven los datos, un individuo puede razonablemente ser identificado por la entidad, o por un tercero que tuviera acceso a los datos, entonces el individuo es «identificable».

7. **Recurso, aplicación y responsabilidad**

a. Una protección eficaz de la vida privada debe incluir sólidos mecanismos para garantizar la conformidad con los principios, una vía de recurso para las personas afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora. Como mínimo, tales mecanismos deben incluir:

i. una vía de recurso independiente e inmediatamente disponible mediante la que las reclamaciones y las controversias de las personas puedan ser investigadas y resueltas sin demora y sin coste alguno para el particular y de acuerdo con los principios, y se conceda una indemnización por daños cuando así lo establezcan la legislación aplicable o las iniciativas del sector privado;

ii. procedimientos de seguimiento para comprobar que los certificados y declaraciones de las entidades sobre sus prácticas en materia de privacidad se ajustan a la verdad y que dichas prácticas se aplican en consecuencia y, en particular, en lo que se refiere a los casos de incumplimiento, y

iii. la obligación de subsanar los problemas derivados del incumplimiento de los principios por las entidades que se hayan adherido a ellos y las sanciones correspondientes contra ellas, que serán lo suficientemente rigurosas para garantizar su cumplimiento.

b. Las entidades y sus mecanismos de recurso independientes responderán rápidamente a las consultas y peticiones de información del Departamento relacionadas con el Escudo de la privacidad. Todas las entidades deberán responder sin demora a las reclamaciones relacionadas con el cumplimiento de los principios remitidas por las autoridades de los Estados miembros de la UE a través del Departamento. Las entidades que hayan decidido colaborar con las APD, en particular las entidades que tratan datos sobre recursos humanos, deberán responder directamente ante estas autoridades con relación a la investigación y la resolución de las reclamaciones.

c. Las entidades están obligadas a arbitrar las reclamaciones y atenerse a las condiciones establecidas en el anexo I, siempre y cuando una persona haya invocado un arbitraje vinculante mediante la entrega de la notificación a la entidad en cuestión de conformidad con los procedimientos y condiciones establecidos en el anexo I.

d. En el contexto de una transferencia ulterior, una entidad adherida al Escudo de la privacidad asume la responsabilidad del tratamiento de la información personal que recibe en virtud del Escudo de la privacidad y posteriormente transfiere a un tercero que actúa como agente en su nombre. La entidad adherida al Escudo de la privacidad será responsable con arreglo a los principios si su agente trata esta información personal contrariamente a los mismos, salvo que la entidad demuestre que no es responsable del suceso que ha provocado el daño.

e. Cuando una entidad sea objeto de una orden de la FTC o de una orden judicial basada en el incumplimiento, la entidad hará público todo apartado relacionado con el Escudo de la privacidad relevante de los informes de cumplimiento o evaluación presentados a la FTC, en la medida en que se cumplan los requisitos de confidencialidad. El Departamento ha establecido un punto de contacto para las APD en caso de problemas de cumplimiento por parte de las entidades adheridas al Escudo de la privacidad. La FTC considerará prioritariamente las remisiones del Departamento y de las autoridades de los Estados miembros de la UE relativas a la inobservancia de los principios, e intercambiará sin demora información relativa a las remisiones con las autoridades públicas que hayan efectuado las remisiones, de acuerdo con las restricciones de confidencialidad existentes.

III. PRINCIPIOS COMPLEMENTARIOS

1. **Datos sensibles**

a. Una entidad no está obligada a obtener un consentimiento explícito y positivo por lo que respecta a los datos sensibles en los casos en que el tratamiento:

i. se realice en función de intereses vitales de la persona afectada o de otra persona,

ii. sea necesario para preparar un recurso o acción en justicia,

iii. se requiera para proporcionar cuidados médicos o establecer un diagnóstico,

iv. se lleve a cabo en el marco de las legítimas actividades de una fundación, asociación o cualquier otro organismo sin fines lucrativos que persiga un objetivo político, filosófico, religioso o sindical, a condición de que el tratamiento se refiera exclusivamente a los miembros del organismo o a las personas que tienen contactos habituales con él relacionados con sus fines, y a condición de que los datos no se revelen a terceros sin el consentimiento de los interesados,

v. sea necesario para cumplir las obligaciones de la entidad en el ámbito de la legislación laboral, o

vi. esté relacionado con los datos hechos públicos por el particular.

2. **Excepciones por razón del periodismo**

a. Habida cuenta del amparo que la Constitución de los Estados Unidos ofrece a la libertad de prensa, así como de las excepciones que contempla la Directiva en materia de periodismo, cuando el derecho a la libertad de prensa consagrado en la Primera Enmienda de la Constitución de los Estados Unidos entra en conflicto con los intereses de la protección de la vida privada, la Primera Enmienda debe regir el equilibrio de tales intereses en lo tocante a las actividades de los particulares o entidades estadounidenses.

b. La información personal que se recoja con fines de publicación, difusión u otras formas de comunicación pública de material periodístico, aunque no se utilice, así como la información que se recabe de material de archivo publicado anteriormente, no estará sujeta a los requisitos de los principios del Escudo de la privacidad.

3. **Responsabilidad subsidiaria**

a. Los Proveedores de servicios de Internet («ISP»), los operadores de telecomunicaciones y otras entidades no son responsables según los principios del Escudo de la privacidad cuando, en nombre de otra entidad, se limiten a transmitir, encaminar, intercambiar o almacenar temporalmente información. Tal como sucede con la propia Directiva, el Escudo de la privacidad no genera una responsabilidad subsidiaria. Si una entidad actúa como mero conducto de los datos transmitidos por terceros y no determina ni la finalidad ni los medios de tratamiento de los datos personales, no será responsable.

4. **Diligencia debida y realización de auditorías**

a. Las actividades de bancos de inversiones y sociedades de auditoría pueden suponer el tratamiento de datos personales sin autorización o conocimiento del interesado. Los principios de notificación, opción y acceso lo permiten en las circunstancias descritas a continuación.

b. Las sociedades anónimas bursátiles y las sociedades de accionariado concentrado, incluidas las entidades adheridas al Escudo de la privacidad, están generalmente sujetas a auditorías. Dichas auditorías, especialmente las que examinan posibles irregularidades, pueden verse amenazadas si son divulgadas antes de tiempo. De igual modo, una entidad adherida al Escudo de la privacidad involucrada en una posible fusión o adquisición deberá realizar, o deberá estar sujeta, a una revisión de «diligencia debida». Con frecuencia esto comportará la recogida y el tratamiento de datos personales tales como información sobre altos directivos y otro personal clave. La divulgación prematura podría impedir la transacción o incluso infringir la regulación de valores aplicable. Los bancos de inversiones o las sociedades de auditoría pueden tratar información sin conocimiento del interesado solo en la medida y durante el período necesarios para cumplir las normas o satisfacer las exigencias del interés público, así como en otras circunstancias en que la aplicación de estos principios perjudicaría los intereses legítimos de la entidad. Entre estos se cuenta la supervisión del cumplimiento por las empresas de sus obligaciones legales y las actividades legítimas de contabilidad, así como la necesidad de secreto relacionada con posibles adquisiciones, fusiones, empresas en participación u otras operaciones similares llevadas a cabo por los bancos de inversiones o las sociedades de auditoría.

5. **Función de las autoridades responsables de la protección de datos**

a. Las entidades aplicarán su compromiso de colaboración con las autoridades de protección de datos («APD») de la Unión Europea tal como se describe a continuación. De conformidad con el Escudo de la privacidad, las entidades estadounidenses que reciban datos personales de la UE deberán comprometerse a utilizar mecanismos eficaces para dar cumplimiento a los principios del Escudo de la privacidad. Más concretamente, tal como se establece en el principio de recurso, aplicación y responsabilidad, las entidades participantes deberán proporcionar: (a)(i) vías de recurso para los particulares a los que se refieren los datos; (a)(ii) procedimientos de seguimiento para comprobar la certeza de las afirmaciones y declaraciones que han realizado sobre sus prácticas de respeto de la intimidad; y (a)(iii) la obligación de subsanar los problemas que surjan por el incumplimiento de los principios, así como de asumir sus consecuencias. La entidad podrá satisfacer los puntos (a)(i) y (a)(iii) del principio de recurso, aplicación y responsabilidad si se adhiere a los requisitos aquí establecidos para la colaboración con las APD.

b. Una entidad se compromete a colaborar con las APD mediante la declaración en la presentación de su autocertificación del Escudo de la privacidad ante el Departamento de Comercio (véase el principio complementario sobre autocertificación) de que la entidad:

i. opta por cumplir los requisitos de los puntos (a)(i) y (a)(iii) del principio de recurso, aplicación y responsabilidad del Escudo de la privacidad, comprometiéndose a colaborar con las APD,

ii. colaborará con las APD competentes en la investigación y resolución de las reclamaciones que se formulen con arreglo al Escudo de la privacidad, y

iii. cumplirá las decisiones de la APD cuando esta determine que la entidad debe tomar medidas concretas para cumplir los principios del Escudo de la privacidad, y en particular el pago de indemnizaciones o compensaciones en beneficio de los afectados por el incumplimiento de los principios, y notificará por escrito a la APD la adopción de dichas medidas.

c. Funcionamiento de los paneles de las APD

i. las APD colaborarán con información y asesoramiento, que se prestarán de la manera siguiente:

1. Las APD proporcionarán asesoramiento a través de un panel informal de APD de ámbito europeo, que permitirá, entre otras cosas, seguir un enfoque armonizado y coherente.

2. El panel asesorará a las entidades estadounidenses afectadas en relación con reclamaciones no resueltas de particulares, en lo que respecta al tratamiento de información personal transferida desde la Unión Europea al amparo del Escudo de la privacidad. Este asesoramiento tendrá como finalidad la correcta aplicación de los principios del Escudo de la privacidad y contemplará todas las vías de recurso para los afectados que las APD consideren adecuadas.

3. El panel proporcionará este asesoramiento en respuesta tanto a los casos que le remitan las entidades afectadas, como a las reclamaciones que reciba directamente de particulares contra entidades que se hayan comprometido a colaborar con las APD en el marco del Escudo de la privacidad. Simultáneamente, animará y, en su caso, ayudará a los particulares en un primer momento a hacer uso de las modalidades internas de resolución de litigios que ofrezcan las entidades.

4. Solo se proporcionará asesoramiento una vez que las partes en litigio hayan dispuesto de una oportunidad razonable de presentar sus observaciones y aportar las pruebas que deseen. El panel tratará de dar su consejo tan pronto como lo permita esta exigencia de garantía jurisdiccional y, de modo general, en un plazo de 60 días tras recibir la reclamación o la remisión, o antes si es posible.

5. El panel hará públicos los resultados de sus deliberaciones sobre las reclamaciones si lo considera conveniente.

6. El asesoramiento del panel no conllevará responsabilidad alguna ni para este ni para una APD en concreto,

ii. como se señaló anteriormente, las entidades que escojan esta opción para la resolución de litigios deben comprometerse a seguir el dictamen de las APD. Si una entidad persiste en el incumplimiento transcurridos 25 días desde que se recibió el dictamen y no ha dado una explicación satisfactoria sobre el retraso, el panel notificará su intención de someter la cuestión a la Comisión Federal de Comercio u otro organismo federal o estatal de los Estados Unidos con jurisdicción para actuar en casos de fraude o engaño, o de certificar que se ha vulnerado gravemente el acuerdo de cooperación, por lo que deberá considerarse nulo de pleno derecho. En este último caso, el panel informará al Departamento de Comercio para que proceda a la debida corrección de la lista del Escudo de la privacidad. Todo incumplimiento del compromiso de cooperar con las APD, así como de los principios del Escudo de la privacidad, podrá originar un procedimiento por fraude de conformidad con el artículo 5 de la Ley de la FTC o de una norma similar.

d. Una entidad que desee beneficiarse del Escudo de la privacidad para cubrir los datos sobre recursos humanos transferidos desde la UE en el contexto de la relación laboral, deberá comprometerse a colaborar con las APD con relación a estos datos (véanse los principios complementarios sobre los datos de recursos humanos).

e. Las entidades que escojan esta opción deberán pagar una tasa anual para cubrir el coste de funcionamiento del panel. Además, podría solicitárseles que se hagan cargo de los gastos de traducción derivados de las deliberaciones del panel sobre las remisiones o reclamaciones contra ellas. La tasa anual no sobrepasará los 500 USD y será de menor cuantía para las empresas más pequeñas.

6. **Autocertificación**

a. Los beneficios del Escudo de la privacidad se garantizan a las entidades desde la fecha en que el Departamento haya incluido la presentación de la autocertificación de la entidad en la lista del Escudo de la privacidad, una vez se haya determinado que el expediente de autocertificación está completo.

b. Para autocertificar la adhesión al Escudo de la privacidad, una entidad deberá presentar al Departamento una declaración de autocertificación firmada por un responsable de la organización en nombre de la entidad que desea adherirse al Escudo de la privacidad, y que debe contener como mínimo la siguiente información:

i. nombre de la entidad, dirección postal, correo electrónico, teléfono y fax,

ii. descripción de las actividades de la entidad en lo relativo a la información personal recibida de la Unión Europea, y

iii. descripción de su política de protección de la vida privada respecto de dicha información personal, con indicación de:

1. si la entidad posee una web pública, la dirección de la web en la que aparece la política de privacidad, o si la entidad no posee una web pública, la dirección donde su política de privacidad pueda ser consultada por el público;

2. su fecha efectiva de aplicación;

3. una oficina de contacto para la tramitación de las reclamaciones, las solicitudes de acceso y cualquier otra cuestión relacionada con el Escudo de la privacidad;

4. el organismo oficial pertinente que tenga jurisdicción para oír las reclamaciones contra la entidad relacionadas con unas posibles prácticas desleales o engañosas y con la violación de las leyes o de las normativas que rigen la privacidad (y que figuran en los principios o en un futuro anexo a los principios);

5. el nombre de cualquier programa de privacidad del que la entidad sea miembro;

6. el método de verificación (por ejemplo, interno, de un tercero) (véase el principio complementario sobre la verificación); y

7. el mecanismo de recurso independiente disponible para la investigación de las reclamaciones no resueltas.

c. Cuando la entidad desee que sus beneficios del Escudo de la privacidad se apliquen a la información sobre recursos humanos transferida desde la Unión Europea para usarla en el contexto de la relación laboral, podrá hacerlo cuando un organismo oficial enumerado en los principios o en un futuro anexo a los principios tenga jurisdicción para oír reclamaciones contra la entidad que se deriven del tratamiento de la información de recursos humanos. Asimismo, la entidad deberá indicarlo en esta autocertificación y expresar su compromiso de cooperar con las autoridades de la UE de conformidad con los principios complementarios sobre los datos de recursos humanos y el papel de las Autoridades de Protección de Datos pertinentes, y que cumplirá las recomendaciones de dichas autoridades. La entidad también debe facilitar al Departamento una copia de su política de privacidad de recursos humanos y proporcionar información sobre el lugar en el que los empleados afectados pueden consultarla.

d. El Departamento mantendrá la lista del Escudo de la privacidad de las entidades que hayan completado la autocertificación, garantizando así la disponibilidad de los beneficios del Escudo de la privacidad, y actualizará esta lista en función de la presentación de las nuevas certificaciones anuales y de las notificaciones recibidas en virtud del principio complementario sobre resolución de conflictos y ejecución. Estas nuevas autocertificaciones deberán ser presentadas con carácter anual, como mínimo; de lo contrario, la entidad será eliminada de la lista del Escudo de la privacidad y no podrá seguir disfrutando de los beneficios del Escudo de la privacidad. Tanto la inclusión de las entidades en la lista del Escudo de la privacidad como la presentación de las nuevas certificaciones por parte de las entidades, se harán públicas. Todas las entidades incluidas en la lista del Escudo de la privacidad por el Departamento deberán también exponer en sus declaraciones de la política de privacidad

publicada su adhesión a los principios del Escudo de la privacidad. Si está disponible en Internet, la política de privacidad de la entidad deberá incluir un enlace a la página web del Escudo de la privacidad del Departamento y otro enlace a la página web o al formulario de presentación de reclamaciones del mecanismo de recurso independiente disponible para investigar las reclamaciones no resueltas.

e. Los principios de Privacidad se aplicarán inmediatamente después de la certificación. Teniendo en cuenta que los principios afectarán a las relaciones comerciales con terceros, las entidades que se certifiquen para el marco del Escudo de la privacidad en el plazo de los dos meses siguientes a la fecha de entrada en vigor del marco, armonizarán cuanto antes las relaciones comerciales existentes con terceros con el principio de responsabilidad de la transferencia ulterior, y en ningún caso después de los nueve meses siguientes a la fecha de su certificación de adhesión al Escudo de la privacidad. Durante este período provisional, cuando las entidades transfieran datos a terceros: i) aplicarán los principios de notificación y opción, y ii) cuando se transfieran datos personales a terceros que actúen de agente, deberán asegurarse de que el agente esté obligado a proporcionar como mínimo el mismo nivel de protección que el exigido por los principios.

f. La entidad deberá someter a los principios del Escudo de la privacidad todos los datos personales recibidos de la UE en virtud del Escudo de la privacidad. El compromiso de adherirse a los principios del Escudo de la privacidad es ilimitado en el tiempo en relación con los datos personales recibidos durante el período en el que la entidad disfrute de los beneficios del Escudo de la privacidad. Según este compromiso, continuarán aplicándose los principios a dichos datos mientras la entidad los almacene, utilice o divulgue, aunque posteriormente se desvincule del Escudo de la privacidad por cualquier motivo. La entidad que abandone el Escudo de la privacidad pero quiera conservar estos datos deberá reiterar con carácter anual su compromiso ante el Departamento de continuar aplicando los principios o de proporcionar una protección «adecuada» a la información a través de otros medios autorizados (por ejemplo, utilizando un contrato que refleje en su totalidad los requisitos de las cláusulas contractuales estándares adoptadas por la Comisión Europea); de lo contrario, la entidad deberá devolver o borrar la información. La entidad que abandone el Escudo de la privacidad deberá eliminar de la política de privacidad pertinente cualquier referencia al Escudo de la privacidad que insinúe que la entidad continúa participando activamente en el Escudo de la privacidad y que tiene derecho a disfrutar de sus beneficios.

g. Una entidad que deje de existir como persona jurídica independiente a resultas de una fusión o adquisición deberá notificarlo previamente al Departamento. La notificación deberá indicar también si la entidad adquirente o la entidad resultante de la fusión: i) mantendrá su adhesión a los principios del Escudo de la privacidad en virtud de la normativa sobre adquisiciones o fusiones; u ii) optará por autocertificar su adhesión a los principios del Escudo de la privacidad o establecer otras salvaguardias, por ejemplo un acuerdo escrito que garantice la adhesión a los principios del Escudo de la privacidad. Si no se aplican los anteriores puntos i) o ii), cualquier dato que se haya adquirido en el marco del Escudo de la privacidad deberá suprimirse inmediatamente.

h. Cuando una entidad abandone el Escudo de la privacidad por cualquier motivo, deberá eliminar todas las afirmaciones que insinúen que la entidad continúa participando en el Escudo de la privacidad o tiene derecho a los beneficios del Escudo de la privacidad. También deberá eliminar la marca de la certificación del Escudo de la privacidad UE-EE. UU. en caso de que la utilice. Cualquier falsedad transmitida al público en general referente a la adhesión de una entidad a los principios del Escudo de la privacidad podrá ser objeto de recurso por parte de la FTC u otro organismo público competente. Cualquier deficiencia de la información transmitida al Departamento podrá perseguirse en virtud de la *False Statements Act* (Ley sobre declaraciones falsas, USC, título 18, artículo 1001).

7. **Verificación**

a. Las entidades deberán proporcionar procedimientos de seguimiento para verificar que los certificados y declaraciones que presentan las empresas sobre sus prácticas de protección de la vida privada relativas al Escudo de la privacidad son ciertos y que estas prácticas se han aplicado de la manera indicada y de conformidad con los principios del Escudo de la privacidad.

b. Para cumplir los requisitos de verificación del principio de recurso, aplicación y responsabilidad, una entidad debe verificar los certificados y declaraciones mencionados mediante autoevaluación o mediante verificaciones por terceros.

c. Siguiendo el método de autoevaluación, la verificación deberá indicar que la política de protección de la vida privada respecto a la información personal recibida de la Unión Europea y hecha pública por la entidad es precisa, completa, está expuesta de manera destacada, se ha aplicado en su totalidad y es accesible. Asimismo, debe indicar que su política de privacidad cumple los principios del Escudo de la privacidad; que los particulares reciben información sobre los mecanismos internos de resolución de reclamaciones y de los mecanismos independientes de presentación de reclamaciones; que la entidad dispone de procedimientos de formación de los trabajadores a estos efectos y que se aplicarán sanciones en caso de incumplimiento; y que existen procedimientos internos para efectuar periódicamente revisiones objetivas sobre el cumplimiento de todo lo anterior.

Un directivo u otro representante autorizado de la empresa deberá firmar un informe de verificación de la autoevaluación como mínimo una vez al año y este deberá difundirse a petición de los consumidores o en el contexto de posibles investigaciones o reclamaciones por incumplimiento.

d. Cuando la entidad haya elegido someterse a la verificación por terceros, dicha verificación deberá demostrar que la política de la entidad en cuanto a la vida privada relativa a la información personal recibida de la Unión Europea se ajusta a los principios del Escudo de la privacidad, que se está cumpliendo y que los particulares reciben información sobre los mecanismos de reclamación. Los métodos de verificación pueden incluir, a título meramente enunciativo, auditorías, comprobaciones imprevistas, el uso de «señuelos» o de herramientas tecnológicas, según se considere apropiado. El informe de que se ha completado satisfactoriamente la verificación por terceros deberá portar la firma del revisor o del directivo u otro representante autorizado de la empresa, se elaborará como mínimo una vez al año y se difundirá a petición de los consumidores o en el contexto de posibles investigaciones o reclamaciones por incumplimiento.

e. Las entidades deberán conservar sus registros sobre la implantación de sus prácticas de privacidad del Escudo de la privacidad y hacerlos públicos previa petición en el contexto de una investigación o de una reclamación por incumplimiento ante el órgano independiente responsable de la investigación de las reclamaciones o ante el organismo competente en materia de prácticas engañosas y fraudulentas. Las entidades deberán responder inmediatamente a las consultas y otras solicitudes de información del Departamento relacionadas con la adhesión de la entidad a los principios.

8. **Acceso**

a. El principio de acceso en la práctica

i. De conformidad con los principios del Escudo de la privacidad, el derecho de acceso es fundamental para la protección de la privacidad. En particular, permite a las personas verificar la exactitud de la información existente sobre ellas. El principio de acceso significa el derecho de las personas a:

1. obtener la confirmación por parte de una entidad de si esta trata o no datos personales relacionados con ellas ([1]);

2. que se les comuniquen estos datos para que puedan comprobar su exactitud y la legalidad del tratamiento, y

3. corregir, modificar o eliminar los datos cuando sean inexactos o se hayan tratado infringiendo los principios.

ii. Las personas no estarán obligadas a justificar las solicitudes de acceso a sus datos personales. En su respuesta a las solicitudes de acceso de las personas, las entidades deberán primero considerar la motivación de dichas solicitudes. Por ejemplo, si una petición de acceso es vaga o muy amplia, la entidad puede dialogar con el afectado para comprender mejor los motivos de la petición y localizar la información correspondiente. La entidad podrá preguntar con qué parte o partes de la entidad interactuó la persona o sobre la naturaleza de la información o de su uso, que sea objeto de la solicitud de acceso.

iii. Al ser fundamental el principio de acceso, las entidades siempre deben esforzarse de buena fe en facilitar el mismo. Por ejemplo, cuando deba protegerse determinada información y esta se distinga fácilmente de otra información personal que sea objeto de una solicitud de acceso, la entidad deberá separar los datos confidenciales y comunicar la otra información. En caso de que una entidad decida restringir el acceso en un caso particular, deberá facilitar a la persona que solicitó el acceso la debida justificación y un contacto para más información.

b. Carga de trabajo o gasto ocasionado por el acceso

i. El derecho de acceso a los datos personales podrá restringirse en circunstancias excepcionales en las que puedan violarse los derechos legítimos de terceros o cuando la carga de trabajo o el gasto de proporcionar el acceso sean desproporcionados en relación con los riesgos para la privacidad de la persona en cuestión. La carga de trabajo y el gasto son factores importantes y deben tenerse en cuenta, pero no son factores importantes para determinar si es razonable facilitar el acceso.

([1]) La entidad deberá responder a las solicitudes de los particulares relacionadas con las finalidades del tratamiento, las categorías de los datos personales en cuestión y los destinatarios o categorías de destinatarios a quienes se revelan los datos personales.

ii. Por ejemplo, si la información personal se utiliza para decisiones que afecten sustancialmente a la persona (por ejemplo, la denegación o la concesión de importantes beneficios como un seguro, una hipoteca o un trabajo), entonces de conformidad con las demás disposiciones de estos principios complementarios, la entidad debería revelar esta información aun cuando hacerlo sea relativamente difícil o caro. Si la información personal solicitada no es confidencial o no se utilizará para tomar decisiones que afecten sustancialmente a la persona, pero es fácilmente accesible y poco costosa de proporcionar, la entidad deberá proporcionar acceso a esta información.

c. Información comercial confidencial

i. La información comercial confidencial es información que la entidad ha protegido de la revelación, cuando la revelación suponga una ayuda para un competidor del mercado. Las entidades pueden denegar o restringir el acceso en la medida en que la concesión de pleno acceso revelaría su propia información comercial confidencial, como en el caso de predicciones de marketing o clasificaciones generadas por la entidad, o información comercial confidencial de un tercero que esté sujeta a la obligación contractual de confidencialidad.

ii. Cuando la información comercial confidencial pueda ser fácilmente separada de otra información personal sujeta a una solicitud de acceso, la entidad deberá separar la información comercial confidencial y dar a conocer la información no confidencial.

d. Organización de las bases de datos

i. El acceso puede facilitarse en forma de revelación de la información personal pertinente por parte de una entidad a una persona y no requiere el acceso de la persona a la base de datos de la entidad.

ii. El acceso debe facilitarse únicamente en la medida en que la entidad conserve información personal. El principio de acceso no comporta en sí ninguna obligación de conservar, mantener, reorganizar o reestructurar los archivos de información personal.

e. Cuándo puede restringirse el acceso

i. Teniendo en cuenta que las entidades deben hacer todo cuanto esté en sus manos para facilitar el acceso de las personas a sus datos personales, las circunstancias en las que las entidades pueden restringir este acceso son limitadas y las razones de esta restricción deberán ser específicas. De conformidad con la Directiva, una entidad puede restringir el acceso a la información en la medida en que su divulgación pueda interferir con la protección de importantes intereses públicos, como la seguridad nacional, la defensa o la seguridad pública. De igual modo también podrá denegarse el acceso cuando la información personal sea tratada únicamente a efectos de investigación o estadística. Entre otros motivos para denegar o limitar el acceso cabe citar los siguientes:

1. interferencia en la ejecución o aplicación de la ley o con acciones particulares, especialmente la prevención, investigación o detección de delitos o el derecho a un juicio justo;

2. divulgación cuando se violen los derechos legítimos o intereses importantes de otras personas;

3. vulneración de un privilegio o una obligación jurídica o profesional;

4. obstáculo para las investigaciones sobre la seguridad de los empleados o los procedimientos de resolución de reclamaciones, o para la planificación de las sustituciones de los empleados y las reestructuraciones de las empresas, o

5. perjuicio para la confidencialidad necesaria para las funciones de control, inspección o regulación relacionadas con la buena gestión económica o financiera.

ii. Una entidad que se acoja a una excepción tendrá que demostrar su necesidad y las razones para la restricción del acceso, así como proporcionar un punto de contacto para las futuras consultas de particulares.

f. Derecho a obtener confirmación y a cobrar una cuota para cubrir los gastos inherentes a la concesión del acceso

i. Los particulares tienen derecho a obtener confirmación de si una entidad posee o no datos personales relacionados con su persona. Los particulares tienen también derecho a que se les comuniquen los datos personales relacionados con su persona. La entidad podrá cobrar una cuota que no sea excesiva.

ii. El cobro de un cuota podrá justificarse, por ejemplo, cuando las solicitudes de acceso sean notoriamente excesivas, en particular por su carácter repetitivo.

iii. No podrá denegarse el acceso por motivos de coste si el particular se ofrece a pagarlo.

g. Peticiones de acceso repetitivas o abusivas

Una entidad podrá establecer límites razonables en cuanto al número de veces que responderá en un período determinado a las peticiones de acceso de cada persona. Al definir estos límites, la entidad deberá analizar factores tales como la frecuencia con que se actualiza la información, los fines para los que se usan los datos y la naturaleza de la información.

h. Peticiones de acceso fraudulentas

Las entidades no estarán obligadas a proporcionar acceso a menos que reciban información suficiente para confirmar la identidad de la persona que realiza la petición.

i. Plazo para las respuestas

Las entidades deberían responder a las solicitudes de acceso en un plazo razonable de tiempo, de una manera razonable y de una forma que sea fácilmente comprensible para la persona. La entidad que proporcione información a los interesados a intervalos regulares podrá satisfacer la solicitud de acceso de una persona con su divulgación regular, siempre que ello no suponga un retraso excesivo.

9. **Datos de recursos humanos**

a. Cobertura del Escudo de la privacidad

i. Cuando una entidad ubicada en la Unión Europea transfiera información personal de sus trabajadores (pasada o presente) obtenida en el contexto de la relación laboral, a una matriz, filial o a un proveedor de servicios no asociado ubicado en los Estados Unidos que se haya adherido al Escudo de la privacidad, la transferencia disfrutará de las ventajas del Escudo de la privacidad. En tal caso, la recogida de la información y su tratamiento previo a la transferencia se habrán sometido a la legislación nacional del país de la Unión Europea donde se hayan realizado y a cualquier condición o restricción aplicable a su transferencia de conformidad con la normativa vigente.

ii. Los principios del Escudo de la privacidad solamente son pertinentes cuando se transfieran registros identificados o identificables de manera individual o se acceda a ellos. Los informes estadísticos basados en datos generales sobre empleo que no contengan datos personales o el uso de datos anónimos no plantean problemas para el derecho a la vida privada.

b. Aplicación de los principios de notificación y opción

i. Aquellas entidades estadounidenses que hayan recibido de la Unión Europea información sobre los trabajadores dentro del Escudo de la privacidad podrán revelarla a terceros y utilizarla con fines diferentes exclusivamente con arreglo a los principios de notificación y de opción. Por ejemplo, cuando las entidades estadounidenses deseen utilizar la información personal obtenida a través de la relación laboral para fines no relacionados con los laborales, como comunicaciones de márketing, deberán facilitar a los afectados el ejercicio de la opción antes de hacerlo, a menos que estos hayan autorizado la utilización de la información para tales fines. Dicho uso no debe ser incompatible con los fines para los que la información personal ha sido recopilada o, posteriormente, autorizada por la persona. Es más, esta opción no se utilizará para limitar sus oportunidades laborales ni para sancionarles.

ii. Debe advertirse que algunas condiciones de aplicación general a las transferencias procedentes de los Estados miembros pueden excluir otras utilizaciones de la información incluso después de su transferencia fuera de la Unión Europea, y que tales condiciones deben respetarse.

iii. Además, los empresarios deberán realizar todos los esfuerzos razonables para tener en cuenta las preferencias de sus trabajadores en cuanto a la protección de su vida privada. Esto incluirá, por ejemplo, restringir el acceso a los datos, anonimizar determinados datos o bien asignar códigos o seudónimos cuando no se necesiten los nombres reales para la finalidad de gestión de que se trate.

iv. La entidad no aplicará los principios de notificación y opción en la medida y tiempo necesarios para que no haya perjuicio de sus intereses legítimos cuando tome decisiones sobre ascensos, nombramientos y otras decisiones laborales similares.

c. Aplicación del principio de acceso

El principio complementario sobre el acceso proporciona orientación sobre los motivos que pueden justificar la denegación o limitación del acceso previa petición en el ámbito de los recursos humanos. Por supuesto, los empresarios de la Unión Europea deben cumplir las normativas locales y garantizar que los trabajadores europeos tengan acceso a la información de la forma exigida por ley en sus países, independientemente del lugar donde se traten y almacenen los datos. El Escudo de la privacidad exige a las entidades que tratan estos datos en los Estados Unidos que cooperen a la hora de facilitar el acceso directamente o a través del empresario de la UE.

d. Ejecución

i. En la medida en que la información se utilice exclusivamente en el contexto de la relación laboral, la entidad de la UE es la responsable principal de los datos ante el trabajador. De ello se deduce que, cuando los trabajadores europeos planteen reclamaciones sobre la violación de sus derechos de protección de datos y no estén satisfechos con los resultados de los procedimientos de verificación interna, reclamación y apelación (o con cualquier procedimiento de resolución de conflictos a tenor de un contrato con entidades sindicales), deben dirigirse a la agencia nacional de protección de datos o a la autoridad laboral correspondiente a su jurisdicción. Se incluyen también los casos en que la presunta gestión inadecuada de la información personal sea responsabilidad de la entidad estadounidense que haya recibido la información a través del empresario y, por consiguiente, suponga un presunto incumplimiento de los principios del Escudo de la privacidad. Este será el método más eficaz para abordar los derechos y obligaciones, con frecuencia coincidentes, impuestos por la legislación local en materia de empleo y por los convenios colectivos, así como por la legislación sobre protección de datos.

ii. Una entidad estadounidense adherida al Escudo de la privacidad que utilice datos sobre recursos humanos transferidos desde la Unión Europea en el contexto de la relación laboral y que desee que dicha transferencia también esté cubierta por el Escudo de la privacidad, deberá comprometerse a cooperar en las investigaciones de las autoridades de la UE competentes y a acatar sus recomendaciones en dichos casos.

e. Aplicación del principio de responsabilidad de la transferencia ulterior

Para las necesidades operativas ocasionales relacionadas con el empleo de las entidades adheridas al Escudo de la privacidad con relación a los datos personales transferidos en virtud del Escudo de la privacidad, como la reserva de un vuelo, de una habitación de hotel o la cobertura de un seguro, pueden realizarse transferencias de datos personales de un pequeño número de empleados a los responsables del tratamiento de los datos sin necesidad de aplicar el principio de acceso ni suscribir un contrato con el responsable externo de datos, a diferencia de lo que exige el principio de responsabilidad de la transferencia ulterior, siempre y cuando la entidad adherida al Escudo de la privacidad haya observado los principios de notificación y opción.

10. **Contratos obligatorios para transferencias ulteriores**

a. Contratos de tratamiento de datos

i. Cuando desde la UE se transfieren datos personales a los Estados Unidos únicamente a efectos de tratamiento, se exigirá un contrato, independientemente de la participación del responsable del tratamiento en el Escudo de la privacidad.

ii. Los responsables del tratamiento de datos de la Unión Europea están obligados a suscribir un contrato cuando se realiza una transferencia a efectos meramente de tratamiento, independientemente de que la operación de tratamiento se realice dentro o fuera de la UE y de si el encargado del tratamiento participa en el Escudo de la privacidad. El propósito del contrato es garantizar que el encargado del tratamiento:

1. actúe únicamente siguiendo las instrucciones del responsable del tratamiento;

2. proporcione las medidas técnicas y organizativas adecuadas para proteger los datos personales contra la destrucción accidental o ilícita, la pérdida accidental, la alteración, la divulgación o el acceso no autorizados, y entienda si se autoriza la transferencia ulterior; y

3. teniendo en cuenta la naturaleza del tratamiento, ayude al responsable del tratamiento a responder a las personas que ejerzan sus derechos en virtud de los principios.

iii. Dada la adecuada protección que ofrecen los participantes en el Escudo de la privacidad, los contratos con estos participantes para el mero tratamiento no requieren autorización previa (o esta autorización será automáticamente garantizada por los Estados miembros de la UE), a diferencia de la exigencia de los contratos suscritos con destinatarios no participantes en el Escudo de la privacidad o que no proporcionen la protección adecuada.

b. Transferencias dentro de un grupo controlado de empresas o entidades

Cuando se transfiere información personal entre dos responsables del tratamiento pertenecientes a un grupo controlado de empresas o entidades, no siempre se exige la suscripción de un contrato en virtud del principio de responsabilidad de la transferencia ulterior. Los responsables del tratamiento de datos pertenecientes a un grupo controlado de empresas o entidades podrán basar estas transferencias en otros instrumentos, como las Normas Corporativas Vinculantes de la UE u otros instrumentos intragrupo (por ejemplo, programas de cumplimiento y control), lo que garantiza la continuidad de la protección de la información personal de conformidad con los principios. En el caso de estas transferencias, la entidad adherida al Escudo de la privacidad seguirá siendo responsable del cumplimiento de los principios.

c. Transferencias entre responsables del tratamiento

Para las transferencias entre responsables del tratamiento, no es necesario que el responsable del tratamiento destinatario sea una entidad adherida al Escudo de la privacidad o tenga un mecanismo de recurso independiente. La entidad adherida al Escudo de la privacidad deberá suscribir un contrato con el responsable del tratamiento destinatario externo que ofrezca el mismo nivel de protección que el Escudo de la privacidad, sin incluir el requisito de que el responsable del tratamiento externo sea una entidad adherida al Escudo de la privacidad o tenga un mecanismo de recurso independiente, siempre y cuando ofrezca un mecanismo equivalente.

11. **Resolución de conflictos y aplicación**

a. El principio de recurso, aplicación y responsabilidad establece los requisitos para la ejecución del Escudo de la privacidad. En el principio complementario sobre la verificación se establece cómo satisfacer los requisitos del punto (a)(ii) del principio. Este principio complementario aborda los puntos (a)(i) y (a)(iii), que exigen mecanismos de recurso independientes. Estos mecanismos pueden adoptar diferentes formas, pero deben cumplir los requisitos del principio de recurso, aplicación y responsabilidad. Las entidades cumplen los requisitos de la siguiente manera: i) conformidad con programas de protección de la vida privada concebidos por el sector privado que incorporen los principios del Escudo de la privacidad en sus normas y cuenten con mecanismos de aplicación eficaces, similares a los descritos en el principio de recurso, aplicación y responsabilidad; ii) conformidad con lo dispuesto por las autoridades de control establecidas legal o reglamentariamente que prevean la tramitación de reclamaciones individuales y la resolución de litigios; o iii) compromiso de colaboración con las autoridades de protección de datos establecidas en la Unión Europea o sus representantes autorizados.

b. Esta lista se ofrece a título ilustrativo y no es de ninguna manera taxativa. El sector privado podrá designar otros mecanismos para garantizar la aplicación, siempre que cumplan los requisitos del principio de recurso, aplicación y responsabilidad y los principios complementarios. Obsérvese que los requisitos del principio de

recurso, aplicación y responsabilidad se añaden al requisito 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), que prohíbe actos desleales y engañosos, u otra ley o normativa que prohíba este tipo de actos.

c. Con el objeto de garantizar el cumplimiento de los compromisos del Escudo de la privacidad y para apoyar la gestión del programa, las entidades, así como sus mecanismos de recurso independientes, deberán proporcionar información sobre el Escudo de la privacidad cuando así lo solicite el Departamento. Asimismo, las entidades deben responder rápidamente a las reclamaciones relacionadas con su cumplimiento de los principios remitidas a través del Departamento por las APD. La respuesta deberá contemplar si la reclamación está fundamentada, y en caso afirmativo, cómo subsanará el problema la entidad. El Departamento protegerá la confidencialidad de la información que reciba de conformidad con la legislación estadounidense.

d. Mecanismos de recurso

i. se alentará a los consumidores a presentar cualquier reclamación que tengan ante la entidad correspondiente antes de acudir a las instancias de recurso independientes. Las entidades deben responder al consumidor en el plazo de los 45 días siguientes a la recepción de la reclamación. La independencia de dichas instancias de recurso es una cuestión de hecho que puede ser demostrada por la imparcialidad y por la transparencia de su composición y de su financiación, o por exhibir unos antecedentes reconocidos. De conformidad con lo estipulado por el principio de recurso, aplicación y responsabilidad, los recursos que se pongan a disposición de los particulares deben ser rápidos y gratuitos. Los organismos de resolución de litigios admitirán a trámite todas las reclamaciones que reciban de los particulares, a menos que sea patente su falta de base o esta sea de poca entidad, lo cual no impedirá que la entidad gestora de la instancia de recurso establezca condiciones de admisibilidad. Sin embargo, dichas condiciones deberán ser transparentes y justificarse debidamente (por ejemplo, para excluir las reclamaciones que no entran en el ámbito de aplicación del programa o que deben estudiarse en otra instancia), y no deberán obstaculizar el compromiso de admitir a trámite las reclamaciones legítimas. Además, las instancias de recurso proporcionarán a los particulares toda la información disponible sobre el funcionamiento del procedimiento de resolución de litigios cuando presenten la reclamación. Esta información deberá incluir la notificación de las prácticas de protección de la vida privada que utilizan tales instancias, de conformidad con los principios de del Escudo de la privacidad. Las instancias también deberán colaborar en el desarrollo de herramientas tales como formularios normalizados de reclamación para facilitar el proceso de resolución de las reclamaciones,

ii. los mecanismos de recurso independientes deben incluir en sus webs públicas información relacionada con los principios del Escudo de la privacidad y los servicios que ofrecen en virtud del Escudo de la privacidad. Dicha información deberá incluir: 1) información o un enlace a los requisitos de los principios del Escudo de la privacidad para los mecanismos de recurso independientes; 2) un enlace a la web del Escudo de la privacidad del Departamento; 3) una explicación de que los servicios de resolución de conflictos contemplados por el Escudo de la privacidad son gratuitos para las personas; 4) una descripción de cómo puede presentarse una reclamación en relación con el Escudo de la privacidad; 5) el plazo de tramitación de las reclamaciones relacionadas con el Escudo de la privacidad; y 6) una descripción de las posibles vías de recurso,

iii. los mecanismos de recurso independientes deberán publicar un informe anual que incluya estadísticas globales relacionadas con sus servicios de resolución de conflictos. El informe anual deberá incluir: 1) el número total de reclamaciones relacionadas con el Escudo de la privacidad recibidas durante el año objeto del informe; 2) los tipos de reclamaciones recibidas; 3) las medidas de calidad de los mecanismos de resolución de conflictos, como el plazo para la tramitación de las reclamaciones; y 4) los resultados de las reclamaciones recibidas, concretamente el número y los tipos de recursos o las sanciones impuestas,

iv. como se indica en el anexo I, la persona dispone de una opción de arbitraje para determinar, en el caso de las reclamaciones no resueltas, si una entidad adherida al Escudo de la privacidad ha infringido sus obligaciones previstas en el Escudo de la privacidad con relación a esta persona y si dicha infracción sigue estando total o parcialmente sin resolver. Esta opción solamente está disponible para este propósito. Esta opción no está disponible, por ejemplo, para las excepciones a los principios ([1]) ni con respecto a una denuncia sobre el carácter adecuado de la protección del Escudo de la privacidad. De conformidad con esta opción de arbitraje, el panel del Escudo de la privacidad (compuesto por de uno a tres árbitros, según el acuerdo entre las partes) posee la autoridad necesaria para imponer una reparación específica, equitativa y no monetaria (como el acceso, la corrección, la eliminación o la devolución de los datos de la persona en cuestión), necesaria para la reparación de la infracción de los principios en lo que se refiere exclusivamente a la persona. Las personas y las entidades adheridas al Escudo de la privacidad podrán buscar control jurisdiccional y ejecución de las sentencias arbitrales de conformidad con la legislación estadounidense prevista en la Federal Arbitration Act (Ley Federal de Arbitraje).

([1]) Sección I.5 de los principios.

e. Vías de recurso y sanciones

Todo recurso presentado ante el organismo de resolución de litigios deberá dar lugar a la corrección o anulación, en la medida de lo posible, de los efectos del incumplimiento de los principios por parte de la entidad; al respeto de los mismos en tratamientos que la entidad haga en el futuro y, cuando proceda, a la interrupción del tratamiento de los datos personales del particular que haya presentado la reclamación. Las sanciones tienen que ser lo suficientemente rigurosas para que la entidad cumpla los principios. Una gama de sanciones con distintos grados de severidad permitirá a los organismos de resolución de litigios responder debidamente a los diferentes niveles de incumplimiento. Las sanciones deberán incluir la publicidad de los casos de incumplimiento y la obligación de suprimir datos en determinadas circunstancias ([1]). Otras sanciones podrían incluir la suspensión y la eliminación del sello, la indemnización a las personas por las pérdidas sufridas como consecuencia del incumplimiento y la concesión de medidas cautelares. Los organismos de resolución de conflictos del sector privado y los órganos autorreguladores deberán notificar los incumplimientos por parte de las entidades adheridas al Escudo de la privacidad de sus decisiones al organismo público competente o a los tribunales, según el caso, y notificarlo al Departamento.

f. Acción de la FTC

La FTC se ha comprometido a revisar con carácter prioritario las remisiones que denuncien el incumplimiento de los principios recibidas de: i) entidades de autorregulación en materia de protección de la privacidad y de otros organismos independientes de resolución de conflictos; ii) los Estados miembros de la UE; y iii) el Departamento, para determinar si se ha infringido el artículo 5 de la Ley de la FTC, que prohíbe actos o prácticas desleales o fraudulentos en el comercio. En caso de que la FTC concluya que hay motivos para creer que se ha infringido el artículo 5, podrá resolver la cuestión recurriendo a una suspensión administrativa y a una orden de cese que prohíba las prácticas denunciadas, o bien presentar una denuncia en un tribunal federal de distrito que, en caso de éxito, podría desembocar en una orden del tribunal federal en el mismo sentido. Estas infracciones incluyen las falsas alegaciones de adhesión a los principios del Escudo de la privacidad o de participación en el Escudo de la privacidad por parte de entidades que ya no figuren en la lista del Escudo de la privacidad o que nunca se hayan autocertificado ante el Departamento. La FTC puede requerir sanciones civiles si se quebrantan las decisiones administrativas de cese, así como ejercer acciones civiles o penales en los casos de incumplimiento de las resoluciones de los tribunal federales. La FTC notificará al Departamento la adopción de estas acciones. El Departamento insta a otros organismos públicos a que le notifiquen el resultado de todos los asuntos análogos o de otras sentencias que establezcan la adhesión a los principios del Escudo de la privacidad.

g. Incumplimiento sistemático

i. si una entidad incumple sistemáticamente los principios, cesará su derecho a beneficiarse del Escudo de la privacidad. Las entidades que hayan incumplido repetidamente los principios serán eliminadas de la lista del Escudo de la privacidad por el Departamento y deberán devolver o eliminar la información personal que recibieron en virtud del Escudo de la privacidad,

ii. se considera incumplimiento sistemático cuando una entidad que haya autocertificado su adhesión a los principios ante el Departamento se niegue a cumplir las resoluciones de un organismo de autorregulación, un organismo de resolución de litigios independiente, o un organismo público, o si uno de estos organismos considera que una entidad incumple con frecuencia los principios, hasta el punto en que su declaración de adhesión deja de ser creíble. En estos casos, la entidad deberá notificar inmediatamente los hechos al Departamento. El incumplimiento de esta obligación puede ser punible en el marco de la False Statements Act (Ley relativa a las declaraciones falsas, USC título 18, artículo 1001). Una entidad que se retire de un programa de autorregulación sobre la protección de la privacidad gestionado por el sector privado o de un mecanismo de resolución de conflictos independiente no queda eximida de su obligación de observar los principios e incurriría en un incumplimiento sistemático,

iii. el Departamento eliminará a una entidad de la lista del Escudo de la privacidad en respuesta a toda notificación que reciba de incumplimiento sistemático, tanto si la recibe de la propia entidad como si procede de un organismo de autorregulación de la privacidad, de otro órgano de resolución de conflictos independiente o de un organismo público, pero proporcionará un plazo de 30 días para notificar este

([1]) Los organismos de resolución de litigios apreciarán las circunstancias en que deben aplicarse estas sanciones. La sensibilidad de los datos en cuestión es un factor a tener en cuenta a la hora de decidir si debe exigirse la supresión de los datos, al igual que también debe tenerse en cuenta si una entidad ha recogido, utilizado o divulgado información incumpliendo manifiestamente los principios del Escudo de la privacidad.

extremo a la entidad incumplidora y le concederá la oportunidad de alegar. En consecuencia, la lista del Escudo de la privacidad mantenida por el Departamento aclarará qué entidades están garantizadas y qué entidades ya no disfrutan de los beneficios del Escudo de la privacidad,

iv. una entidad que solicite participar en un organismo de autorregulación con el fin de volver a acogerse a los principios del Escudo de la privacidad deberá facilitar a dicho organismo información completa sobre su participación anterior en el Escudo de la privacidad.

12. **Opción — Momento del ejercicio del derecho de exclusión**

a. En general, el objeto del principio de opción es garantizar que la información personal se utiliza y difunde de manera coherente con las expectativas y opciones del afectado. Por tanto, cualquier persona debería tener la posibilidad de ejercer el derecho de «exclusión» de su información personal con fines de márketing directo en cualquier momento, con los límites de tiempo razonables establecidos por la entidad, como dejar un plazo suficiente para que esta pueda aplicar dicho derecho de exclusión. Asimismo, una entidad puede requerir información suficiente para confirmar la identidad de la persona que solicita la «exclusión». En los Estados Unidos, se puede ejercer esta opción mediante un programa central de «exclusión» como el «Mail Preference Service» de la Direct Marketing Association. Las entidades que participen en este programa deberán fomentar la disponibilidad del mismo entre los consumidores que no deseen recibir información comercial. En cualquier caso, todo ciudadano debe tener acceso a un mecanismo rápido y asequible para ejercitar esta opción.

b. De la misma forma, una entidad puede utilizar la información para determinados fines de márketing directo cuando sea imposible proporcionar al afectado la oportunidad de ejercer su derecho de exclusión antes de usar la información, siempre que le ofrezca de inmediato dicha posibilidad (y en cualquier momento, previa petición) de negarse (sin coste alguno para el consumidor) a recibir posteriores envíos de márketing directo y que la entidad se ajuste a los deseos del afectado.

13. **Información sobre viajes**

a. La reserva de un billete de avión y otra información de viaje, como la información de viajero frecuente, de reserva hotelera y de necesidades especiales como la dieta por motivos religiosos, o la asistencia física, podrá ser transferida a entidades radicadas fuera de la UE en diversas circunstancias. De conformidad con el artículo 26 de la Directiva, podrá efectuarse una transferencia de datos personales «a un tercer país que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25» siempre y cuando: i) la transferencia sea necesaria para proporcionar los servicios solicitados por el consumidor o cumplir un convenio, como el programa de fidelización «viajero frecuente» («frequent flyer»); o ii) el consumidor haya dado su consentimiento inequívocamente. Las entidades estadounidenses que suscriben el Escudo de la privacidad ofrecen una protección adecuada de los datos y por consiguiente pueden recibir datos transferidos de la Unión Europea sin cumplir estas condiciones u otras condiciones expuestas en el artículo 26 de la Directiva. Dado que el Escudo de la privacidad incluye normas específicas para datos sensibles, dicha información (que puede ser preciso recoger, por ejemplo, en relación con las necesidades de asistencia física de los clientes) puede incluirse en las transferencias a participantes en el Escudo de la privacidad. No obstante, en todos los casos, la organización que transfiere la información ha de cumplir la legislación del Estado miembro de la Unión Europea en el que opera, que, entre otras cosas, puede imponer condiciones especiales para el tratamiento de datos sensibles.

14. **Productos médicos y farmacéuticos**

a. Aplicación de la legislación del Estado miembro de la UE o de los principios del Escudo de la privacidad

Las leyes de los Estados miembros se aplican a la recogida de los datos personales y a cualquier tratamiento previo a su transferencia a los Estados Unidos. Los principios del Escudo de la privacidad se aplicarán a los datos una vez que se hayan transferido a los Estados Unidos. Los datos personales utilizados con fines de investigación farmacéutica u otros deben ser convertidos en datos anónimos cuando resulte adecuado.

b. Futuras investigaciones científicas

i. los datos personales elaborados en estudios de investigación médica o farmacéutica suelen desempeñar un valioso papel en futuras investigaciones científicas. Cuando se transfieren datos personales recogidos para un estudio de investigación a una entidad estadounidense acogida al Escudo de la privacidad, la entidad podrá utilizar los datos en una nueva actividad de investigación científica si ha proporcionado con anterioridad la debida notificación y posibilidad de optar. En la notificación se proporcionará información sobre la utilización concreta que se dará a los datos, a saber, seguimiento, otros estudios o márketing,

ii. se sobreentiende que no podrán especificarse todas las utilizaciones futuras de los datos, ya que estas pueden resultar de un nuevo enfoque de los datos originales, de nuevos descubrimientos y avances médicos, y de novedades en materia legislativa y de salud pública. Por consiguiente, la notificación debería incluir, si procede, una referencia a la posible utilización de los datos personales en futuras actividades de investigación médica y farmacéutica que todavía se desconocen. Será necesario obtener un nuevo consentimiento si la utilización no es coherente con las finalidades de investigación general para las que se recogieron originalmente los datos o dieron posteriormente los particulares su consentimiento.

c. Retirada de un ensayo clínico

Los participantes pueden decidir voluntariamente o a instancias de terceros retirarse de un ensayo clínico en cualquier momento. No obstante, los datos recogidos con anterioridad a la retirada podrán seguir siendo tratados con los demás datos del ensayo clínico si este extremo quedó claro en la notificación a los participantes en el momento en que dieron su acuerdo para participar.

d. Transferencias con fines de regulación y control

Las empresas de productos farmacéuticos y médicos tienen autorización para facilitar datos personales obtenidos en ensayos clínicos realizados en la Unión Europea a las autoridades de regulación de los Estados Unidos con fines de regulación y control. Se autorizan transferencias similares a terceros que no sean las autoridades de regulación, como filiales de las empresas u otros investigadores, con arreglo a los principios de notificación y opción.

e. Experimentos a ciegas

i. muchas veces, para garantizar la objetividad de los ensayos clínicos, se priva a los participantes y, con frecuencia, también a los investigadores, de información sobre el tratamiento. Este proceder podría poner en peligro la validez de los estudios de investigación y de sus resultados. A los participantes en estos ensayos clínicos (denominados «experimentos a ciegas») no se les proporcionará acceso a datos sobre su tratamiento durante el ensayo si se les explicó tal restricción cuando se unieron al ensayo y si la revelación de la información puede poner en peligro la integridad de la investigación,

ii. consentir la participación en los ensayos en estas condiciones constituye un modo razonable de renunciar al derecho de acceso. Tras la conclusión del ensayo y el análisis de los resultados, los participantes tendrán acceso a sus datos si lo solicitan. En primer lugar, se dirigirán al médico o profesional sanitario de quien recibieron tratamiento en el marco del ensayo clínico y, en segundo lugar, a la empresa patrocinadora.

f. Control de la eficacia y la seguridad de los productos

Las empresas de productos médicos o farmacéuticos no están obligadas a aplicar los principios del Escudo de la privacidad en lo relativo a la notificación, opción, transferencia ulterior y acceso, en las actividades que realizan para garantizar la seguridad de los productos y controlar su eficacia, entre ellas la información sobre circunstancias adversas y el seguimiento de los pacientes o personas que utilicen determinadas medicinas o dispositivos

médicos, en la medida en que la adhesión a los principios interfiera en el cumplimiento de las exigencias legales. Esto se aplica tanto a los informes de los profesionales sanitarios dirigidos a las empresas de productos médicos y farmacéuticos, como a los de estos a organismos de la administración como la *Food and Drug Administration*.

g. Datos codificados

El investigador principal codifica siempre los datos de la investigación, en su origen, con una clave única, para que no se conozca la identidad de los interesados. Las empresas farmacéuticas que patrocinan la investigación no reciben la clave. El código original solo lo conoce el investigador, de modo que solo él puede identificar al sujeto de la investigación en determinadas circunstancias (por ejemplo, cuando es necesario un seguimiento médico). Una transferencia de datos codificados de esta forma desde la Unión Europea a los Estados Unidos no constituiría una transferencia de datos personales sujeta a los principios del Escudo de la privacidad.

15. **Información de registros públicos e información accesible al público**

a. Una entidad deberá aplicar los principios del Escudo de la privacidad relativos a la seguridad, la integridad de los datos y limitación de la finalidad, y recurso, aplicación y responsabilidad, a los datos personales obtenidos de fuentes accesibles al público. Estos principios se aplicarán también a los datos personales obtenidos de registros públicos, por ejemplo, los registros mantenidos por los organismos públicos o entidades a cualquier nivel abiertos a la consulta del público en general.

b. No es necesario aplicar los principios de notificación, opción y responsabilidad de la transferencia ulterior a la información extraída de registros públicos siempre que no se combine con información de otros registros no públicos y se cumplan las condiciones de consulta establecidas por la jurisdicción competente. Asimismo, generalmente no es necesario aplicar los principios de notificación, opción y responsabilidad de la transferencia ulterior a la información de dominio público a menos que el remitente europeo indique que dicha información está sujeta a restricciones que exigen la aplicación de tales principios por parte de la entidad para los usos a los que piensa destinarla. Las entidades no tendrán ninguna responsabilidad sobre el uso de la información por quienes la obtengan de materiales publicados.

c. Cuando se descubra que una entidad ha hecho pública intencionadamente información personal contraviniendo los principios, para beneficiarse de estas excepciones o beneficiar a terceros, la entidad dejará de estar cualificada para disfrutar de los beneficios del Escudo de la privacidad.

d. No es necesario aplicar el principio de acceso a la información de los registros públicos, siempre que no se combine con otra información personal, excepto en el caso de que se utilice una pequeña cantidad de datos para indizar u organizar la información de los registros públicos; sin embargo, deberán respetarse las condiciones de consulta establecidas por la jurisdicción correspondiente. Por el contrario, cuando la información de registros públicos se combine con información de otros registros que no sean públicos (con la excepción indicada anteriormente) las entidades deben facilitar el acceso a toda la información, suponiendo que no esté sujeta a otras excepciones permitidas.

e. Como sucede con la información de los registros públicos, no es necesario facilitar el acceso a la información de dominio público siempre que no se combine con información que no sea de dominio público. Las entidades dedicadas a la venta de información de dominio público podrán cobrar los honorarios habituales para responder a las peticiones de acceso. Alternativamente, los afectados podrán acceder a su información directamente a través de la entidad que haya compilado los datos inicialmente.

16. **Solicitudes de acceso de las autoridades públicas**

a. Con el objeto de garantizar la transparencia de las solicitudes lícitas de acceso a la información personal procedentes de las autoridades públicas, las entidades adheridas al Escudo de la privacidad podrán emitir voluntariamente informes periódicos de transparencia sobre el número de solicitudes de información personal que reciben de las autoridades públicas para la aplicación de la ley o por razones de seguridad nacional, siempre y cuando dichas divulgaciones sean permisibles en virtud de la ley aplicable.

b. La información proporcionada por las entidades adheridas al Escudo de la privacidad en estos informes, junto con la información emitida por los servicios de inteligencia y otras informaciones, podrá ser utilizada para contribuir a la revisión conjunta anual del funcionamiento del Escudo de la privacidad de conformidad con los principios.

c. La falta de notificación prevista en el punto (a)(xii) del principio de notificación no impedirá ni perjudicará la capacidad de la entidad de responder a las solicitudes lícitas.

ANEXO I

Modelo de arbitraje

Este anexo I comprende los términos en virtud de los cuales las entidades adheridas al Escudo de la privacidad están obligadas a arbitrar las reclamaciones, de conformidad con el principio de recurso, aplicación y responsabilidad. La opción del arbitraje vinculante descrita a continuación se aplica a determinadas reclamaciones «no resueltas» relativas a los datos cubiertos por el Escudo de la privacidad UE-EE. UU. El objetivo de esta opción es ofrecer un mecanismo rápido, independiente y equitativo, opcional para los ciudadanos, para la resolución de las infracciones denunciadas de los principios no resueltas por uno de los mecanismos del Escudo de la privacidad, si los hay.

A. **Ámbito de aplicación**

Los ciudadanos disponen de una opción de arbitraje para determinar, en el caso de las reclamaciones no resueltas, si una entidad adherida al Escudo de la privacidad ha infringido sus obligaciones previstas con relación al ciudadano en cuestión, y si dicha infracción sigue estando total o parcialmente sin resolver. Esta opción solamente está disponible para este propósito. Esta opción no está disponible, por ejemplo, por lo que respecta a las excepciones a los principios ([1]) ni con respecto a una denuncia sobre el carácter adecuado del Escudo de la privacidad.

B. **Recursos disponibles**

De conformidad con esta opción de arbitraje, el panel del Escudo de la privacidad (compuesto por de uno a tres árbitros, según el acuerdo entre las partes) posee la autoridad necesaria para imponer una reparación específica, equitativa y no monetaria (como el acceso, la corrección, la eliminación o la devolución de los datos de la persona en cuestión), necesaria para la reparación de la infracción de los principios en lo que se refiere exclusivamente a la persona. Estos son los únicos poderes del panel de arbitraje con respecto a los recursos. Al ponderar las reparaciones, el panel de arbitraje deberá considerar otras reparaciones previamente aplicadas por otros mecanismos en virtud del Escudo de la privacidad. No están disponibles las indemnizaciones, costes, honorarios u otras reparaciones. Cada parte asume los honorarios de sus abogados.

C. **Requisitos previos al arbitraje**

La persona que decida invocar esta opción de arbitraje deberá tomar las siguientes medidas antes de entablar una demanda de arbitraje: 1) plantear la infracción denunciada directamente a la entidad y ofrecerle la posibilidad de resolver la cuestión dentro del plazo establecido en el apartado III.11(d)(i) de los principios; 2) utilizar el mecanismo de recurso independiente contemplado en los principios, sin coste alguno para la persona, y 3) plantear la cuestión a través de su Autoridad de Protección de Datos al Departamento de Comercio y ofrecer al Departamento de Comercio la posibilidad de hacer todo cuanto pueda para resolver la cuestión en los plazos estipulados en la carta de la *International Trade Administration* (Administración de Comercio Internacional) del Departamento de Comercio, sin cargo alguno para la persona.

Esta opción de arbitraje no podrá ser invocada si esta misma infracción de los principios denunciada por la persona 1) estuvo anteriormente sujeta al arbitraje vinculante; 2) fue objeto de una sentencia firme dictada en un proceso judicial del que el particular fuera parte; o 3) fue anteriormente resuelta por las partes. Además, esta opción no podrá ser invocada si una Autoridad de Protección de Datos de la UE 1) tiene autoridad en virtud de los apartados III.5 o III.9 de los principios; o 2) tiene autoridad para resolver la infracción denunciada directamente con la entidad. La autoridad que tiene una APD para resolver la misma reclamación contra un responsable del tratamiento de la UE no impide la invocación de esta opción de arbitraje contra una entidad jurídica distinta no sujeta a la autoridad de la APD.

D. **Naturaleza vinculante de las decisiones**

La decisión de una persona de invocar esta opción de arbitraje vinculante es totalmente voluntaria. Las decisiones arbitrales serán vinculantes para todas las partes del arbitraje. Una vez invocada, la persona renuncia a la opción de solicitar reparación por la misma infracción denunciada en otro foro, con la excepción de que, en caso de que una medida no monetaria equitativa no resuelva totalmente la infracción denunciada, la invocación del arbitraje por parte de la persona no impedirá una reclamación por daños y perjuicios, recurriendo para ello a la justicia ordinaria.

([1]) Apartado I.5 de los principios.

E. **Control y ejecución**

Los particulares y las entidades adheridas al Escudo de la privacidad podrán solicitar el control judicial y la ejecución de las decisiones arbitrales de conformidad con la legislación estadounidense prevista en la Ley Federal de Arbitraje ([1]). Todos estos casos pueden ser llevados al tribunal de distrito federal cuya competencia territorial incluya el domicilio social principal de la entidad adherida al Escudo de la privacidad.

Esta opción de arbitraje pretende resolver las disputas individuales, y las sentencias arbitrales no pretenden funcionar como un precedente persuasivo o vinculante en cuestiones que impliquen a otras partes, inclusive en los futuros arbitrajes o en los tribunales de la UE o de EE. UU. o en los procedimientos de la FTC.

F. **Panel de arbitraje**

Las partes elegirán a los árbitros de la lista de árbitros mencionada a continuación.

De conformidad con la legislación aplicable, el Departamento de Comercio estadounidense y la Comisión Europea elaborarán una lista de como mínimo 20 árbitros, elegidos en función de su independencia, integridad y experiencia. Con relación a este proceso se aplicará cuanto sigue:

Árbitros:

1) se mantendrán en la lista durante un período de 3 años, a falta de circunstancias excepcionales o motivos justificados, renovable por un período adicional de 3 años;

2) no podrán recibir instrucciones ni estar asociados a ninguna de las partes, ninguna entidad adherida al Escudo de la privacidad, ni a ninguna otra autoridad gubernamental, autoridad pública u organismo de ejecución de EE. UU., de la UE o de un Estado miembro de la UE, y

3) deberán estar habilitados para ejercer la práctica jurídica en EE. UU. y ser expertos en legislación estadounidense en materia de privacidad, así como tener conocimientos en materia de legislación sobre protección de datos de la UE.

G. **Procedimientos de arbitraje**

De conformidad con la legislación aplicable, en el plazo de los 6 meses siguientes a la adopción de la decisión de adecuación, el Departamento de Comercio y la Comisión Europea acordarán adoptar un conjunto de procedimientos arbitrales estadounidenses existente y establecido (como AAA o JAMS) para regular los procedimientos ante el panel del Escudo de la privacidad, a reserva de las siguientes consideraciones:

1. Un particular podrá entablar un arbitraje vinculante sujeto a la disposición de los requisitos de pre-arbitraje antes mencionados, presentando una «notificación» a la entidad. La notificación deberá contener un resumen de los pasos acometidos en virtud del apartado C para resolver la reclamación, una descripción de la presunta infracción y, a discreción del particular, documentos y material justificativo o un análisis de la legislación aplicable a la reclamación en cuestión.

([1]) El capítulo 2 de la Ley Federal de Arbitraje («FAA», por sus siglas en inglés) establece que «un acuerdo de arbitraje o una sentencia arbitral que se derive de una relación jurídica, contractual o no, considerada comercial, incluida una transacción, contrato o acuerdo descrito en la [sección 2 de la FAA] corresponde a la Convención [sobre el reconocimiento y ejecución de las sentencias arbitrales extranjeras, de 10 de junio de 1958, 21 U.S.T. 2519, T.I.A.S. n.º 6997 ("Convención de Nueva York")]». 9 U.S.C. § 202. La FAA establece asimismo que «el acuerdo o la sentencia que se derive de dicha relación entre los ciudadanos de Estados se considerará que no corresponde a la Convención [de Nueva York] salvo que esa relación comporte una propiedad situada en el extranjero, contemple el cumplimiento o la ejecución en el extranjero o tenga alguna relación razonable de otro tipo con uno o más países extranjeros». *Íd.* De conformidad con el capítulo 2, «cualquier parte del arbitraje podrá recurrir a un tribunal que tenga jurisdicción en virtud de este capítulo para obtener una orden que confirme la sentencia contra cualquier otra parte del arbitraje. El tribunal confirmará la sentencia salvo que encuentre fundamentos para la denegación o el aplazamiento del reconocimiento o de la ejecución de la sentencia especificados en dicha Convención [de Nueva York]». *Id.* § 207. El capítulo 2 establece además que «los tribunales de distrito de los Estados Unidos... tendrán jurisdicción original sobre... una acción o procedimiento [en virtud de la Convención de Nueva York], independientemente del importe en cuestión». *Id.* § 203.
El capítulo 2 también establece que «se aplicará el capítulo 1 a las acciones y procedimientos contemplados en el presente capítulo, en la medida en que dicho capítulo no contravenga al presente capítulo o a la Convención [de Nueva York], tal como fue ratificada por Estados Unidos.» *Id.* § 208. A su vez, el capítulo 1 establece que «una disposición por escrito en... un contrato que evidencie una transacción comercial dirigida a resolver mediante arbitraje una controversia derivada de dicho contrato o transacción, o de la negativa a ejecutar la totalidad o parte del dicho contrato o transacción, o un acuerdo por escrito que comprometa a las partes a someter a arbitraje una controversia existente derivada de este contrato, transacción o negativa, será válido, irrevocable y ejecutable, salvo que existan motivos previstos por la ley o por el principio de equidad para la revocación de un contrato». *Id.* § 2. El capítulo 1 establece además que «cualquier parte del arbitraje podrá solicitar al tribunal especificado una orden que confirme la sentencia, y acto seguido el tribunal deberá conceder esta orden salvo que la sentencia haya sido anulada, modificada o corregida de conformidad con lo estipulado en las secciones 10 y 11 de [la FAA]». *Id.* § 9.

2. Se desarrollarán los procedimientos necesarios para garantizar que una misma infracción denunciada por una persona no sea objeto de recursos o procedimientos por duplicado.

3. La acción de la FTC podrá continuar en paralelo con el arbitraje.

4. Ningún representante de EE. UU., de la UE o de un Estado miembro de la UE ni ninguna autoridad gubernamental, autoridad pública u organismo de ejecución podrá participar en estos arbitrajes, si bien a petición de un particular de la UE, las APD de la UE podrán ofrecer asistencia para preparar la notificación únicamente, pero sin poder acceder a los contenidos ni a ningún otro material relacionado con estos arbitrajes.

5. La ubicación del arbitraje será los Estados Unidos, y la persona podrá elegir participar por videoconferencia o por teléfono, lo que se le facilitará sin coste alguno para la misma. No se exigirá la participación presencial.

6. El idioma del arbitraje será el inglés, salvo que las partes acuerden lo contrario. Tras una petición razonada, y teniendo en cuenta si la persona está representada por un abogado, se ofrecerá servicio de interpretación en la vista del arbitraje así como de traducción de los materiales del arbitraje, sin coste alguno para la persona, salvo que el panel decida que, en las circunstancias del arbitraje en concreto, esto supondría unos costes injustificados o desproporcionados.

7. Los materiales presentados a los árbitros serán tratados confidencialmente y solo se utilizarán con relación al arbitraje.

8. Si es necesario, podrá permitirse la revelación de contenidos específicos de la persona, y dicha revelación será tratada confidencialmente por las partes y solo se utilizará con relación al arbitraje.

9. Los arbitrajes deberán finalizarse en el plazo de los 90 días siguientes a la entrega de la notificación a la entidad en cuestión, salvo que las partes acuerden lo contrario.

H. **Costes**

Los árbitros deberán tomar medias razonables para minimizar los costes o gastos de los arbitrajes.

De conformidad con la legislación aplicable, el Departamento de Comercio facilitará el establecimiento de un fondo al que las entidades adheridas al Escudo de la privacidad deberán pagar una contribución anual, basada en parte en el tamaño de la entidad, que cubrirá el coste del arbitraje, incluidos los honorarios de los árbitros, hasta unas cantidades máximas («límites»), en consulta con la Comisión Europea. El fondo será gestionado por un tercero, el cual informará regularmente sobre las operaciones del fondo. En la revisión anual, el Departamento de Comercio y la Comisión Europea examinarán el funcionamiento del fondo, incluida la necesidad de ajustar el importe de las contribuciones o de los límites, y tendrán en cuenta, entre otras cosas, el número de arbitrajes, los costes y la duración de los arbitrajes, con el entendimiento mutuo de que no se impondrá una carga excesiva a las entidades adheridas al Escudo de la privacidad. Los honorarios de los abogados no están cubiertos por esta disposición ni por ningún fondo contemplado en esta disposición.

ANEXO III

Carta del Secretario de Estado estadounidense, John Kerry

7 de julio de 2016

Estimada Comisaria Jourová:

Me complace haber alcanzado un acuerdo sobre el Escudo de la privacidad UE-EE. UU. que incluirá el mecanismo del Defensor del Pueblo a través del cual las autoridades de la UE podrán presentar peticiones en nombre de los ciudadanos de la UE relacionadas con las prácticas de la inteligencia de señales.

El 17 de enero de 2014, el presidente Barack Obama anunció las importantes reformas de inteligencia incluidas en la *Presidential Policy Directive* 28 (en lo sucesivo, «PPD-28»). En virtud de la PPD-28, nombré a la Subsecretaria de Estado Catherine A. Novelli, que a su vez es *Senior Coordinator for International Information Technology Diplomacy* (coordinadora superior de la diplomacia internacional en materia de tecnología de la información), como punto de contacto para los gobiernos extranjeros que deseen plantear sus dudas con relación a las actividades de la inteligencia de señales estadounidense. En la definición de esta función, he creado la figura del Defensor del Pueblo en el ámbito del Escudo de la privacidad de acuerdo con los términos establecidos en el anexo A, que se han actualizado desde mi carta de 22 de febrero de 2016. He dado órdenes a la Subsecretaria Novelli para que realice esta función. La Subsecretaria Novelli es miembro independiente de los servicios de inteligencia estadounidenses y está bajo mis órdenes directas.

He dado instrucciones a mi personal para que dedique los recursos necesarios a la implantación de esta nueva figura del Defensor del Pueblo y confío en que será un medio eficaz para abordar las preocupaciones de los particulares de la UE.

Atentamente,

John F. Kerry

Anexo A

La figura del Defensor del Pueblo en el ámbito del Escudo de la privacidad UE-EE. UU. con relación a la inteligencia de señales

En reconocimiento a la importancia del marco del Escudo de la privacidad UE-EE. UU., este memorando establece el procedimiento para la implantación de un nuevo mecanismo, en virtud de la Presidential Policy Directive 28 (PPD-28), que contempla la inteligencia de señales ([1]).

El 17 de enero de 2014, el presidente Obama pronunció un discurso en el que anunció importantes reformas en el ámbito de la inteligencia. En este discurso, hizo hincapié en que «nuestros esfuerzos nos permiten proteger no solo nuestra nación, sino también a nuestros amigos y aliados. Nuestros esfuerzos solo serán efectivos si los ciudadanos de otros países confían en que los Estados Unidos respetan también su privacidad». El presidente Obama anunció la publicación de una nueva directiva presidencial, la PPD-28, para «exponer con claridad lo que hacemos y lo que no hacemos en lo que se refiere a nuestra vigilancia en el extranjero».

El artículo 4(d) de la PPD-28 exige que el Secretario de Estado designe un «*Senior Coordinator for International Information Technology Diplomacy*» (coordinador superior) «para […] que actúe como punto de contacto con los gobiernos extranjeros que deseen plantear sus dudas con respecto a las actividades de la inteligencia de señales llevadas a cabo por los Estados Unidos». A partir de enero de 2015, la Subsecretaria C. Novelli ejerce de coordinadora superior.

El presente memorando describe el nuevo mecanismo que deberá observar la coordinadora superior para facilitar el tratamiento de las peticiones relacionadas con el acceso a efectos de la seguridad nacional a los datos transmitidos desde la UE a los Estados Unidos en virtud del Escudo de la privacidad, las cláusulas contractuales estándar, las normas vinculantes para las empresas, las «excepciones» ([2]) o «posibles futuras excepciones» ([3]), a través de las vías establecidas en virtud de la legislación y la política estadounidense aplicable, y la respuesta a estas peticiones.

1. **El Defensor del Pueblo en el ámbito del Escudo de la privacidad.** La coordinadora superior actuará de Defensor del Pueblo en el ámbito del Escudo de la privacidad y designará otros funcionarios del Departamento de Estado para que le ayuden en el ejercicio de las responsabilidades detalladas en este memorando. (En lo sucesivo, la coordinadora y los agentes que realicen este cometido recibirán el nombre de «Defensor del Pueblo en el ámbito del Escudo de la privacidad»). El Defensor del Pueblo en el ámbito del Escudo de la privacidad trabajará estrechamente con los funcionarios de otros departamentos y organismos responsables del tratamiento de las solicitudes de conformidad con la legislación y la política aplicable de los Estados Unidos. El Defensor del Pueblo es independiente de los servicios de inteligencia. El Defensor del Pueblo informará directamente al Secretario de Estado, que garantizará que aquel desempeñe sus funciones de manera objetiva y sin ninguna influencia indebida que pueda afectar a la respuesta que debe proporcionarse.

2. **Coordinación eficaz.** El Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá utilizar y coordinarse efectivamente con los organismos supervisores, descritos a continuación, con el objeto de garantizar que la respuesta del Defensor del Pueblo a las solicitudes presentadas por el organismo de tramitación de reclamaciones de los

([1]) Dado que la Decisión de la Comisión sobre la adecuación de la protección ofrecida por el Escudo de la privacidad UE-EE. UU. es aplicable a Islandia, Liechtenstein y Noruega, el paquete del Escudo de la privacidad cubrirá tanto a la Unión Europea como a estos tres países. En consecuencia, deberá interpretarse que las referencias a la UE y a sus Estados miembros incluyen a Islandia, Liechtenstein y Noruega.

([2]) En este contexto, «excepciones» significa una transferencia o transferencias comerciales que se realicen con la condición de que: a) el interesado haya dado su consentimiento a la transferencia propuesta de forma inequívoca; o b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la aplicación de medidas precontractuales a petición del interesado; o c) la transferencia sea necesaria para la conclusión o ejecución de un contrato celebrado en beneficio del interesado entre el responsable del tratamiento y un tercero; o d) la transmisión es necesaria o legalmente obligatoria por razones importantes de interés público o para el establecimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial; o e) la transferencia sea necesaria para proteger intereses vitales 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.

([3]) En este contexto, «posibles futuras excepciones» significa una transferencia o transferencias comerciales que se realicen bajo una de las siguientes condiciones, siempre y cuando la condición constituya un fundamento legalmente admisible para las transferencias de datos personales desde la UE a EE. UU.: a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías apropiadas; o b) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; o c) en el caso de una transferencia a un tercer país o a una entidad internacional y cuando ninguna de las demás excepciones o posibles futuras excepciones sean aplicables, únicamente si la transferencia no es repetitiva, afecta solo a un reducido número de interesados y es necesaria a efectos de los intereses legítimos imperiosos perseguidos por el responsable del tratamiento, siempre que dichos intereses no se vean anulados por los intereses o derechos y libertades del interesado, y si el responsable del tratamiento ha valorado todas las circunstancias que rodean a la transferencia de datos y, a partir de esta valoración, ha aportado las protecciones adecuadas con respecto a la protección de los datos personales.

ciudadanos de la UE se fundamente en la información necesaria. Cuando la solicitud se refiera a la compatibilidad de la vigilancia con la legislación estadounidense, el Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá colaborar con uno de los órganos de supervisión independientes que tenga competencias de investigación.

a. El Defensor del Pueblo en el ámbito del Escudo de la privacidad colaborará estrechamente con otros funcionarios del Gobierno estadounidense, incluidos los organismos de vigilancia independientes, para garantizar el tratamiento de las solicitudes y resolverlas de conformidad con las leyes y las políticas aplicables. Concretamente, el Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá coordinarse con la Office of the Director of National Intelligence (Oficina del Director de Inteligencia Nacional), el Departamento de Justicia y otros departamentos y organismos implicados en la seguridad nacional de los Estados Unidos, y con los inspectores generales, los agentes responsables de la ejecución de la Freedom of Information Act (Ley relativa a la libertad de información) y los agentes responsables de la protección de las libertades civiles y la privacidad.

b. El Gobierno de los Estados Unidos confiará en los mecanismos de coordinación y supervisión de las cuestiones de seguridad nacional previstos en los departamentos y organismos para garantizar que el Defensor del Pueblo en el ámbito del Escudo de la privacidad pueda responder de conformidad con el significado de la sección 4(e) a las solicitudes estipuladas en la sección 3(b).

c. El Defensor del Pueblo en el ámbito del Escudo de la privacidad podrá remitir las cuestiones relacionadas con las solicitudes al Privacy and Civil Liberties Oversight Board (consejo de supervisión de la privacidad y de las libertades civiles) para su consideración.

3. **Presentación de solicitudes**

a. Las solicitudes se presentarán inicialmente a las autoridades de control de los Estados miembros competentes para la supervisión de los servicios de seguridad nacional y/o el tratamiento de datos personales por parte de las autoridades públicas. La solicitud se presentará al Defensor del Pueblo por parte de un organismo centralizado de la UE (en adelante, conjuntamente: «organismo de tramitación de las reclamaciones de ciudadanos de la UE»).

b. El organismo de tramitación de las reclamaciones de ciudadanos de la UE garantizará, de conformidad con las siguientes acciones, que la solicitud esté completa:

i) Comprobará la identidad de la persona y que dicha persona actúe en su propio nombre y no como representante de una entidad gubernamental o intergubernamental.

ii) Comprobará que la solicitud sea por escrito y que contenga la siguiente información básica:

— cualquier información que constituya la base para la solicitud,

— la naturaleza de la información o de la reparación solicitada,

— las entidades del Gobierno de los Estados Unidos presuntamente implicadas, si las hay, y

— el resto de medidas adoptadas para obtener la información o la reparación solicitada y la respuesta recibida a través de esas otras medidas.

iii) Comprobará que la solicitud corresponda a unos datos que se acredite razonablemente que han sido transferidos desde la UE a los Estados Unidos en virtud del Escudo de la privacidad, las cláusulas contractuales estándar, las normas vinculantes para las empresas, las excepciones o las posibles futuras excepciones.

iv) Procederá a una determinación inicial de que la solicitud no sea infundada, abusiva o presentada de mala fe.

c. Para que sea completa a efectos de la posterior tramitación por el Defensor del Pueblo en el ámbito del Escudo de la privacidad de conformidad con este memorando, no es preciso que la solicitud demuestre que el Gobierno de los Estados Unidos ha accedido a los datos del solicitante a través de las actividades de inteligencia de señales.

4. **Compromisos de comunicación con el organismo responsable de la tramitación de reclamaciones de los ciudadanos de la UE que presente la solicitud.**

a. El Defensor del Pueblo en el ámbito del Escudo de la privacidad acusará recibo de la solicitud al organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE que la presente.

b. El Defensor del Pueblo en el ámbito del Escudo de la privacidad llevará a cabo una revisión inicial para verificar que la solicitud está completa de conformidad con la sección 3(b). En caso de que el Defensor del Pueblo en el ámbito del Escudo de la privacidad observe deficiencias o tenga dudas al respecto, intentará abordar y resolver estas dudas con el organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE que la haya presentado.

c. Si para facilitar el correcto tratamiento de la solicitud, el Defensor del Pueblo en el ámbito del Escudo de la privacidad necesita más información sobre la solicitud, o si es necesario que la persona que originalmente presentó la solicitud acometa una acción concreta, el Defensor del Pueblo en el ámbito del Escudo de la privacidad lo comunicará al organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE que haya presentado la solicitud.

d. El Defensor del Pueblo en el ámbito del Escudo de la privacidad hará un seguimiento del estado de las solicitudes y facilitará información actualizada al organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE en cuestión.

e. Una vez completadas las solicitudes según lo descrito en la sección 3 del presente memorando, el Defensor del Pueblo en el ámbito del Escudo de la privacidad proporcionará puntualmente una respuesta adecuada al organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE que las haya presentado, de conformidad con la obligación continua de proteger la información con arreglo a las leyes y políticas aplicables. El Defensor del Pueblo en el ámbito del Escudo de la privacidad ofrecerá una respuesta al organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE en cuestión, confirmando: i) que la reclamación ha sido debidamente investigada; y ii) la observancia de las leyes, estatutos, órdenes ejecutivas, directivas presidenciales y políticas de los organismos estadounidenses, siempre y cuando se hayan respetado las limitaciones y las protecciones descritas en la carta de la ODNI o, en caso de incumplimiento, cuando este incumplimiento haya sido subsanado. El Defensor del Pueblo en el ámbito del Escudo de la privacidad no confirmará ni negará si el individuo ha sido objeto de vigilancia ni tampoco confirmará la reparación concreta aplicada. Tal como se explica con más detalle en la sección 5, las solicitudes relacionadas con la FOIA se tramitarán con arreglo a dicha Ley y a la normativa aplicable.

f. El Defensor del Pueblo en el ámbito del Escudo de la privacidad se comunicará directamente con el organismo responsable de la tramitación de las reclamaciones de los ciudadanos de la UE que las haya presentado, el cual, a su vez, será el responsable de ponerse en contacto con la persona que haya presentado la solicitud. Si las comunicaciones directas forman parte de los procesos subyacentes descritos a continuación, estas comunicaciones se realizarán con arreglo a los procedimientos existentes.

g. Los compromisos establecidos en el presente memorando no se aplicarán a denuncias de carácter general que aleguen que el Escudo de la privacidad UE-EE. UU. es incompatible con los requisitos de protección de datos de la Unión Europea. Dichos compromisos se basan en el entendimiento común por parte de la Comisión Europea y del Gobierno estadounidense de que, teniendo en cuenta el alcance de los compromisos previstos en este mecanismo, podrían surgir limitaciones de recursos, inclusive con relación a solicitudes relacionadas con la Freedom of Information Act (Ley sobre libertad de información-FOIA). En caso de que el cumplimiento de las funciones del Defensor del Escudo exceda las limitaciones de recursos razonables e impida el cumplimiento de estos compromisos, el Gobierno estadounidense debatirá con la Comisión Europea los ajustes necesarios para resolver la situación.

5. **Solicitudes de información.** Las solicitudes de acceso a los registros del Gobierno de los Estados Unidos deberán hacerse y tramitarse de conformidad con la Freedom of Information Act (FOIA).

a. La FOIA ofrece los medios necesarios para que cualquier persona solicite acceso a los registros existentes de los organismos federales, independientemente de la nacionalidad del solicitante. Esta ley está codificada en el USC, título 5, artículo 552. La ley, junto con información adicional sobre la FOIA, se encuentra disponible en www.FOIA.gov y en http://www.justice.gov/oip/foia-resources. Cada organismo tiene un Chief FOIA Officer, y ha proporcionado información en su web pública sobre cómo presentar una solicitud relacionada con la FOIA al organismo. Los organismos cuentan con procedimientos para consultarse entre sí sobre las solicitudes relacionadas con la FOIA que se refieran a registros mantenidos por otro organismo.

b. A título de ejemplo:

i) la Office of the Director of National Intelligence (Oficina del Director de Inteligencia Nacional) (ODNI) ha creado el portal ODNI FOIA para la ODNI: http://www.dni.gov/index.php/about-this-site/foia. Este portal ofrece información sobre la presentación de una solicitud, la comprobación del estado de una solicitud existente y el acceso a la información que ha sido divulgada y publicada por la ODNI con arreglo a la FOIA. El portal ODNI FOIA incluye enlaces a otros sitios web de la FOIA sobre elementos relacionados con los servicios de inteligencia: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites

ii) la Office of Information Policy (Oficina de Política de la Información) del Departamento de Justicia ofrece información exhaustiva sobre la FOIA: http://www.justice.gov/oip. No solo incluye información sobre la presentación de una solicitud relacionada con la FOIA al Departamento de Justicia, sino que también ofrece orientaciones al Gobierno de los Estados Unidos sobre la interpretación y la aplicación de los requisitos de la FOIA.

c. De conformidad con la FOIA, el acceso a los registros públicos está sujeto a determinadas exenciones enumeradas. Estas exenciones incluyen límites en el acceso a información de seguridad nacional clasificada, información personal de terceros e información referente a la investigaciones policiales, y pueden compararse con las limitaciones impuestas por cada Estado miembro de la UE con su propia legislación en materia de acceso a la información. Estas limitaciones se aplican tanto a los estadounidenses como a los ciudadanos de otras nacionalidades.

d. Los litigios sobre la divulgación de información solicitada en virtud de la FOIA podrán ser recurridos por vía administrativa y posteriormente ante un tribunal federal. El tribunal está obligado a determinar *de novo* si la información se denegó debidamente [USC, título 5, artículo 552(a)(4)(B)] y podrá obligar al Gobierno a facilitar el acceso a la misma. En determinados casos, los tribunales han revocado las alegaciones del Gobierno de que la información debe retenerse por ser clasificada. Aunque no se prevén indemnizaciones pecuniarias, los tribunales podrán decidir sobre los honorarios de los abogados.

6. **Solicitudes de medidas suplementarias.** Una solicitud que alegue la vulneración de la ley u otra mala conducta será remitida al organismo del Gobierno de los Estados Unidos pertinente, incluidos los órganos de supervisión, con poder para investigar la correspondiente solicitud y abordar el incumplimiento tal como se describe a continuación.

a. Los inspectores generales son, por ley, independientes; tienen amplios poderes para llevar a cabo investigaciones, auditorías y revisiones de programas, incluidos los de fraude y abuso o violación de la ley; y pueden recomendar acciones correctivas:

i) la Ley sobre el inspector general de 1978, con sus posteriores enmiendas, establece por ley los inspectores generales federales (IG) como unidades independientes y objetivas en la mayoría de los organismos cuyo cometido es combatir el despilfarro, el fraude y el abuso en los programas y operaciones de sus correspondientes organismos. En este sentido, los IG son los responsables de realizar auditorías e investigaciones relacionadas con los programas y las operaciones de su organismo. Asimismo, los IG ofrecen liderazgo y coordinación y recomiendan políticas para las actividades destinadas a promover el ahorro, la eficiencia y la efectividad, y previenen y detectan el fraude y el abuso en los programas y operaciones del organismo,

ii) cada servicio de inteligencia posee su propia Oficina del Inspector General con responsabilidad para la supervisión de las actividades de inteligencia exterior, entre otras cuestiones. Se ha hecho público un determinado número de informes de los inspectores generales sobre los programas de inteligencia,

iii) a título de ejemplo:

— la Oficina del Inspector General de los servicios de inteligencia (IG de los servicios de inteligencia) se estableció en virtud del artículo 405 de la Intelligence Authorization Act of Fiscal Year 2010 (Ley de autorización de los servicios de inteligencia del ejercicio fiscal 2010). El IG de los servicios de inteligencia es responsable de realizar auditorías, investigaciones, inspecciones y revisiones en los servicios de inteligencia que identifiquen y aborden los riesgos sistémicos, las vulnerabilidades y las deficiencias transversales de las misiones de los servicios de inteligencia, a fin de influir positivamente en los ahorros y las eficiencias en el sector de los servicios de inteligencia. El IG de los servicios de inteligencia está autorizado a investigar las denuncias o la información relacionada con las acusaciones de violación de la ley, norma, reglamento, despilfarro, fraude, abuso de autoridad o peligro sustancial o específico para la salud pública y la seguridad con relación a la ODNI y/o a los programas y actividades de inteligencia de los servicios de inteligencia. El IG de los servicios de inteligencia ofrece información sobre cómo contactar directamente con él para presentar un informe: http://www.dni.gov/index.php/about-this-site/contact-the-ig

— la Oficina del Inspector General (OIG) del Departamento de Justicia (DOJ) de los Estados Unidos es, por ley, una entidad independiente cuya misión es detectar e impedir el despilfarro, el fraude, el abuso y la mala conducta en los programas y en el personal del DOJ y promover el ahorro y la eficiencia en estos programas. La OIG investiga las presuntas violaciones de las leyes penales y de los derechos civiles por parte de los empleados del DOJ y audita e inspecciona los programas del DOJ. La OIG tiene jurisdicción sobre todas las denuncias de mala conducta contra los empleados del Departamento de Justicia, incluido el Federal Bureau of Investigation (FBI); la Drug Enforcement Administration; la Federal Bureau of Prisons; el U.S. Marshals Service; el Bureau of Alcohol, Tobacco, Firearms, and Explosives; las United States Attorneys Offices; y los empleados que trabajan en otras secciones u oficinas del Departamento de Justicia. (La única excepción es que las acusaciones de mala conducta de un fiscal del Departamento o del personal de los

servicios con funciones coercitivas, relacionadas con el ejercicio de la autoridad del fiscal del Departamento para investigar, pleitear o proporcionar asesoramiento jurídico, son responsabilidad de la Oficina de Responsabilidad Profesional del Departamento). Asimismo, el artículo 1001 de la Patriot Act (Ley patriótica), promulgada el 26 de octubre de 2001, obliga al inspector general a revisar la información y a recibir las denuncias que aleguen abusos de los derechos civiles y de las libertades civiles por parte de los empleados del Departamento de Justicia. La OIG mantiene una web pública, https://www.oig.justice.gov, que incluye una «línea directa» para la presentación de denuncias: https://www.oig.justice.gov/hotline/index.htm

b. Los organismos y entidades responsables de la protección de la privacidad y de las libertades civiles del Gobierno de los Estados Unidos tienen también importantes responsabilidades. A título de ejemplo:

i) la sección 803 de las Recomendaciones de ejecución de la Ley de la Comisión 9/11 de 2007, codificada en el USC, título 42, artículo 2000-ee1, instituye agentes responsables de la protección de la privacidad y de las libertades civiles en determinados departamentos y organismos (incluido el Departamento de Estado, el Departamento de Justicia y la ODNI). La sección 803 especifica que estos agentes actuarán de asesores principales para, entre otras cosas, garantizar que el departamento, organismo o servicio dispone de los procedimientos adecuados para tratar las denuncias de los individuos que aleguen que dicho departamento, organismo o servicio ha violado su privacidad o sus libertades civiles,

ii) la Oficina de Libertades Civiles y Privacidad de la ODNI (ODNI CLPO, por sus siglas en inglés) está dirigida por el Civil Liberties Protection Officer (agente responsable de la protección de las libertades civiles) de la ODNI, cargo establecido por la Ley de Seguridad Nacional de 1948, y sus enmiendas. El cometido de la ODNI CLPO incluye garantizar que las políticas y procedimientos de los servicios de inteligencia contemplen las protecciones adecuadas para la privacidad y las libertades civiles, y revisar e investigar las denuncias que aleguen abuso o violación de las libertades civiles y de la privacidad en los programas y actividades de la ODNI. La ODNI CPLO ofrece información al público en su web, incluidas las instrucciones para presentar una denuncia: www.dni.gov/clpo. En caso de que la ODNI CLPO reciba una denuncia relacionada con la privacidad o las libertades civiles que implique a los programas y actividades de los servicios de inteligencia, trabajará en coordinación con otros servicios de inteligencia sobre cómo debería tramitarse esta denuncia en los servicios de inteligencia. Cabe señalar que la *National Security Agency* (NSA) (Agencia de Seguridad Nacional) cuenta también con una Civil Liberties and Privacy Office, que proporciona información sobre sus responsabilidades en su sitio web: https://www.nsa.gov/civil_liberties/. Si la información indica que un organismo incumple los requisitos de privacidad (por ejemplo, un requisito contemplado en el artículo 4 de la PPD-28), los organismos poseen mecanismos de cumplimiento para revisar y subsanar el incidente. Los organismos deben informar a la ODNI de los incidentes de incumplimiento con arreglo a la PPD-28,

iii) la Office of Privacy and Civil Liberties (OPCL, Oficina de privacidad y libertades civiles) del Departamento de Justicia respalda los deberes y las responsabilidades del Chief Privacy and Civil Liberties Officer (CPCLO, Director de Privacidad y Libertades Civiles) del Departamento. La misión principal de la OPCL es proteger la privacidad y las libertades civiles de los ciudadanos estadounidenses a través de la revisión, supervisión y coordinación de las operaciones de privacidad del Departamento. La OPCL ofrece asesoramiento y orientación jurídica a los componentes del Departamento; garantiza el respeto de la privacidad por parte del Departamento, incluido el cumplimiento de la Privacy Act (Ley de privacidad) de 1974, las disposiciones de privacidad de la E-Government Act (Ley de administración electrónica) de 2002 y la Federal Information Security Management Act (Ley federal de gestión de la seguridad de la información), así como las directrices de las políticas de la administración promulgadas en apoyo a estas Leyes; desarrolla e imparte formación sobre la privacidad en el Departamento; colabora con la CPCLO en el desarrollo de la política de privacidad del Departamento; elabora informes relacionados con la privacidad para el presidente y el Congreso; y revisa las prácticas de gestión de la información del Departamento para garantizar la coherencia de estas prácticas con la protección de la privacidad y de las libertades civiles. La OPCL proporciona información al público sobre sus responsabilidades en http://www.justice.gov/opcl

iv) de conformidad con el USC, título 42, artículo 2000ee y ss., el Privacy and Civil Liberties Oversight Board (Consejo de Supervisión de la Privacidad y de las Libertades Civiles) deberá revisar continuamente i) las políticas y los procedimientos, así como su implantación, de los departamentos, organismos y servicios del poder ejecutivo relacionados con las iniciativas para proteger a la Nación contra el terrorismo y garantizar la protección de la privacidad y de las libertades civiles; y ii) otras acciones del poder ejecutivo relacionadas con estas iniciativas para determinar si dichas acciones protegen adecuadamente la privacidad y las libertades civiles y se ajustan a la legislación, las normativas y las políticas relacionadas con la privacidad y las libertades civiles. Recibirá y revisará los informes y otra información de los agentes responsables de la protección de la

privacidad y las libertades civiles y, cuando proceda, les hará las recomendaciones pertinentes para sus actividades. La sección 803 de las Recomendaciones de ejecución de la Ley de la Comisión 9/11 de 2007, codificada en el USC, título 42, artículo 2000ee-1, da instrucciones a los agentes responsables de la protección de la privacidad y las libertades civiles de ocho organismos federales (incluida la Secretaría de Defensa, la Secretaría de Seguridad Nacional, el Director de Inteligencia Nacional y el Director de la Agencia Central de Inteligencia), así como de cualquier otro organismo designado por el Consejo, para presentar informes periódicos al PCLOB, que incluyan el número, naturaleza y disposición de las denuncias recibidas por el correspondiente organismo por presuntas infracciones. La ley de habilitación del PCLOB establece que esta entidad recibir estos informes y, cuando proceda, hacer las recomendaciones a los agentes responsables de la protección de la privacidad y las libertades civiles relacionadas con sus actividades.

ANEXO IV

Carta de la Presidenta de la Comisión Federal de Comercio, Edith Ramirez

7 de julio de 2016

Por CORREO ELECTRÓNICO

Věra Jourová
Comisaria de Justicia, Consumidores e Igualdad de Género
Comisión Europea
Rué de la Loi/Wetstraat 200
1049 Bruselas
Bélgica

Estimada Comisaria Jourová:

La Comisión Federal de Comercio («FTC») de los Estados Unidos aprecia la oportunidad para describir su aplicación del nuevo marco del Escudo de la privacidad UE- EE. UU. (el «marco del Escudo de la privacidad» o «marco»). Creemos que el marco desempeñará un papel fundamental a la hora de facilitar la protección de la privacidad de las operaciones comerciales en un mundo cada vez más interconectado. Permitirá a las empresas realizar importantes operaciones en el ámbito de la economía mundial, y al mismo tiempo garantizará la protección de la privacidad de los consumidores de la UE. La FTC apuesta desde hace tiempo por la protección de la privacidad entre fronteras y tiene como objetivo prioritario la aplicación del nuevo marco. A continuación explicamos el historial de estricta aplicación de la protección de la privacidad de la FTC en general, y en particular la aplicación del programa del «puerto seguro», así como la estrategia de la FTC para la aplicación del nuevo marco.

La FTC expresó públicamente por primera vez su compromiso de aplicar el programa del puerto seguro en 2000. En aquel momento, el entonces presidente de la FTC, Robert Pitofsky, envió una carta a la Comisión Europea en la que destacaba el compromiso de la FTC de aplicar firmemente los principios de privacidad del puerto seguro. La FTC ha continuado manteniendo este compromiso a través de casi 40 medidas de ejecución, numerosas investigaciones adicionales y la colaboración con las autoridades europeas de protección de datos personales («APD de la UE») en cuestiones de interés mutuo.

Después de que en noviembre de 2013 la Comisión Europea expresara su preocupación por la gestión y la aplicación del programa del puerto seguro, la FTC y el Departamento de Comercio estadounidense iniciaron una ronda de consultas con los funcionarios de la Comisión Europea para buscar la manera de reforzarlo. El 6 de octubre de 2015, en pleno proceso de consultas, el Tribunal Europeo de Justicia dictó una sentencia en el caso Schrems que, entre otras cosas, invalidó la decisión de la Comisión Europea sobre el carácter adecuado de la protección del programa del puerto seguro. Tras esta sentencia, continuamos trabajando estrechamente con el Departamento de Comercio y la Comisión Europea en un intento de reforzar las protecciones de la privacidad de los particulares de la UE. El marco del Escudo de la privacidad es fruto de estas consultas en curso. Al igual que hizo con el programa del puerto seguro, la FTC se compromete por la presente a aplicar estrictamente el nuevo marco. Esta carta deja constancia de este compromiso.

En concreto, confirmamos nuestro compromiso en cuatro áreas clave: 1) priorización de las remisiones e investigaciones; 2) tratamiento de las declaraciones falsas o fraudulentas de adhesión al Escudo de la privacidad; 3) supervisión continua de las órdenes; y 4) mayor compromiso y colaboración en lo que respecta a la ejecución, con las APD de la UE. A continuación ofrecemos información detallada sobre cada uno de estos compromisos y los antecedentes pertinentes sobre el papel de la FTC en la protección de la privacidad de los consumidores y en la aplicación del puerto seguro, así como el contexto general sobre la privacidad en los Estados Unidos ([1]).

I. ANTECEDENTES

A. **Protección de la privacidad y labor política de la FTC**

La FTC posee amplias competencias en materia de ejecución civil para promover la protección del consumidor y la competencia en el ámbito comercial. Como parte integrante de su mandato de protección del consumidor, la FTC aplica una amplia gama de leyes para proteger la privacidad y la seguridad de la información del consumidor. La ley

([1]) En el anexo A ofrecemos más información sobre las leyes estadounidenses federales y estatales relativas a la protección de la privacidad, y en el anexo B figura un resumen de nuestras últimas medidas coercitivas relacionadas con la privacidad y la seguridad. Este resumen también se encuentra disponible en la web de la FTC: https://www.ftc.gov/reports/privacy-data-security-update-2015

fundamental aplicada por la FTC, la Ley de la FTC, prohíbe actos o prácticas «desleales» y «engañosos» en el comercio o que afecten al comercio ([1]). Una declaración, omisión o práctica es engañosa cuando es importante y es susceptible de inducir a error a los consumidores que actúan razonablemente de acuerdo con las circunstancias ([2]). Un acto o práctica es desleal cuando provoca o es susceptible de provocar daños sustanciales que no puedan ser razonablemente evitados por los consumidores o compensados con unos beneficios equivalentes para los consumidores o la competencia ([3]). La FTC también aplica leyes específicas para la protección de la información relacionada con la salud, los créditos y otras cuestiones financieras, así como de la información sobre menores en Internet, y ha dictado normativas que aplican dichas leyes.

La competencia de la FTC en virtud de la Ley de la FTC se aplica a cuestiones «propias del comercio o que afecten al comercio». La FTC no tiene competencia sobre la aplicación del Derecho penal o sobre cuestiones de seguridad nacional. Tampoco puede involucrarse en la mayoría de las restantes acciones gubernamentales. Además, existen determinadas excepciones a la competencia de la FTC sobre actividades comerciales, en particular relacionadas con los bancos, las compañías aéreas, el sector de seguros y las actividades de los proveedores de servicios de telecomunicaciones. La FTC tampoco tiene competencia sobre la mayoría de las organizaciones sin ánimo de lucro, pero sí la tiene sobre las organizaciones benéficas u otras organizaciones sin ánimo de lucro que en realidad operan con fines de lucro. La FTC también tiene competencia sobre las organizaciones sin ánimo de lucro que operan en beneficio de sus miembros con ánimo de lucro, incluso proporcionando beneficios económicos sustanciales a dichos miembros ([4]). En algunos casos, la competencia de la FTC coincide con la de otros organismos con funciones coercitivas.

Hemos desarrollado unas estrecha relación de trabajo con las autoridades federales y estatales y colaboramos estrechamente con ellos para coordinar las investigaciones o remitirlas, si procede.

La ejecución es el eje central de la estrategia de la FTC para la protección de la privacidad. Hasta la fecha, la FTC ha interpuesto 500 acciones dirigidas a la protección de la privacidad y la seguridad de la información del consumidor, que cubren tanto la información fuera de línea como en línea e incluyen medidas coercitivas contra grandes y pequeñas empresas que, según la FTC, han incumplido su obligación de suprimir correctamente los datos confidenciales de los consumidores, no han garantizado la seguridad de la información personal de los consumidores, han realizado un seguimiento engañoso en línea de los consumidores, han enviado correo basura a los consumidores, han instalado programas espía y maliciosos en los ordenadores de los consumidores, han violado la norma de «no llamar» y otras normas de telemarketing, y han recopilado e intercambiado incorrectamente información de los consumidores en dispositivos móviles. Las medidas coercitivas de la FTC, tanto en el mundo físico como digital, transmiten un mensaje importante a las empresas sobre la necesidad de proteger la privacidad del consumidor.

La FTC ha llevado a cabo también numerosas iniciativas políticas destinadas a favorecer la privacidad del consumidor y que orientan su labor de aplicación de las normas. La FTC ha organizado talleres y ha elaborado informes recomendando las mejores prácticas destinadas a favorecer la privacidad en el ecosistema móvil; aumentar la transparencia del sector de intermediación en el ámbito de los datos; maximizar los beneficios de los macrodatos y, a la vez, atenuar sus riesgos, sobre todo para los consumidores con ingresos bajos y desatendidos; y destacar las implicaciones para la privacidad y la seguridad del reconocimiento facial y el Internet de las Cosas, entre otros ámbitos.

La FTC interviene también en la educación al consumidor y a las empresas para aumentar el impacto de sus iniciativas de aplicación y de desarrollo de políticas. La FTC ha utilizado una amplia variedad de herramientas, publicaciones, recursos en línea, talleres de trabajo y redes sociales, para ofrecer materiales educativos sobre una amplia gama de temas, entre ellos aplicaciones móviles, privacidad infantil y seguridad de los datos. Recientemente, la Comisión lanzó su iniciativa «*Start With Security*» (Comencemos con la seguridad), que incluye una nueva orientación para las empresas basada en las lecciones aprendidas de los casos de seguridad de datos del organismo, así como una serie de talleres en todo el país. Asimismo, la FTC es desde hace mucho tiempo líder en educación de los consumidores sobre seguridad informática básica. El año pasado, nuestro sitio web OnGuard Online y su versión en español, Alerta en Línea, recibieron más de 5 millones de visitas.

B. **Medidas de protección jurídica en los Estados Unidos que benefician a los consumidores de la UE**

El marco operará en el contexto más amplio de las medidas adoptadas en los Estados Unidos, que protegen a los consumidores de la UE de diferentes maneras.

([1]) USC, título 15, artículo 45(a).
([2]) Véase FTC Policy Statement on Deception, adjunto a Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), disponible en: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception
([3]) Véase USC, título 15, artículo 45(n); FTC Policy Statement on Unfairness, adjunto a Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), disponible en: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness
([4]) Véase California Dental Ass'n v. FTC, 526 U.S. 756 (1999).

La prohibición de la Ley de la FTC sobre actos o prácticas desleales o engañosas no se limita a la protección de los consumidores estadounidenses frente a las empresas estadounidenses, ya que incluye aquellas prácticas que: 1) causen o puedan causar daños razonablemente previsibles en los Estados Unidos, o 2) impliquen un comportamiento concreto en los Estados Unidos. Además, la FTC puede utilizar todos los recursos, incluida la restitución, disponibles para la protección de los consumidores nacionales, para la protección de los consumidores extranjeros.

Está claro que la labor de ejecución de la FTC beneficia enormemente tanto a los consumidores estadounidenses como a los de la UE. Por ejemplo, nuestras acciones dirigidas a aplicar la sección 5 de la Ley de la FTC han protegido de igual manera la privacidad de los consumidores estadounidenses y la de los extranjeros. En un caso contra un intermediador de información, Accusearch, la FTC alegó que la venta por parte de la empresa de registros telefónicos confidenciales a terceros sin el conocimiento o el consentimiento de los consumidores era una práctica desleal que infringía la sección 5 de la Ley de la FTCA. Accusearch vendió información relacionada con consumidores estadounidenses y extranjeros ([1]). El tribunal dictó medidas de reparación contra Accusearch prohibiendo, entre otras cosas, la comercialización o venta de la información personal de los consumidores sin el previo consentimiento por escrito, salvo que se hubiera obtenido legalmente de la información públicamente disponible, y exigió el pago de casi 200 000 USD ([2]).

Otro ejemplo es la transacción celebrada por la FTC con TRUSTe. Garantiza que los consumidores, incluidos los de la Unión Europea, puedan confiar en las declaraciones de una organización autorreguladora global sobre su revisión y certificación de servicios en línea nacionales y extranjeros ([3]). Cabe señalar que nuestra acción contra TRUSTe también refuerza más profundamente el sistema autorregulador de la privacidad garantizando la responsabilidad de las entidades que desempeñan un papel importante en los regímenes autorreguladores, incluidos los marcos transfronterizos de protección de la privacidad.

La FTC también garantiza el cumplimiento de otras leyes específicas cuyas protecciones se extienden a los consumidores no estadounidenses, tales como la Children's Online Privacy Protection Act («COPPA», Ley de Protección de la Privacidad Infantil en Internet). Entre otras cosas, la COPPA exige que los operadores de servicios en línea y de páginas web dirigidas a menores, o de páginas web dirigidas al público en general, que recopilen a sabiendas información personal de niños menores de 13 años, lo notifiquen a los padres y obtengan un consentimiento parental verificable. Los sitios web y servicios radicados en EE. UU. que estén sujetos a la COPPA y que recopilen información personal de menores extranjeros, deberán ajustarse a la COPPA. Los sitios web y servicios en línea extranjeros también deberán ajustarse a la COPPA si van dirigidos a menores estadounidenses, o si recopilan a sabiendas información personal de menores estadounidenses. Además de las leyes federales estadounidenses cuya ejecución garantiza la FTC, otras leyes federales y estatales relativas a la protección de los consumidores y la privacidad pueden ofrecer beneficios adicionales a los consumidores de la UE.

C. **Aplicación del puerto seguro**

Como parte de su programa de aplicación de las normas sobre privacidad y seguridad, la FTC busca también proteger a los consumidores de la UE mediante la interposición de acciones relacionadas con vulneraciones del puerto seguro. La FTC ha interpuesto 39 acciones relacionadas con la aplicación del puerto seguro: 36 en las que se alegaban declaraciones falsas de certificación, y tres casos, contra Google, Facebook y Myspace, que alegaban el incumplimiento de los principios de privacidad del puerto seguro ([4]). Estos casos demuestran la posibilidad de hacer cumplir los principios de la certificación, y las consecuencias del incumplimiento. Unos autos de avenencia a veinte años exigen a Google, Facebook y Myspace la implantación de programas de privacidad integrales que deberán estar razonablemente diseñados para abordar los riesgos de privacidad relacionados con el desarrollo y la gestión de productos y servicios nuevos y existentes, y para proteger la privacidad y la confidencialidad de la información personal. Los programas integrales de privacidad estipulados en estos autos deberán identificar los riesgos materiales previsibles y disponer de controles para hacerles frente. Las empresas también deberán someterse a evaluaciones independientes continuas de sus programas de privacidad, que deberán comunicarse a la FTC. Los autos también prohíben a estas empresas hacer falsas declaraciones sobre sus prácticas en materia de protección de la privacidad y su participación en programas protección de la privacidad o la seguridad. Esta prohibición se aplica también a los actos y prácticas de las empresas contemplados en el

([1]) Véase Oficina del Comisario de Privacidad de Canadá, denuncia en virtud de PIPEDA contra Accusearch, Inc., que opera como Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. La Oficina del Comisario de Privacidad de Canadá elaboró un informe amicus curiae en el recurso contra la acción de la FTC y llevó a cabo su propia investigación, que llegó a la conclusión de que las prácticas de Accusearch también incumplían la ley canadiense.

([2]) Véase FTC v. Accusearch, Inc., n.o 06CV015D (D. Wyo. Dec. 20, 2007), aff'd 570 F.3d 1187 (10th Cir. 2009).

([3]) Véase In the Matter of True Ultimate Standards Everywhere, Inc., n.oC-4512 (F.T.C. 12 de marzo de 2015) (decisión y resolución), disponible en https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf

([4]) Véase In the Matter of Google, Inc., n.oC-4336 (F.T.C. 13 de octubre de 2011) (decisión y resolución), disponible en https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; In the Matter of Facebook, Inc., n.oC-4365 (F.T.C. 27 de julio de 2012) (decisión y resolución), disponible en https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; In the Matter of Myspace LLC, n.oC-4369 (F.T.C. 30 de agosto de 2012) (decisión y resolución), disponible en https://www.ftc.gov/news-events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace

nuevo marco del Escudo de la privacidad. La FTC puede ejecutar estos autos reclamando sanciones civiles. De hecho, en 2012 Google pagó una multa civil récord de 22,5 millones USD a raíz de las alegaciones de que había violado el auto correspondiente. Por consiguiente, estos autos de la FTC contribuyen a proteger a más de mil millones de consumidores de todo el mundo, de los cuales cientos de millones residen en Europa.

Las acciones de la FTC se han centrado también en las declaraciones falsas, fraudulentas o engañosas relacionadas con la participación en el puerto seguro. La FTC se toma estas denuncias en serio. Por ejemplo, en FTC vs. Karmani, la FTC interpuso en 2011 una demanda a un comercializador de Internet en los Estados Unidos acusándole de que él y su empresa engañaban a los consumidores británicos haciéndoles creer que la empresa estaba radicada en el Reino Unido, incluso con el uso de extensiones web «.uk» y con referencias a la moneda británica y al sistema postal británico ([1]). No obstante, cuando los consumidores recibían los productos descubrían unos derechos de importación imprevistos, garantías que no eran válidas en el Reino Unido y gastos relacionados con la obtención de reembolsos. La FTC también acusó a los demandados de engañar a los consumidores sobre su participación en el programa del puerto seguro. Cabe señalar que todas las víctimas residían en el Reino Unido.

Muchos otros de nuestros casos de aplicación del puerto seguro implicaban a organizaciones que se adhirieron al programa del puerto seguro pero que no renovaron su certificación anual aunque continuaron presentándose a sí mismas como miembros actuales. Tal como declaramos a continuación, la FTC también se compromete a abordar las declaraciones falsas de participación en el marco del Escudo de la privacidad. Esta actividad estratégica de aplicación complementará a las cada vez más numerosas acciones del Departamento de Comercio destinadas a verificar el cumplimiento de los requisitos del programa para la certificación y la recertificación, su supervisión del cumplimiento efectivo, inclusive mediante el uso de cuestionarios entre los participantes en el marco, y sus crecientes esfuerzos para identificar las declaraciones falsas de pertenencia al marco y el uso indebido de la marca de certificación del marco ([2]).

II. PRIORIZACIÓN DE LOS RECLAMACIONES REMITIDAS E INVESTIGACIONES

Tal como hicimos con el programa del puerto seguro, la FTC se compromete a dar prioridad a las reclamaciones relacionadas con el Escudo de la privacidad remitidas por los Estados miembros de la UE. También daremos prioridad a las reclamaciones remitidas relativas al incumplimiento de las directrices autorreguladoras relacionadas con el marco del Escudo de la privacidad de las organizaciones autorreguladoras en materia de protección de la privacidad y de otros órganos independientes de resolución de litigios.

Para facilitar la presentación de reclamaciones, al amparo del marco, por los Estados miembros de la UE, la FTC está creando un procedimiento estandarizado de remisiones y proporcionando información a los Estados miembros de la UE sobre el tipo de información más útil para la FTC en su investigación de una remisión. Como parte de esta iniciativa, la FTC designará un punto de contacto para las remisiones de los Estados miembro de la UE. Resulta muy útil que la autoridad remitente realice una investigación preliminar de la presunta infracción y colabore con la FTC en la investigación.

Tras la recepción de una remisión procedente de un Estado miembro de la UE o de una organización autorreguladora, la FTC puede adoptar una serie de medidas para abordar las cuestiones planteadas. Por ejemplo, podemos revisar las políticas de privacidad de la empresa, obtener más información directamente de la empresa o de terceros, realizar un seguimiento con la entidad remitente, evaluar si existe un patrón de infracciones o un número significativo de consumidores afectados, determinar si la remisión implica cuestiones que recaen en el ámbito de competencia del Departamento de Comercio, evaluar la utilidad de la educación de consumidores y empresas, y si procede, iniciar un proceso para exigir el cumplimiento.

La FTC también se compromete a intercambiar información sobre las remisiones con las autoridades competentes, incluido el estado de las remisiones, de conformidad con las leyes y restricciones de confidencialidad. En la medida en que sea viable por el número y tipo de remisiones recibidas, la información proporcionada incluirá una evaluación de las cuestiones remitidas, en particular una descripción de las cuestiones importantes planteadas y cualquier medida adoptada para abordar las violaciones de la ley en el ámbito de competencia de la FTC. La FTC ofrecerá también sus comentarios a la autoridad remitente sobre los tipos de remisiones recibidas con el objeto de aumentar la efectividad de

([1]) Véase FTC v. Karnani, n.o 2:09-cv-05276 (C.D. Cal., 20 de mayo de 2011) (resolución definitiva), disponible en: https://www.ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; véase también Lesley Fair, FTC Business Center Blog, Around the World in Shady Ways, https://www.ftc.gov/blog/2011/06/around-world-shady-ways (9 de junio de 2011).

([2]) Carta de Stefan M. Selig, subsecretario de comercio responsable del comercio internacional, administración de comercio internacional, a Věra Jourová, comisaria de Justicia, Consumidores e Igualdad de Género (23 de febrero de 2016).

las iniciativas para hacer frente a las conductas ilícitas. En caso de que una autoridad remitente necesite información sobre el estado de una determinada remisión a efectos de aplicar su propio procedimiento de ejecución, la FTC responderá, teniendo en cuenta el número de remisiones objeto de análisis y de conformidad con los requisitos de confidencialidad y otros requisitos legales.

La FTC también colaborará estrechamente con las APD de la UE para ofrecerles ayuda en la ejecución. En los casos en que proceda, esto podría incluir el intercambio de información y ayuda en la investigación en virtud de la SAFE WEB Act (Ley estadounidense de seguridad en Internet), que autoriza a la FTC a ayudar a los organismos de seguridad extranjeros cuando dichos organismos apliquen leyes que prohíban prácticas sustancialmente parecidas a las prohibidas por las leyes que aplica la FTC ([1]). Como parte de esta ayuda, la FTC podrá compartir la información obtenida relacionada con una investigación de la FTC, dictar medidas obligatorias en nombre de la APD de la UE que lleve a cabo su propia investigación y buscar testimonios orales de los testigos o demandados con relación a los procedimientos de ejecución de la APD, de conformidad con los requisitos de la SAFE WEB Act. La FTC utiliza generalmente esta competencia para ayudar a otras autoridades de todo el mundo en los casos de protección de la privacidad y del consumidor ([2]).

Además de dar prioridad a las remisiones relacionadas con el Escudo de la privacidad procedentes de los Estados miembros de la UE y de las organizaciones autorreguladoras ([3]), la FTC se compromete a investigar por iniciativa propia la posible violación del marco cuando lo considere procedente, utilizando varias herramientas.

Durante más de una década, la FTC ha mantenido un programa consolidado de investigación de las cuestiones de privacidad y seguridad relacionadas con organizaciones comerciales. Como parte de estas investigaciones, la FTC examinó rutinariamente si la entidad en cuestión hacía declaraciones relacionadas con el puerto seguro. En caso de que hiciera estas declaraciones y la investigación revelara presuntas violaciones de los principios de privacidad del puerto seguro, la FTC incluía alegaciones de infracción del puerto seguro en sus acciones de ejecución. Continuaremos aplicando esta estrategia proactiva al amparo del nuevo marco. Y lo que es más importante, la FTC lleva a cabo muchas investigaciones que en último lugar desembocan en medidas de ejecución públicas. Muchas investigaciones de la FTC se cierran porque el personal no identifica una presunta violación de la ley. Dado que las investigaciones de la FTC no son públicas sino confidenciales, generalmente no se hace público el cierre de una investigación.

Las casi 40 acciones de ejecución iniciadas por la FTC con relación al programa del puerto seguro evidencian el compromiso del organismo en la aplicación proactiva de los programas transfronterizos de protección de la privacidad. La FTC buscará posibles violaciones del marco como parte de las investigaciones de privacidad y seguridad que acometemos con regularidad.

III. TRATAMIENTO DE LAS DECLARACIONES FALSAS O ENGAÑOSAS DE ADHESIÓN AL ESCUDO DE LA PRIVACIDAD

Tal como se ha mencionado antes, la FTC adoptará medidas contra las entidades que engañen sobre su participación en el marco. La FTC dará prioridad a la consideración de las remisiones por parte del Departamento de Comercio relacionadas con las organizaciones que identifique que declaran engañosamente su actual pertenencia al marco o que utilicen una marca de certificación del marco sin autorización.

Asimismo, cabe señalar que si la política de privacidad de una organización promete el cumplimiento de los principios del Escudo de la privacidad, el hecho de no registrarse o no mantener su registro en el Departamento de Comercio no eximirá a la organización de la obligación, controlada por la FTC, de cumplir estos compromisos en virtud del marco.

([1]) Para determinar si puede o no ejercer sus competencias en virtud de la SAFE WEB Act, la FTC considera, entre otros: «(A) si el organismo solicitante ha aceptado proporcionar o proporcionará ayuda recíproca a la Comisión; (B) si el cumplimiento de la solicitud perjudicaría los intereses públicos de los Estados Unidos; y (C) si la investigación o el procedimiento de ejecución del organismo solicitante se refiere a actos o prácticas que causen o puedan causar daños a un número significativo de personas». USC, título 15, artículo 46(j)(3). Estas competencias no se aplican a la ejecución de las leyes en materia de competencia.

([2]) En los ejercicios fiscales 2012-2015, por ejemplo, la FTC utilizó sus competencias en virtud de la SAFE WEB Act para compartir información en respuesta a casi 60 solicitudes de organismos extranjeros y emitió casi 60 demandas de investigaciones civiles (equivalentes a citaciones administrativas) para prestar ayuda a 25 investigaciones extranjeras.

([3]) Aunque la FTC no resuelve ni media en las denuncias de consumidores particulares, la FTC confirma que dará prioridad a las remisiones relacionadas con el Escudo de la privacidad procedentes de las APD de la UE. Asimismo, la FTC utiliza las denuncias de su base de datos Consumer Sentinel, a la que pueden acceder otros organismos de seguridad, para identificar las tendencias, determinar las prioridades de aplicación e identificar los posibles objetivos de investigación. Los ciudadanos de la UE pueden utilizar el mismo sistema de denuncia que está disponible para los ciudadanos estadounidenses, para presentar una denuncia ante la FCT: www.ftc.gov/complaint. Para las denuncias de particulares relacionadas con el Escudo de la privacidad, no obstante, sería más práctico que los ciudadanos de la UE presentaran sus denuncias a las APD de su Estado miembro o a un órgano de resolución alternativa de conflictos.

IV. SUPERVISIÓN DE LAS ÓRDENES

La FTC también afirma su compromiso de supervisar las órdenes de ejecución para garantizar el cumplimiento del marco del Escudo de la privacidad.

Exigiremos el cumplimiento del marco a través de diversas medidas cautelares en las futuras órdenes de la FTC relativas a de observancia del marco. Esto incluye la prohibición de realizar declaraciones falsas con relación al marco y a otros programas de privacidad cuando estas declaraciones constituyan la base de la acción subyacente de la FTC.

Los casos de la FTC que exigen el cumplimiento del programa del puerto seguro son ilustrativos. En los 36 casos de declaraciones falsas o engañosas relacionadas con la certificación del puerto seguro, todas las órdenes prohíben al demandado declarar falsamente su participación en el puerto seguro u otro programa de privacidad o seguridad, y exigen a la empresa que presente los informes de cumplimiento a la FTC. En los casos relacionados con las violaciones de los principios de privacidad del puerto seguro, las empresas están obligadas a implantar programas integrales de privacidad y obtener evaluaciones externas independientes de estos programas cada dos años durante veinte años, que deberán presentar a la FTC.

Las violaciones de las órdenes administrativas de la FTC pueden comportar sanciones civiles de hasta 16 000 USD por infracción, o de 16 000 USD por día de infracción continuada ([1]), que en el caso de prácticas que afecten a muchos consumidores, pueden ascender a millones de dólares. Los autos de avenencia incluyen también disposiciones en materia de presentación de informes y de cumplimiento. Las entidades sujetas a un el auto deben conservar los documentos que demuestren su cumplimiento durante un cierto número de años. Los autos también deberán divulgarse entre los empleados responsables de garantizar su cumplimiento.

La FTC supervisa sistemáticamente el cumplimiento de las órdenes del puerto seguro, al igual que lo hace con todas sus órdenes. La FTC se toma en serio la aplicación de sus órdenes de privacidad y seguridad, y cuando es necesario, acomete las acciones pertinentes para exigir su cumplimiento. Por ejemplo, tal como se ha señalado antes, Google pagó una sanción civil de 22,5 millones USD para resolver las acusaciones de que había violado la orden de la FTC. Y lo que es más importante, las órdenes de la FTC continuarán protegiendo a los consumidores de todo el mundo que interactúen con una empresa, no tan solo a los consumidores que hayan presentado denuncias.

Por último, la FTC continuará manteniendo en Internet una lista de empresas sometidas a órdenes obtenidas con relación a la aplicación del programa del puerto seguro y del nuevo marco del Escudo de la privacidad ([2]). Asimismo, los principios del Escudo de la privacidad exigen ahora a las empresas sometidas a una orden de la FTC o a una orden judicial basada en el incumplimiento de los principios, que hagan público cualquier apartado relacionado con el marco del informe de cumplimiento o de evaluación presentado a la FTC, siempre que se ajuste a las leyes y normas en materia de confidencialidad.

V. COMPROMISO CON LAS APD DE LA UE Y COLABORACIÓN EN LA APLICACIÓN

La FTC reconoce el importante papel que desempeñan las APD de la UE con respecto al cumplimiento del marco y alienta un refuerzo de las consultas y una mayor colaboración en la aplicación. Además de las consultas con las APD remitentes sobre cuestiones de casos concretos, la FTC se compromete a participar en reuniones periódicas con los representantes designados del Grupo de Trabajo del Artículo 29 para debatir, en términos generales, cómo mejorar la colaboración en la aplicación del marco. La FTC participará también, junto con los representantes del Departamento de Comercio, de la Comisión Europea y del Grupo de Trabajo Artículo 29, en la revisión anual del marco para debatir su implantación.

La FTC también fomenta el desarrollo de herramientas que mejoren la colaboración en materia de aplicación con las APD de la UE, así como con otras autoridades de aplicación de las normas sobre protección de la privacidad de todo el mundo. Concretamente, la FTC, junto con los socios de aplicación de la Unión Europea y de todo el mundo, lanzó el año pasado un sistema de alerta dentro del ámbito de la Red Global de Vigilancia de la Privacidad («GPEN», por sus siglas en inglés) para compartir información sobre las investigaciones y fomentar la coordinación en materia de aplicación. Esta alerta de la GPEN podría resultar especialmente útil en el contexto del marco del Escudo de la privacidad. La FTC y las APD de la UE podrían utilizarla para coordinarse con respecto al marco y a otras investigaciones de privacidad, en particular como punto de partida para el intercambio de información con el fin de ofrecer una protección coordinada y más efectiva de la privacidad para los consumidores. Continuamos trabajando con las

([1]) USC, título 15, artículo 45(m); C.F.R. título 16, artículo 1.98.
([2]) Véase FTC, Business Center, Legal Resources, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field

autoridades de la UE participantes para implantar la generalización del sistema de alerta de la GPEN y desarrollar otras herramientas para la mejora de la colaboración en materia de aplicación en casos de privacidad, incluidos los relacionados con el marco.

La FTC se complace en ratificar su compromiso para la aplicación del nuevo marco del Escudo de la privacidad. Esperamos continuar colaborando con nuestros colegas de la UE para trabajar juntos en la protección de la privacidad del consumidor en ambos lados del Atlántico.

Atentamente,

Edith Ramirez

Presidenta

Apéndice A

El marco del Escudo de la privacidad UE-EE. UU. en u contexto: visión general del panorama del sistema jurídico americano en materia de protección de la privacidad y la seguridad

Las protecciones previstas por el marco del Escudo de la privacidad UE-EE. UU. (el «marco») existen en el contexto de las protecciones generales de la privacidad que ofrece el sistema jurídico estadounidense en su conjunto. En primer lugar, la Comisión Federal de Comercio de EE. UU. («FTC», por sus siglas en inglés) cuenta con un sólido programa de privacidad y seguridad de los datos para las operaciones comerciales de EE. UU. que protege a los consumidores a escala mundial. En segundo lugar, el contexto relativo a la protección de la privacidad y la seguridad de los consumidores en EE. UU. ha evolucionado considerablemente desde el año 2000, cuando se adoptó el programa original del puerto seguro entre EE. UU. y la UE. Desde entonces, se han promulgado numerosas leyes federales y estatales sobre privacidad y seguridad, y ha aumentado significativamente el número de pleitos públicos y privados destinados a aplicar los derechos de privacidad. El amplio alcance de las protecciones legales estadounidenses para la privacidad y la seguridad de los consumidores que son aplicables a las prácticas comerciales relativas a datos complementa las protecciones previstas para los particulares de la UE en el nuevo marco.

I. PROGRAMA GENERAL DE APLICACIÓN DE LA PRIVACIDAD Y LA SEGURIDAD DE LA FTC

La FTC es la principal agencia de protección del consumidor en EE. UU. especializada en la privacidad del sector comercial. La FTC tiene autoridad para enjuiciar los actos o prácticas desleales y engañosos que violan la privacidad de los consumidores, así como para hacer cumplir leyes de privacidad más específicas que protegen determinados datos financieros y sanitarios, la información sobre los menores de edad y la información utilizada para tomar ciertas decisiones de idoneidad sobre los consumidores.

La FTC tiene una amplia experiencia en la aplicación de las leyes de privacidad de los consumidores. Las acciones coercitivas de la FTC se han ocupado de prácticas ilegales tanto en contextos fuera de línea como en línea. Por ejemplo, la FTC ha tomado medidas coercitivas contra empresas muy conocidas, como Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC y Snapchat, así como contra empresas menos conocidas. La FTC ha denunciado a empresas que, presuntamente, enviaban correo basura a consumidores, instalaban programas espía en ordenadores, no ofrecían seguridad para los datos personales de los consumidores, realizaban fraudulentamente un seguimiento en línea de los consumidores, violaban la privacidad de los menores de edad, recopilaban ilegalmente información de los dispositivos móviles de los consumidores y no ofrecían seguridad a los dispositivos conectados a Internet utilizados para almacenar información personal. Los autos dictados contra estas empresas han dado lugar en general a un control continuo por parte de la FTC durante un período de veinte años, han prohibido nuevos incumplimientos de las leyes y han impuesto importantes sanciones financieras a las empresas por el incumplimiento de los autos ([1]). Cabe destacar que los autos de la FTC no solo protegen a las personas que hayan denunciado un problema; también protegen a todos los consumidores que tengan relación con las empresas en el futuro. En el contexto transfronterizo, la FTC tiene competencia para proteger a los consumidores de todo el mundo contra prácticas que se lleven a cabo en EE. UU ([2]).

Hasta la fecha, la FTC ha iniciado más de 130 acciones en casos de correo basura y programas espía, más de 120 casos de llamadas de marketing telefónico no deseado, más de 100 acciones relativas a la *Fair Credit Reporting Act* (Ley sobre imparcialidad de los informes de solvencia), casi 60 acciones sobre seguridad de los datos, más de 50 acciones generales sobre privacidad, casi 30 acciones por incumplimiento de la Ley Gramm-Leach-Bliley, y más de 20 acciones de aplicación de la Ley de Protección de la Privacidad Infantil en Internet («COPPA») ([3]). Además de estos casos, la FTC también ha emitido y publicado cartas de advertencia ([4]).

([1]) Cualquier entidad que no cumpla una orden de la FTC está sujeta a una sanción civil de hasta 16 000 USD por incumplimiento o 16 000 USD por día en el caso de incumplimiento continuado. Véase USC, título 15, artículo 45(l); C.F.R. título 16, artículo 1.98(c).

([2]) El Congreso ha confirmado explícitamente la competencia de la FTC para presentar recursos jurídicos, incluyendo la restitución, por cualquier acto o práctica que implique comercio internacional y que: 1) cause o pueda causar daños razonablemente previsibles en los Estados Unidos; o 2) impliquen un comportamiento concreto en los Estados Unidos. Véase USC, título 15, artículo 45(a)(4).

([3]) En algunas ocasiones, los casos de la Comisión relativos a la seguridad de los datos y a la privacidad alegan que una empresa ha realizado tanto prácticas engañosas como prácticas desleales; a veces, estos casos también conllevan presuntos incumplimientos de varias normativas, como la Ley sobre imparcialidad de los informes de solvencia, la Ley Gramm-Leach-Bliley y la COPPA.

([4]) Véase, por ejemplo, la nota de prensa de la Comisión Federal de Comercio «FTC Warns Children's App Maker BabyBus About Potential COPPA Violations» (22 de diciembre de 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; Nota de prensa de la Comisión Federal de Comercio «FTC Warns Data Broker Operations of Possible Privacy Violations» (7 de mayo de 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; Nota de prensa de la Comisión Federal de Comercio «FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act» (3 de abril de 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may

En el marco de su experiencia de aplicación estricta de la legislación sobre privacidad, la FTC también ha intentado detectar regularmente posibles incumplimientos del programa del puerto seguro. Desde que se adoptó el programa del puerto seguro, la FTC ha realizado numerosas investigaciones sobre el cumplimiento del puerto seguro por iniciativa propia y ha emprendido 39 acciones contra empresas estadounidenses por incumplimientos al respecto. La FTC mantendrá esta estrategia proactiva priorizando la aplicación del nuevo marco.

II. PROTECCIONES FEDERAL Y ESTATAL DE LA PRIVACIDAD DE LOS CONSUMIDORES

El «Informe sobre la aplicación del puerto seguro», que figura como un anexo a la decisión de adecuación de la Comisión Europea, proporciona un resumen de muchas de las leyes de privacidad federales y estatales vigentes en el momento de la adopción del programa del puerto seguro, en el año 2000 ([1]). En ese momento, numerosas leyes federales regulaban la recopilación y el uso comercial de información personal, más allá del artículo 5 de la *FTC Act* (Ley de la FTC), incluyendo las siguientes: Cable Communications Policy Act (Ley de política de comunicaciones por cable), Driver's Privacy Protection Act (Ley de protección de la privacidad del conductor), Electronic Communications Privacy Act (Ley de privacidad de las comunicaciones electrónicas), Electronic Funds Transfer Act (Ley de transferencia electrónica de fondos), Fair Credit Reporting Act (Ley sobre imparcialidad de los informes de solvencia), Gramm-Leach-Bliley Act (Ley Gramm-Leach-Bliley), Right to Financial Privacy Act (Ley del derecho a la privacidad financiera), Telephone Consumer Protection Act (Ley de protección del consumidor de telefonía) y Video Privacy Protection Act (Ley de protección de la privacidad de vídeo). Muchos Estados también contaban con leyes análogas en estos ámbitos.

Desde 2000, se han producido numerosos avances, tanto a nivel federal como a nivel estatal, que establecen protecciones adicionales para la privacidad de los consumidores ([2]). A nivel federal, por ejemplo, la FTC modificó el Reglamento COPPA en 2013 para introducir varias protecciones adicionales a la información personal de los menores de edad. Asimismo, la FTC emitió dos normas de aplicación de la Ley Gramm-Leach-Bliley —la Regla de privacidad y la Regla de salvaguardias— que exigen que las instituciones financieras ([3]) efectúen revelaciones sobre sus prácticas de intercambio de información y apliquen un programa integral de seguridad de la información para proteger los datos de los consumidores ([4]). Asimismo, la Fair and Accurate Credit Transactions Act («FACTA») (Ley de Transacciones de Crédito Justas y Exactas), promulgada en 2003, complementa a las antiguas leyes estadounidenses sobre el crédito estableciendo requisitos para el enmascaramiento, el intercambio y la eliminación de determinados datos financieros confidenciales. La FTC ha promulgado varias normas con arreglo a la FACTA relativas, entre otras cosas, al derecho de los consumidores a un informe de crédito anual gratuito; los requisitos de eliminación segura de los datos de informe de los consumidores; el derecho de los consumidores a anular la recepción de determinadas ofertas de crédito y seguros; el derecho de los consumidores a cancelar el uso de información proporcionada por una empresa filial para comercializar sus productos y servicios; y requisitos para las instituciones financieras y los acreedores para que apliquen programas de detección y prevención del robo de identidad ([5]). Además, las normas promulgadas en virtud de la Ley de Transferibilidad y Responsabilidad del Seguro Sanitario se revisaron en 2013 añadiendo medidas adicionales para proteger la privacidad y la seguridad de la información personal sobre salud ([6]). También han entrado en vigor normas que protegen a los consumidores contra llamadas de marketing telefónico no deseadas, llamadas telefónicas automáticas y recepción de correo basura. El Congreso también ha promulgado leyes que exigen a ciertas empresas que recopilan información de salud que envíen a los consumidores una notificación en caso de incumplimiento ([7]).

Asimismo, los Estados han sido muy activos en la aprobación de leyes relacionadas con la privacidad y la seguridad. Desde 2000, cuarenta y siete estados, el Distrito de Columbia, Guam, Puerto Rico y las Islas Vírgenes han promulgado

([1]) Véase Departamento de Comercio de EE. UU., «Informe sobre la aplicación del puerto seguro», https://build.export.gov/main/safeharbor/eu/eg_main_018476

([2]) Para obtener un resumen más completo de las protecciones legales en EE.. UU., véase Daniel J. Solove y Paul Schwartz, Information Privacy Law (5.ª ed., 2015).

([3]) Las instituciones financieras se definen de manera muy amplia en la Ley Gramm-Leach-Bliley a fin de que queden incluidas todas las empresas que «se dedican de un modo significativo» a la provisión de productos o servicios financieros. Esto incluye, por ejemplo, los servicios de cobro de cheques, los prestamistas, los agentes hipotecarios, los prestamistas no bancarios, los tasadores de bienes muebles o inmuebles y los especialistas en impuestos.

([4]) En virtud de la Ley de Protección Financiera del Consumidor de 2010 («CFPA»), título X de Pub. L. 111-203, 124 Stat. 1955 (21 de julio de 2010) (también conocida como «Ley Dodd-Frank de Protección del Consumidor y Reforma de Wall Street»), la mayor parte de las competencias normativas de la FTC respecto a la Ley Gramm-Leach-Bliley se han transferido a la Oficina de Protección Financiera del Consumidor («CFPB»). La FTC conserva competencia de ejecución en virtud de la Ley Gramm-Leach-Bliley, así como competencia normativa para la Regla de Salvaguardias y competencia normativa limitada en virtud de la Regla de Privacidad con respecto a los concesionarios de automóviles.

([5]) En virtud de la CFPA, la Comisión comparte con la CFPB su función de aplicación de la FCRA, pero la competencia normativa se ha transferido en gran parte a la CFPB (excepto la Regla de las alertas rojas y la Regla de eliminación).

([6]) Véase 45 C.F.R., puntos 160, 162 y 164.

([7]) Véase, por ejemplo, la Ley Americana de Recuperación y Reinversión de 2009, Pub. L. n.º 111-5, 123 Stat. 115 (2009) y las normativas pertinentes, 45 C.F.R. §§ 164.404-164.414; 16 C.F.R., punto 318.

leyes que exigen a las empresas que notifiquen a los particulares los incumplimientos de la seguridad de la información personal ([1]). Al menos treinta y dos estados y Puerto Rico cuentan con leyes de eliminación de datos que establecen los requisitos para la destrucción o eliminación de información personal. Varios Estados también han promulgado leyes generales de seguridad de los datos. Además, California ha promulgado varias leyes de privacidad, incluyendo una ley que obliga a las empresas a tener políticas de privacidad y a revelar sus prácticas de no seguimiento ([2]), una ley «Shine the Light» que exige mayor transparencia a los agentes de datos ([3]) y una ley que obliga a ofrecer un «botón de eliminación» que permita a los menores de edad solicitar la eliminación de determinados datos de las redes sociales ([4]). A través de estas leyes y otras competencias, los gobiernos federales y estatales han impuesto cuantiosas sanciones contra empresas que no han protegido la privacidad y la seguridad de la información personal de los consumidores ([5]).

Asimismo, algunas demandas privadas se han resuelto con sentencias y acuerdos exitosos que proporcionan a los consumidores una mayor privacidad y protección de la seguridad de los datos. Por ejemplo, en 2015, Target acordó pagar 10 millones USD en el marco de un acuerdo con consumidores que denunciaron que sus datos financieros personales se vieron comprometidos por un amplio acceso ilegal a los datos. En 2013, AOL aceptó pagar 5 millones USD para resolver una demanda colectiva por una presunta anonimización inadecuada relacionada con la publicación de consultas de búsqueda de cientos de miles de miembros de AOL. Además, un tribunal federal aprobó un pago de 9 millones USD por parte de Netflix por mantener presuntamente registros de historial de alquiler incumpliendo la Ley de Protección de la Privacidad de Vídeo de 1988. Los tribunales federales de California aprobaron dos acuerdos separados con Facebook, uno de 20 millones USD y otro de 9,5 millones USD, en relación con la recopilación, el uso y el intercambio por parte de la empresa de información personal de sus usuarios. En 2008, un tribunal del Estado de California aprobó un acuerdo de 20 millones USD con LensCrafters por la divulgación ilegal de información médica de los consumidores.

En suma, tal como ilustra este resumen, EE. UU. ofrece un importante nivel de protección legal de la privacidad y la seguridad de los consumidores. El nuevo marco del Escudo de la privacidad, que garantiza protecciones significativas para los particulares de la UE, operará en este contexto más amplio en el que la protección de la privacidad y la seguridad de los consumidores sigue siendo una prioridad importante.

([1]) Véase, por ejemplo: National Conference of State Legislatures («NCSL»), State Security Breach Notification Laws (4 de junio de 2016), disponible en http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

([2]) Código Comercial y Profesional de California, §§ 22575-22579.

([3]) Código Civil de California, §§ 1798.80-1798.84.

([4]) Código Comercial y Profesional de California, § 22580-22582.

([5]) Véase Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17 de febrero de 2014), disponible en: http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1

ANEXO V

Carta del Secretario de Transporte estadounidense, Anthony Foxx

19 de febrero de 2016

Comisaria Vera Jourová
Comisión Europea
Rue de la Loi/Wetstraat 200
l 049 Bruselas
Bélgica

Ref.: Marco del Escudo de la UE-EE. UU.

Estimada Comisaria Jourová:

El Departamento de Transportes de EE. UU. («Departamento») agradece la posibilidad de describir su función en la aplicación del marco del Escudo de la privacidad UE-EE. UU. Este marco desempeña un papel fundamental en la protección de los datos personales proporcionados durante las operaciones comerciales en un mundo cada vez más interconectado. Permite a las empresas realizar importantes operaciones en el ámbito de la economía mundial, y al mismo tiempo garantiza la protección de la privacidad de los consumidores de la UE.

El Departamento expresó públicamente por primera vez su compromiso de aplicar el marco del puerto seguro en una carta enviada a la Comisión Europea hace ya 15 años. El Departamento se comprometió en esta carta a aplicar estrictamente los principios de privacidad del puerto seguro. El Departamento continúa manteniendo este compromiso y su carta da constancia de este compromiso.

En particular, el Departamento renueva su compromiso en las siguientes áreas clave: 1) priorización de la investigación de las presuntas violaciones del Escudo de la privacidad; 2) medidas coercitivas adecuadas contra entidades que realicen declaraciones falsas o engañosas de adhesión al Escudo de la privacidad; y 3) supervisión y adopción de órdenes de ejecución relacionadas con infracciones en el marco del Escudo de la privacidad. Ofrecemos información sobre cada uno de estos compromisos y, a efectos del contexto necesario, los antecedentes pertinentes sobre el papel del Departamento en la protección de la privacidad y la aplicación del marco del Escudo de la privacidad.

I. ANTECEDENTES

A. **Competencia del Departamento en materia de privacidad**

El Departamento declara su compromiso inquebrantable para garantizar la privacidad de la información proporcionada por los consumidores a las líneas aéreas y a los agentes de venta de billetes. La competencia del Departamento para acometer acciones en esta área se contempla en el USC, título 49, artículo 41712, que prohíbe que un transportista o un agente de venta de billetes adopte una práctica «desleal o engañosa o un método desleal de competencia» en la venta de transporte aéreo que desemboque o pueda desembocar en daños para el consumidor. El artículo 41712 sigue el modelo del artículo 5 de la Ley de la Comisión Federal de Comercio (FTC) (USC, título 15, artículo 45). Interpretamos que nuestra ley de prácticas desleales o engañosas prohíbe que una compañía aérea o un agente de venta de billetes: 1) infrinja los términos de su política de privacidad; o 2) recopile o revele información privada de una manera que incumpla la política pública, sea inmoral o provoque daños importantes al consumidor no compensados por unos beneficios equivalentes. También interpretamos el artículo 41712 en el sentido de que prohíbe que los transportistas y los agentes de venta de billetes: 1) infrinjan una norma dictada por el Departamento que identifica determinadas prácticas de privacidad como desleales o engañosas; o 2) infrinjan la Ley de Protección Infantil en Internet (COPPA) o las normas de la FTC que implanten la COPPA. De conformidad con las leyes federales, el Departamento posee la competencia exclusiva de regular las prácticas de privacidad de las compañías aéreas, y comparte jurisdicción con la FTC con respecto a las prácticas de privacidad de los agentes de venta de billetes en la venta de transporte aéreo.

Por ello, cuando un transportista o un vendedor de trasporte aéreo se compromete públicamente a adoptar los principios de privacidad del marco del Escudo de la privacidad, el Departamento podrá utilizar las competencias estatutarias del artículo 41712 para garantizar el cumplimiento de estos principios. Por consiguiente, cuando un pasajero proporciona información a un transportista o a un agente de venta de billetes que se ha comprometido en la adopción de los principios de privacidad del marco del Escudo de la privacidad, el incumplimiento por parte del transportista o del agente de venta de billetes constituirá una violación del artículo 41712.

B. **Prácticas de aplicación de la normativa**

La Office of Aviation Enforcement and Proceedings (Oficina de Observancia y Procedimientos de la Aviación) investiga y enjuicia los casos contemplados en el USC, título 49, artículo 41712. Aplica la prohibición legal contemplada en el artículo 41712 contra las prácticas desleales y engañosas principalmente a través de la negociación con la preparación de órdenes de cese y suspensión, y redacta órdenes que valoran sanciones civiles. La oficina conoce las posibles infracciones principalmente por las reclamaciones que recibe de individuos, agencias de viajes, compañías aéreas y organismos públicos estadounidenses y extranjeros. Los consumidores podrán utilizar la web del Departamento para presentar denuncias de privacidad contra compañías aéreas y agentes de venta de billetes ([1]).

En caso de no alcanzar un acuerdo razonable y adecuado, la Oficina de Observancia de la Aviación posee competencia para entablar un procedimiento de aplicación que implique una audiencia de pruebas ante un juez administrativo del Departamento. El juez tiene potestad para dictar órdenes de cese y suspensión y sanciones civiles. Las violaciones del artículo 41712 pueden desembocar en la expedición de órdenes de cese y suspensión y la imposición de sanciones civiles de hasta 27 500 USD por cada violación del artículo 41712.

El Departamento no tiene competencia para indemnizar por daños y perjuicios ni para ofrecer una reparación monetaria a los demandantes en particular. No obstante, el Departamento tiene competencia para aprobar los acuerdos que resulten de las investigaciones llevadas a cabo por la Oficina de Observancia de la Aviación que beneficien directamente a los consumidores (por ejemplo, dinero en efectivo, bonos) como compensación a las sanciones monetarias que deberían pagar al Gobierno estadounidense. Esto ha sucedido en el pasado y podría también suceder en el contexto de los principios del marco del Escudo de la privacidad cuando las circunstancias lo exijan. Las repetidas violaciones del artículo 41712 por parte de una compañía aérea podrían plantear cuestiones relacionadas con la buena voluntad de la compañía para cumplir su compromiso, lo que en situaciones graves podría comportar la imposibilidad de una compañía aérea para operar, y por consiguiente, la pérdida de su licencia de explotación.

Hasta la fecha, el Departamento ha recibido pocas denuncias de presuntas violaciones de la privacidad por parte de agentes de venta de billetes o compañías aéreas. Cuando surjan serán investigadas de conformidad con los principios antes establecidos.

C. **Medidas de protección jurídica del Departamento que benefician a los consumidores de la UE**

De conformidad con el artículo 41712, la prohibición de prácticas desleales o engañosas en el transporte aéreo o en la venta de transporte aéreo se aplica a compañías aéreas y agentes de venta de billetes estadounidense y extranjeros. El Departamento adopta con frecuencia medidas en contra de compañías aéreas estadounidenses y extranjeras por las prácticas que afectan tanto a consumidores estadounidenses como extranjeros en función de que las prácticas de la compañía aérea tengan lugar en el transcurso del transporte con destino a los Estados Unidos o procedente de los Estados Unidos. El Departamento utiliza y continuará utilizando todos los recursos disponibles para proteger a los consumidores estadounidenses y extranjeros de las prácticas desleales o engañosas en el transporte aéreo por parte de las entidades reguladas.

El Departamento también aplica, con respecto a las compañías aéreas, otras leyes específicas cuyas protecciones se extienden a los consumidores no estadounidenses, como la Ley COPPA. Entre otras cosas, la COPPA exige que los operadores de páginas web y de servicios en línea dirigidos a menores, o de páginas web para el público en general que recopilen a sabiendas información personal de niños menores de 13 años, lo notifiquen a los padres y obtengan un consentimiento parental verificable. Las páginas web y los servicios radicados en EE. UU. que estén sujetos a la COPPA y recopilen información personal de menores extranjeros, deberán hacerlo de conformidad con la Ley COPPA. Las páginas web y los servicios en línea radicados en el extranjero deberán también hacerlo de conformidad con la Ley COPPA si van dirigidos a menores estadounidenses, o si recopilan a sabiendas información personal de menores estadounidenses. En la medida en que las compañías aéreas o extranjeras que operen en los Estados Unidos violen la Ly COPPA, la Departamento tendrá competencia para adoptar medidas coercitivas.

II. APLICACIÓN DEL ESCUDO DE LA PRIVACIDAD

En caso de que una compañía aérea o un agente de venta de billetes decida participar en el marco del Escudo de la privacidad y el Departamento reciba una denuncia de que dicha compañía aérea o agente de venta de billetes ha infringido presuntamente el marco, el Departamento adoptará las medidas necesarias para la estricta aplicación del marco.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints

A. **Priorización de la investigación de presuntas infracciones**

La Oficina de Observancia de la Aviación del Departamento investigará todas y cada una de las denuncias de presuntas infracciones del Escudo de la privacidad (incluidas las denuncias recibidas de las Autoridades de Protección de Datos de la UE) y adoptará la medida coercitiva pertinente cuando existan pruebas de una infracción. Asimismo, la Oficina de Observancia de la Aviación colaborará con la FTC y el Departamento de Comercio y dará prioridad a la consideración de las acusaciones de incumplimiento de los compromisos de privacidad establecidos en el marco del Escudo de la privacidad por parte de las entidades reguladas.

Tras la recepción de una acusación de infracción del marco del Escudo de la privacidad, la Oficina de Observancia de la Aviación del Departamento podrá acometer una serie de medidas como parte de su investigación. Por ejemplo, podrá revisar las políticas de privacidad del agente de venta de billetes o de las compañías aéreas, obtener más información del agente de venta de billetes, de la compañía aérea o de terceros, y valorar si existe un patrón de infracciones o un número considerable de consumidores afectados. Además, podrá determinar si el problema implica cuestiones que recaen dentro del ámbito del Departamento de Comercio o de la FTC, valorar la utilidad de educación de los consumidores o de las empresas, y si procede, entablar un procedimiento de ejecución.

En caso de que el Departamento tenga conocimiento de infracciones del Escudo de la privacidad por parte de agentes de venta de billetes, se coordinará con la FTC. También asesoraremos a la FTC y al Departamento de Comercio sobre los resultados de una acción de aplicación del Escudo de la privacidad.

B. **Tratamiento de las declaraciones falsas o engañosas de adhesión**

El Departamento mantiene su compromiso en la investigación de las infracciones del Escudo de la privacidad, incluidas las declaraciones falsa o engañosa de adhesión al programa del Escudo de la privacidad. Daremos prioridad a la consideración de las remisiones por parte del Departamento de Comercio relacionadas con las organizaciones que declaren engañosamente su actual pertenencia al Escudo de la privacidad o que utilicen una marca de certificación del marco del Escudo de la privacidad sin autorización.

Asimismo, cabe señalar que si la política de privacidad de una organización promete el cumplimiento de los principios del Escudo de la privacidad, el hecho de no registrarse o no mantener su registro en el Departamento de Comercio no eximirá a la organización de la obligación, controlada por el Departamento de Transporte, de cumplir estos compromisos en virtud del marco.

C. **Supervisión y publicación de las órdenes de aplicación relacionadas con infracciones del Escudo de la privacidad**

La Oficina de Observancia de la Aviación del Departamento también mantiene su compromiso para la supervisión de las órdenes de aplicación necesarias para garantizar el cumplimiento del programa del Escudo de la privacidad. Concretamente, en caso de que la Oficina expida una orden dirigida a una compañía aérea o a un agente de venta de billetes de cese y suspensión de futuras infracciones del Escudo de la privacidad y del artículo 41712, supervisará el cumplimiento de la entidad con la disposición de cese y suspensión en la orden. De igual modo, la Oficina garantizará la publicación de las órdenes que se deriven de los casos relacionados con el Escudo de la privacidad en su página web.

Esperamos seguir trabajando con nuestros socios federales y las partes interesadas de la UE sobre cuestiones relacionadas con el Escudo de la privacidad.

Espero que esta información le sea útil. Si desea preguntarme algo o necesita más información, no dude en dirigirse a mí.

Atentamente,

Anthony R. Foxx

Secretario de Transporte

ANEXO VI

Carta del Asesor General, Robert Litt
Oficina del Director de Inteligencia Nacional

22 de febrero de 2016

D. Justin S. Antonipillai
Consejero
Departamento de Comercio de los Estados Unidos
1401 Constitution Ave., NW
Washington, DC 20230

D. Ted Dean
Subsecretario
Administración del Comercio Internacional
1401 Constitution Ave., NW
Washington, DC 20230

Estimados Sr. Antonipillai y Sr. Dean:

Durante los últimos dos años y medio, en el contexto de las negociaciones para el Escudo de la privacidad UE-EE. UU., los Estados Unidos han proporcionado información sustancial sobre el funcionamiento de la actividad de recopilación de la inteligencia de señales de los servicios de inteligencia estadounidenses. Esta incluye información sobre el marco legal vigente, la supervisión a varios niveles de estas actividades, la gran transparencia sobre estas actividades, y las protecciones generalizadas de la privacidad y las libertades civiles para colaborar con la Comisión Europea en la determinación del carácter adecuado de estas protecciones en la medida en que estén relacionadas con la excepción de la seguridad nacional a los principios del Escudo de la privacidad. Este documento resume la información que ha sido proporcionada.

I. PPD-28 Y EL PROCEDER DE LA ACTIVIDAD DE LA INTELIGENCIA DE SEÑALES ESTADOUNIDENSE

Los servicios de inteligencia estadounidense recopilan inteligencia extranjera de una manera cuidadosamente controlada, ajustándose estrictamente a las leyes estadounidenses y sujeta a múltiples niveles de supervisión que se centra en las importantes prioridades de la inteligencia exterior y de la seguridad nacional. La recopilación de la inteligencia de señales por EE. UU. está regida por numerosas leyes y políticas, incluyendo la Constitución estadounidense, la Foreign Intelligence Surveillance Act (FISA, Ley de Vigilancia de la Inteligencia Exterior) (USC, título 50, artículo 1801 *et seq*.), la Orden Ejecutiva 12333 y sus procedimientos de implantación, la Directiva Presidencial y numerosos procedimientos y directrices, aprobados por el Tribunal de la FISA y el Fiscal General, que establece nuevas normas que limitan la recopilación, conservación, uso y divulgación de la información de la inteligencia exterior ([1]).

a. **Aspectos generales de la PPD-28**

En enero de 2014, el presidente Obama pronunció un discurso en el que subrayó diversas reformas en las actividades de inteligencia de señales de EE. UU. y promulgó la Directiva Presidencial 28 (PPD-28), relativa a estas actividades ([2]). El presidente hizo hincapié en que las actividades de inteligencia de señales no solo permiten garantizar la de nuestro país y nuestras libertades sino también la seguridad y las libertades de otros países, incluidos los Estados miembros de la UE, que confían en la información de las agencias de inteligencia estadounidenses para garantizar la protección de sus propios ciudadanos.

La PPD-28 establece una serie de principios y requisitos que se aplican a todas las actividades de inteligencia de señales de EE. UU. y a todas las personas, independientemente de su nacionalidad o ubicación. Concretamente establece determinados requisitos para los procedimientos de abordaje de la recopilación, conservación y divulgación de la información personal sobre personas no estadounidenses obtenida en virtud de la inteligencia de señales estadounidenses. Estos requisitos se describen con más detalle a continuación, pero en resumen:

— la PPD reitera la recopilación de inteligencia de señales por parte de los Estados Unidos únicamente si está autorizada por ley, por una orden ejecutiva u otra directiva presidencial,

([1]) Más información sobre las actividades de inteligencia exterior estadounidenses puede consultarse en Internet y es accesible al público a través de IC on the Record (www.icontherecord.tumblr.com), la página web pública de la ODNI dedicada a promover una mayor visibilidad pública en las actividades de inteligencia del Gobierno.
([2]) Disponible en https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

— la PPD establece procedimientos para garantizar que la actividad de inteligencia de señales solo se realice para propósitos legítimos y de seguridad nacional,

— la PPD exige también que la privacidad y las libertades civiles sean cuestiones fundamentales en la planificación de las actividades de recopilación de inteligencia de señales. Concretamente, los Estados Unidos no recopilan inteligencia para acallar o lastrar críticas o disidencias; para perjudicar a personas en función de su etnia, raza, género, orientación sexual o religión; o para ofrecer una ventaja comercial competitiva a las empresas estadounidenses y los sectores empresariales estadounidenses,

— la PPD establece que la recopilación de inteligencia de señales deberá ser lo más adaptada posible y que la inteligencia de señales recogida indiscriminadamente solo se utilice para determinados propósitos tasados,

— la PPD establece que los servicios de inteligencia deberán adoptar procedimientos «razonablemente diseñados para minimizar la divulgación y conservación de información personal obtenida de actividades de inteligencia de señales», y en particular ampliar determinadas protecciones ofrecidas a la información personal de los ciudadanos estadounidenses a la información de ciudadanos no estadounidenses,

— se han adoptado y se han hecho públicos los procedimientos del organismo que implantan la PPD-28.

La aplicabilidad de los procedimientos y de las protecciones establecidas en este documento al Escudo de la privacidad es evidente. Cuando se transfieren datos a empresas de los Estados Unidos en virtud del Escudo de la privacidad, o por cualquier otro medio, los servicios de inteligencia estadounidenses únicamente pueden pedir estos datos a estas empresas si la solicitud observa la FISA o se realiza de conformidad con una de las disposiciones estatutarias de la Carta de Seguridad Nacional, que se examinan a continuación ([1]). Además, sin confirmar ni negar los informes de medios que acusan a los servicios de inteligencia de recopilar datos de los cables transatlánticos mientras son transmitidos a los Estados Unidos, en caso de que los servicios de inteligencia estadounidense recopilaran datos de los cables transatlánticos lo deberían hacer de conformidad con las limitaciones y las protecciones establecidas en este documento, incluidos los requisitos de la PPD-28.

b. **Limitaciones de la recopilación**

La PPD-28 establece diversos principios generales importantes que rigen la recopilación de inteligencia de señales:

— la recopilación de inteligencia de señales debe ser autorizada por ley o por una autorización presidencial, y debe llevarse a cabo de conformidad con la Constitución y la legislación,

— la privacidad y las libertades civiles deben ser consideraciones fundamentales para la planificación de las actividades de inteligencia de señales,

— la inteligencia de señales solo será recopilada cuando haya un propósito de inteligencia exterior o de contrainteligencia válido,

— los Estados Unidos no recopilarán inteligencia de señales con el fin de acallar o lastrar críticas o disidencias,

— los Estados Unidos no recopilarán inteligencia de señales para perjudicar a las personas en función de su etnia, raza, género, orientación sexual o religión,

— los Estados Unidos no recopilarán inteligencia de señales para ofrecer ventajas comerciales competitivas a empresas y sectores empresariales estadounidenses,

— la actividad de inteligencia de señales estadounidense deberá ser siempre tan adaptada como sea posible, teniendo en cuenta la disponibilidad de otras fuentes de información. Esto significa, entre otras cosas, que cuando es factible, las actividades de recopilación de inteligencia de señales se realizan de una manera selectiva y no indiscriminada.

El requisito de que la actividad de la inteligencia de señales sea «tan adaptada como sea factible» se aplica a la manera en que se recopila la inteligencia de señales, así como a lo que en realidad se recopila. Por ejemplo, para la determinación

([1]) Los organismos de seguridad o los organismos reguladores podrán solicitar información a las sociedades radicadas en los Estados Unidos con fines de investigación, de conformidad con otras autoridades penales, civiles y reguladoras que van más allá del alcance de este documento, que se limita a las autoridades de seguridad nacional.

de la posibilidad de recopilar la inteligencia de señales, los servicios de inteligencia deberán considerar la disponibilidad de otra información, incluidas las fuentes diplomáticas o públicas, y priorizar la recopilación a través de estos medios, siempre que proceda y sea factible. Además, las políticas de los elementos de los servicios de inteligencia podrían exigir que, cuando sea factible, la recopilación debería centrarse en determinados objetivos o temas de inteligencia exterior a través del uso de discriminantes (por ejemplo, canales, criterios de selección e identificadores específicos).

Es importante ver la información proporcionada a la Comisión en su conjunto. Las decisiones relacionadas con lo que es «viable» o «factible» no se dejan al criterio de los individuos, sino que están sujetas a las políticas que los organismos han dictado en virtud de la PPD-28, que se encuentra públicamente disponible, y a los demás procedimientos descritos en ella ([1]). Tal como establece la PPD-28, la recopilación en bloque de la inteligencia de señales es una recopilación que debido a consideraciones técnicas u operativas, es obtenida sin el uso de discriminantes (por ejemplo, determinados discriminantes, criterios de selección, etc.) En este sentido, la PPD-28 reconoce que los elementos de los servicios de inteligencia deberán recopilar la inteligencia de señales en bloque en determinadas circunstancias con el objeto de identificar las amenazas nuevas o emergentes y otra información vital de seguridad nacional que a menudo se esconde dentro del enorme y complejo sistema de las comunicaciones globales modernas. También reconoce la preocupación relacionada con la privacidad y las libertades civiles que supone la recopilación en bloque de la inteligencia de señales. Por consiguiente, la PPD-28 establece que los servicios de inteligencia deben dar prioridad a las alternativas que permitan una recopilación de inteligencia de señales selectiva en lugar de una recopilación de inteligencia de señales en bloque. Por tanto, los elementos de los servicios de inteligencia deberían realizar actividades de recopilación selectiva de la inteligencia de señales en lugar de actividades de recopilación en bloque de la inteligencia de señales, en los casos en que sea factible ([2]). Estos principios garantizan que la excepción de la recopilación en bloque no absorberá la regla general.

En lo que se refiere al concepto de «razonabilidad», este es un principio básico de la legislación estadounidense. Significa que los elementos de los servicios de inteligencia no estarán obligados a adoptar ninguna medida teóricamente posible, sino más bien deberán equilibrar sus esfuerzos para la protección de los intereses legítimos de privacidad y libertades civiles con las necesidades prácticas de las actividades de inteligencia de señales. En este caso también se han hecho públicas la políticas de los organismos y se puede garantizar que el término «razonablemente diseñado para minimizar la divulgación y la conservación de información personal» no socava la norma general.

La PPD-28 también establece que la inteligencia de señales recopilada en bloque solo puede utilizarse para seis propósitos concretos: la detección y el contraataque ante determinadas actividades de potencias extranjeras; la lucha antiterrorista; la lucha contra la proliferación; la ciberseguridad; la detección y el contraataque a amenazas a los ejércitos estadounidense o aliados; y la lucha contra las amenazas criminales transnacionales, incluida la elusión de sanciones. El Consejero de seguridad nacional del presidente (National Security Advisor), en consulta con el Director de Inteligencia Nacional (Director for National Intelligence, DNI), revisará anualmente estos usos permisibles de la inteligencia de señales recopilada en bloque para ver si deben cambiarse. El DNI hará pública esta lista en la mayor medida posible y de conformidad con la seguridad nacional. Esto constituye una limitación importante y transparente sobre el uso de la recopilación en bloque de la inteligencia de señales.

Asimismo, los elementos de los servicios de inteligencia que implanten la PPD-28 han reforzado las prácticas y las normas analíticas existentes para las consultas sobre inteligencia de señales no evaluada ([3]). Los analistas deben estructurar sus consultas u otros términos y técnicas de búsqueda a fin de garantizar su idoneidad para la identificación de información pertinente para una misión válida de inteligencia extranjera o de aplicación de la ley. En este sentido, los servicios de inteligencia deben centrar sus consultas relativas a personas en las categorías de información de inteligencia de señales adecuadas a efectos de la información exterior o una exigencia de aplicación de la ley con el objeto de evitar el uso de información personal no pertinente para la inteligencia exterior o la aplicación de la ley.

Es importante hacer hincapié en que las actividades de recopilación en bloque relacionadas con las comunicaciones por Internet que realizan los servicios de inteligencia estadounidense a través de la inteligencia de señales operan en una pequeña parta de Internet. Asimismo, el uso de consultas selectivas, tal como se ha descrito antes, garantiza que solo aquellos elementos que se considera que poseen un posible valor de información son sometidos a los analistas para su examen. Estos límites pretenden proteger la privacidad y las libertades civiles de todas las personas, independientemente de su nacionalidad y de donde residan.

([1]) Disponible en www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Estos procedimientos implantan los conceptos de selección y adaptación debatidos en esta carta de una manera determinada para cada elemento de los servicios de inteligencia.

([2]) Para citar solo un ejemplo, los procedimientos de la Agencia Nacional de Seguridad que implantan la PPD-28 afirman que «cuando sea factible, la recopilación se llevará a cabo mediante el uso de uno o más criterios de selección con el objeto de centrar la recopilación en determinados objetivos de inteligencia exterior (por ejemplo, un terrorista o grupo terrorista reconocido a nivel internacional) o un determinado tema de inteligencia exterior (por ejemplo, la proliferación de armas de destrucción masiva por parte de una potencia extranjera o sus agentes»).

([3]) Disponible en: http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf

Los Estados Unidos han elaborado procedimientos para garantizar que las actividades de inteligencia de señales se realizan solo para unos propósitos de seguridad nacional adecuados. Cada año, el presidente establece las prioridades del país para la recopilación de inteligencia exterior tras un exhaustivo proceso formal interinstitucional. El DNI es el responsable de trasladar estas prioridades de inteligencia al marco de prioridades de la inteligencia nacional (National Intelligence Priorities Framework, NIPF). La PPD-28 reforzó y mejoró el proceso interinstitucional para garantizar la revisión de todas las prioridades de inteligencia de los servicios de inteligencia y su aprobación por parte de responsables políticos de alto nivel. La Directiva de los servicios de inteligencia (Intelligence Community Directive, ICD) 204 ofrece una mayor orientación sobre el NIPF y se actualizó en enero de 2015 para incorporar los requisitos de la PPD-28 ([1]). Aunque los datos del NIPF están clasificados, la información relacionada con unas determinadas prioridades de inteligencia exterior de EE. UU. se refleja anualmente en un documento no clasificado del DNI, la Evaluación de la Amenaza Mundial (Wordwide Threat Assessment), que también se encuentra disponible en la web de la ODNI.

Las prioridades del NIPF están formuladas a un nivel de generalidad relativamente elevado. Incluyen temas como el desarrollo de capacidades en materia de misiles nucleares y balísticos por parte de algunos adversarios extranjeros, los efectos de la corrupción de los cárteles de droga y los abusos de los derechos humanos en determinados países. Y no se aplican tan solo a la inteligencia de señales, sino también a todas las actividades de inteligencia. La organización responsable de trasladar las prioridades del NIPF a la recopilación real de inteligencia de señales recibe el nombre de Comité Nacional de Inteligencia de Señales, o (National Signals Intelligence Committee, SIGCOM). Opera bajo los auspicios del Director de la Agencia Nacional de Seguridad (National Security Agency, NSA), el cual es designado por la Orden Ejecutiva 12333 como el «jefe funcional de la inteligencia de señales», responsable de la supervisión y la coordinación de la inteligencia de señales en el ámbito de los servicios de inteligencia, bajo la supervisión del Secretario de Defensa y del DNI. El SIGCOM cuenta con representantes de todos los servicios de inteligencia y, en cuanto se implante íntegramente la PPD-28 en los Estados Unidos, también contará con representantes de otros departamentos y organismos con un interés político en la inteligencia de señales.

Todos los departamentos y organismos de EE. UU. que sean consumidores de inteligencia exterior presentan sus solicitudes de recopilación al SIGCOM. El SIGCOM revisa estas solicitudes, comprueba su coherencia con el NIPF y les asigna prioridades utilizando criterios tales como:

— ¿puede la inteligencia de señales proporcionar información útil en este caso, o existen fuentes de información mejores o más rentables para tratar la solicitud en cuestión, como imágenes o información de dominio público?,

— ¿qué importancia tiene esta necesidad de información? Si es una prioridad en el NIPF, será generalmente una prioridad de la inteligencia de señales,

— ¿qué tipo de inteligencia de señales podría utilizarse?,

— ¿es la recopilación lo más adecuada posible? ¿Debería haber limitaciones temporales, geográficas o de otro tipo?

El proceso de evaluación de las necesidades de inteligencia de señales aplicado por los Estados Unidos también exige la explícita consideración de otros factores, en especial:

— ¿son el objetivo de la recopilación o la metodología utilizada para la recopilación, especialmente delicados? En caso afirmativo, se exigirá la revisión por parte de políticos de primer orden,

— ¿supondrá la recopilación un riesgo innecesario para la privacidad y las libertades civiles, independientemente de la nacionalidad de los interesados?,

— ¿se precisan otras garantías en materia de divulgación y conservación para proteger la privacidad o los intereses de la seguridad nacional?

Por último, al final del proceso, personal cualificado de la NSA recoge las prioridades validadas por el SIGCOM y busca e identifica determinados criterios de selección, como números de teléfono o direcciones de correo electrónico, que permitirán recopilar inteligencia exterior conforme a estas prioridades. Todos los selectores deberán ser revisados y aprobados antes de su inclusión en los sistemas de recopilación de la NSA. Incluso entonces, la posibilidad de que se

([1]) Disponible en: http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligenc%20Priorities%20Framework.pdf

lleve a cabo la recopilación y en qué momento dependerá en parte de otras consideraciones como la disponibilidad de unos recursos apropiados. Este proceso garantiza que los objetivos de la recopilación de inteligencia de señales estadounidense reflejen unas necesidades de inteligencia exterior válidas e importantes. Y, por supuesto, cuando la recopilación se lleva a cabo de conformidad con la FISA, la NSA y otros organismos deben acatar otras restricciones aprobadas por el Tribunal de la FISA. En pocas palabras, ni la NSA ni ningún otro servicio de inteligencia estadounidense decide por sí misma lo que debe recopilar.

En general, este proceso garantiza que todas las prioridades de la inteligencia estadounidense sean establecidas por políticos de primer orden, que están en la mejor posición para identificar los requisitos de EE. UU. de inteligencia exterior, y que estos políticos tienen en cuenta no tan solo el posible valor de la recopilación de inteligencia, sino también los riesgos relacionados con esta recopilación, incluidos los riesgos para la privacidad, los intereses económicos nacionales y las relaciones exteriores.

Con respecto a los datos transmitidos a los Estados Unidos en virtud del Escudo de la privacidad, aunque los Estados Unidos no pueden confirmar ni negar determinados métodos u operaciones, se aplican los requisitos de la PPD-28 a las operaciones de inteligencia de señales llevadas a cabo por los Estados Unidos, independientemente del tipo o de la fuente de los datos que se recopilen. Además, las limitaciones y las protecciones aplicables a la recopilación de la inteligencia de señales se aplicarán a la inteligencia de señales recopilada para cualquier propósito autorizado, incluidas las relaciones exteriores y a efectos de la seguridad nacional.

Los procedimientos mencionados muestran un compromiso evidente de los Estados Unidos para impedir una recopilación arbitraria e indiscriminada de información relacionada con la inteligencia de señales y aplicar, desde las esferas más altas de nuestro Gobierno, el principio de razonabilidad. La PPD-28 y sus procedimientos de ejecución en los organismos aclaran las limitaciones nuevas y las existentes y describen con mayor detalle el propósito para el que los Estados Unidos recopilan y utilizan la inteligencia de señales. Esto debería garantizar que las actividades de inteligencia se lleven a cabo y continúen llevándose a cabo únicamente con el propósito de legitimar los objetivos de la inteligencia exterior.

c. **Limitaciones de la conservación y la divulgación**

El artículo 4 de la PPD-28 exige que todos los servicios de inteligencia posean unos límites explícitos de conservación y divulgación de la información personal de ciudadanos no estadounidenses obtenida por la inteligencia de señales, comparables a los límites establecidos para los ciudadanos estadounidenses. Estas normas se incorporan a los procedimientos de cada organismo de los servicios de inteligencia dados a conocer en febrero de 2015 y públicamente disponibles. Para optar a la conservación o divulgación en calidad de inteligencia exterior, la información personal deberá estar relacionada con un requisito de inteligencia autorizado, tal como se establece en el proceso del NIPF antes descrito; ser considerada razonablemente como prueba de un delito; o satisfacer a alguno de los otros criterios de conservación de información sobre ciudadanos estadounidenses identificado en la Orden Ejecutiva 12333, sección 2.3.

La información para la que no se cumpla ninguno de estos criterios no podrá ser conservada más de cinco años, salvo que el DNI determine explícitamente que la prolongación de su conservación es en aras de la seguridad nacional de los Estados Unidos. Por tanto, los servicios de inteligencia deberán eliminar la información de ciudadanos estadounidenses obtenida a través de la inteligencia de señales cinco años después de su obtención, salvo que, por ejemplo, la información se considere que responde a una necesidad de información exterior autorizada, o si el DNI determina, una vez considerada la opinión del agente de la ODNI responsable de la protección de las libertades civiles y de los responsables de la protección de la privacidad y de las libertades civiles de los organismos, que la prolongación de su conservación responde a intereses de seguridad nacional.

Paralelamente, todas las políticas del organismo que implanten la PPD-28 exigen ahora explícitamente que la información relativa a una persona no pueda ser divulgada simplemente por el hecho de que el individuo no sea ciudadano estadounidense, y la ODNI ha emitido una directiva para que todos los servicios de inteligencia ([1]) cumplan este requisito. El personal de los servicios de inteligencia estará específicamente obligado a considerar los intereses de privacidad de las personas no estadounidenses en la elaboración y divulgación de los informes de inteligencia. Concretamente, la inteligencia de señales relacionada con las actividades rutinarias de una persona extranjera no se considerará inteligencia exterior que pueda ser divulgada o conservada con carácter permanente en virtud de este hecho aislado, salvo que se considere que atiende a un requerimiento autorizado de inteligencia exterior. Esto supone una limitación importante y atiende a la preocupación de la Comisión Europea sobre el alcance de la definición de inteligencia exterior establecida en la Orden Ejecutiva 12333.

([1]) Directiva relativa a los servicios de inteligencia (ICD) 203, disponible en: http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

d. **Observancia y supervisión**

El sistema estadounidense de supervisión de la inteligencia exterior ofrece un control estricto y a varios niveles para garantizar la observancia de las leyes y de los procedimientos aplicables, incluidos los relacionados con la recopilación, conservación y divulgación de la información de ciudadanos no estadounidenses obtenida por la inteligencia de señales, tal como se establece en la PPD-28. Este sistema cuenta con los siguientes elementos:

— los servicios de inteligencia emplean a cientos de personas dedicadas a la supervisión. Solo la NSA cuenta con más de 300 personas dedicadas al control del respeto de las normas, y en otros casos se cuenta también con oficinas de supervisión. Asimismo, el Departamento de Justicia, al igual que el Departamento de Defensa, ofrece una supervisión exhaustiva de las actividades de inteligencia,

— cada elemento de los servicios de inteligencia posee su propia Oficina del Inspector General con responsabilidad para la supervisión de las actividades de inteligencia exterior, entre otras cuestiones. Los inspectores generales son, por ley, independientes; tienen amplios poderes para llevar a cabo investigaciones, auditorías y revisiones de programas, incluidos los relativos al fraude y abuso o violación de la ley; y pueden recomendar acciones correctivas. A pesar de que las recomendaciones de los inspectores generales no son vinculantes, generalmente los informes de los inspectores generales se hacen públicos y, en todo caso, se presentan al Congreso; esto incluye los informes de seguimiento en caso de que no se hayan implantado las acciones correctivas recomendadas en anteriores informes. Por consiguiente, el Congreso recibe información de los incumplimientos y puede ejercer presión, incluso por vía presupuestaria, para la implantación de la acción correctiva. Se han hecho públicos varios informes de inspectores generales sobre los programas de inteligencia ([1]),

— la Oficina de Libertades Civiles y Privacidad de la ODNI (Civil Liberties and Privacy Office, CLPO) se encarga de garantizar que la actuación de los servicios de inteligencia favorezca la seguridad nacional y proteja las libertades civiles y los derechos a la privacidad ([2]). Otros elementos de los servicios de inteligencia tienen sus propios agentes responsables de la privacidad,

— el Consejo de Supervisión de la Privacidad y de las Libertades Civiles (Privacy and Civil Liberties Oversight Board, PCLOB), órgano independiente establecido por ley, se encarga de analizar y revisar los programas y las políticas de la lucha antiterrorista, incluido el uso de la inteligencia de señales, para garantizar una protección adecuada de la privacidad y de las libertades civiles. Ha emitido varios informes públicos sobre las actividades de inteligencia,

— tal como se detalla a continuación, el Tribunal de la FISA, compuesto por jueces federales independientes, es el responsable de la supervisión y el cumplimiento de las actividades de recopilación de inteligencia de señales llevadas a cabo en virtud de la FISA,

— por último, el Congreso estadounidense, concretamente las Comisiones de Inteligencia y de Asuntos Judiciales de la Cámara de Representantes y del Senado, poseen importantes responsabilidades de supervisión con relación a todas las actividades de inteligencia exterior de EE. UU., incluida la inteligencia de señales.

Aparte de estos mecanismos formales de supervisión, los servicios de inteligencia poseen numerosos mecanismos para garantizar la observancia, en su seno, de las limitaciones a la recopilación antes descritas, por ejemplo:

— los altos funcionarios del gabinete presidencial están obligados a validar cada año sus requisitos en materia de inteligencia de señales,

— la NSA comprueba los objetivos del proceso de recopilación de inteligencia de señales en su totalidad para determinar si está realmente ofreciendo una inteligencia exterior acorde con las prioridades, y suspenderá la recopilación en caso contrario. Existen otros procedimientos que garantizan la revisión periódica de los criterios de selección,

([1]) Véase, por ejemplo, el informe del inspector general del Departamento de Justicia «A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008» («Revisión de las actividades de investigación de la Oficina Federal previstas en el artículo 702 de la Ley de Vigilancia de la Inteligencia Exterior de 2008») (septiembre de 2012), disponible en: https://oig.justice.gov/reports/2016/o1601a.pdf

([2]) Véase www.dni.gov/clpo

— sobre la base de la recomendación de un grupo de revisión independiente nombrado por el presidente Obama, el DNI ha establecido un nuevo mecanismo para la supervisión de la recopilación y divulgación de la inteligencia de señales especialmente delicada debido a la naturaleza del objetivo o a los medios de recopilación, para garantizar su coherencia con los objetivos de los políticos,

— por último, la ODNI revisa anualmente la asignación de recursos a los servicios de inteligencia con arreglo a las prioridades del NIPF y la misión de inteligencia en su conjunto. Esta revisión incluye la evaluación del valor de todos los tipos de recopilación de inteligencia, incluida la inteligencia de señales, y realiza un análisis retrospectivo (¿han alcanzado los servicios de inteligencia sus objetivos?)- y un análisis prospectivo (¿cuáles serán las necesidades de los servicios de inteligencia en el futuro?). De este modo, se garantiza que los recursos de la inteligencia de señales se asignen a las prioridades nacionales más importantes.

Tal como se demuestra en esta visión general, los servicios de inteligencia no deciden por sí mismos qué conversaciones deben escuchar, no intentan recopilarlo todo, y no operan sin control. Sus actividades se centran en las prioridades establecidas por los políticos a través de un proceso que incluye aportaciones del Gobierno, y que son supervisadas tanto por la NSA como por la ODNI, el Departamento de Justicia y el Departamento de Defensa.

La PPD-28 contiene también otras muchas disposiciones para garantizar la protección de la información personal obtenida en virtud de la inteligencia de señales, independientemente de la nacionalidad. Por ejemplo, la PPD-28 contempla la seguridad de los datos, el acceso y los procedimientos de calidad para la protección de la información personal obtenida a través de la inteligencia de señales, y ofrece formación obligatoria para garantizar que el personal comprende su responsabilidad en la protección de la información personal, independientemente de la nacionalidad del interesado. La PPD también contempla los mecanismos de supervisión y de observancia. Estos mecanismos incluyen auditorías y revisiones periódicas por parte de los funcionarios de supervisión y observancia de las prácticas para la protección de la información personal contenida en la inteligencia de señales. Las revisiones deberán también examinar el cumplimiento por parte de los organismos de los procedimientos para la protección de esta información.

Asimismo, la PPD-28 establece que las cuestiones de observancia importantes relacionadas con ciudadanos no estadounidenses serán remitidas al más alto nivel gubernamental. En caso de que surja una cuestión de observancia importante que esté relacionada con la información personal de cualquier persona, obtenida a través de las actividades de inteligencia de señales, esto deberá comunicarse rápidamente al DNI, además de otros requisitos de notificación. Si la cuestión está relacionada con la información personal de una persona no estadounidense, el DNI, tras consultarlo con el secretario de Estado y el responsable del correspondiente servicio de inteligencia, determinará los pasos que deberán acometerse para notificarlo al Gobierno extranjero pertinente, respetando la protección de las fuentes y métodos del personal estadounidense. Además, tal como establece la PPD-28, el secretario de Estado ha designado a una alta funcionaria, la subsecretaria Catherine Novelli, para actuar de punto de contacto para los gobiernos extranjeros que deseen resolver sus dudas sobre las actividades de la inteligencia de señales de los Estados Unidos. Este compromiso de alto nivel ejemplifica los esfuerzos realizados por el Gobierno estadounidense durante los últimos años para crear un sentimiento de confianza en las numerosas y coincidentes protecciones de la privacidad aplicadas a ciudadanos estadounidenses y no estadounidenses.

e. **Resumen**

Los procedimientos estadounidenses para la recopilación, la conservación y la divulgación de la inteligencia exterior ofrecen importantes protecciones de la privacidad para la información personal de todas las personas, independientemente de su nacionalidad. Concretamente, estos procesos velan por que nuestros servicios de inteligencia se concentren en su misión de seguridad nacional en aplicación de por las leyes vigentes, las órdenes ejecutivas y las directivas presidenciales, protejan la información contra el acceso, el uso y la divulgación no autorizados, y lleven a cabo sus actividades con revisiones y controles a distintos niveles, incluidas las comisiones de supervisión del Congreso. La PPD-28 y los procedimientos que la implantan reflejan nuestros esfuerzos por extender una cierta minimización y otros principios de protección de los datos sustanciales a la información personal de todas las personas, independientemente de su nacionalidad. La información personal obtenida de la recopilación de la inteligencia de señales estadounidense está sujeta a los principios y requisitos de la legislación estadounidense y de las directivas presidenciales, incluidas las protecciones establecidas en la PPD-28. Estos principios y requisitos garantizan el tratamiento digno y respetuoso de todas personas, independientemente de su nacionalidad o del lugar donde residan, y reconocen que todas las personas tienen intereses legítimos de privacidad en el tratamiento de su información personal.

II. LEY DE VIGILANCIA DE LA INTELIGENCIA EXTERIOR — SECCIÓN 702

La recopilación llevada a cabo de conformidad con la Ley de Vigilancia de la Inteligencia Exterior no es ([1])«masiva e indiscriminada», sino que está estrictamente centrada en la recopilación de inteligencia exterior de objetivos legítimos identificados individualmente; está claramente autorizada por una autoridad legal explícita; y está sujeta a un control judicial independiente y a la revisión y supervisión por parte del poder ejecutivo y del Congreso. La recopilación en virtud del artículo 702 se considera inteligencia de señales sujeta a los requisitos de la PPD-28 ([2]).

La recopilación estipulada en el artículo 702 es una de las fuentes de inteligencia más valiosas tanto para la protección de los Estados Unidos como de nuestros socios europeos. Se encuentra públicamente disponible una información más exhaustiva sobre el funcionamiento y la supervisión del artículo 702. Se han desclasificado y publicado numerosos expedientes judiciales, resoluciones judiciales e informes de supervisión relativos al programa en la página web pública de la ODNI, www.icontherecord.tumblr.com. Asimismo, el PCLOB analizó exhaustivamente el artículo 702 en un informe disponible en https://www.pclob.gov/library/702-Report.pdf ([3]).

El artículo 702 entró a formar parte de la Ley de Enmiendas de la FISA de 2008, ([4]) tras un debate público exhaustivo en el Congreso. Autoriza la obtención de información de inteligencia exterior mediante la segmentación de las personas no estadounidenses que se encuentran fuera de los Estados Unidos, con la colaboración obligada de los proveedores de servicios de comunicaciones electrónicas. El artículo 702 autoriza al Fiscal General y al DNI –dos altos funcionarios del gabinete presidencial nombrados por el presidente y confirmados por el Senado–, a presentar certificaciones anuales al Tribunal de la FISA ([5]). Estas certificaciones identifican las categorías concretas de inteligencia exterior a recopilar, como la inteligencia relacionada con la lucha antiterrorista o las armas de destrucción masiva, que deben recaer dentro del ámbito de las categorías de inteligencia exterior definidas por la FISA ([6]). Tal como señala el PCLOB, «estas limitaciones *no* permiten la recopilación ilimitada de información sobre los extranjeros» ([7]).

Las certificaciones deben incluir también los procedimientos de «segmentación» y «minimización», que deben ser revisados y aprobados por el Tribunal de la FISA ([8]). Los procedimientos de segmentación han sido diseñados para garantizar únicamente la recopilación autorizada por la ley y contemplada en las certificaciones; los procedimientos de minimización han sido diseñados para limitar la obtención, divulgación y conservación de la información sobre ciudadanos estadounidenses, pero también contienen disposiciones que ofrecen una protección sustancial de la información sobre ciudadanos no estadounidenses, tal como se describe a continuación. Además, tal como se ha descrito antes, en la PPD-28 el presidente dio órdenes de que los servicios de inteligencia ofrecieran otras protecciones para la información personal sobre los ciudadanos estadounidenses, y estas protecciones se aplican a la información recopilada en virtud del artículo 702.

Una vez que el tribunal apruebe los procedimientos de segmentación y de minimización, la recopilación contemplada en el artículo 702 no será en bloque o indiscriminada, sino que «consistirá únicamente en la segmentación de personas concretas sobre las cuales se ha realizado una determinación individualizada», tal como afirma el PCLOB ([9]). La segmentación de la recopilación se realiza con el uso de selectores individuales, como las direcciones de correo

([1]) Cuando los actos o prácticas desleales o fraudulentos tengan lugar de forma continuada, o si ya se han dictado mandamientos para el cese de los mismos, la FTC puede promulgar una norma administrativa que prohíba los actos o prácticas en cuestión, véase USC, título 50, artículo 1881a.

([2]) Los Estados Unidos podrán obtener órdenes judiciales de conformidad con otras disposiciones de la FISA para la obtención de datos, incluidos los datos transferidos en virtud del Escudo de la privacidad. Véase USC, título 50, artículo 1801 *et seq*. Los títulos I y III de la FISA, que autorizan, respectivamente, la vigilancia electrónica y las búsquedas físicas, exigen una orden judicial (salvo en situaciones de emergencia) y requieren siempre que hayan razones para pensar que el objetivo es una potencia extranjera o un agente de una potencia extranjera. El título IV de la FISA autoriza el uso de escuchas telefónicas y de registros de llamadas salientes en virtud de una orden judicial (salvo en situaciones de emergencia) en la inteligencia exterior autorizada, el contraespionaje o las investigaciones necesarias para la lucha antiterrorista. El título V de la FISA permite que el FBI, de conformidad con una orden judicial (salvo en situaciones de emergencia), pueda obtener registros comerciales importantes para una inteligencia exterior autorizada, el contraespionaje o las investigaciones necesarias para la lucha antiterrorista. Tal como se ha mencionado antes, la Ley de la Libertad (USA FREEDOM) prohíbe explícitamente el uso de órdenes FISA que autoricen escuchas telefónicas o registros de llamadas salientes para la recopilación en bloque, e impone la exigencia de un «criterio de selección específico» para garantizar el uso selectivo de estas facultades.

([3]) Consejo de Privacidad y Libertades Civiles, «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act» («Informe sobre el Programa de Vigilancia aplicado en virtud del artículo 702 de la Ley de Vigilancia de la Inteligencia Exterior») (2 de julio de 2014) («Informe del PCLOB»).

([4]) Véase Pub. L. n.º 110-261, 122 Stat. 2436 (2008).

([5]) Véase USC, título 50, artículo 1881a(a) y (b).

([6]) Véase *íd*. artículo 1801(e).

([7]) Véase el informe del PCLOB en 99.

([8]) Véase USC, título 50, artículo 1881a(d) y (e).

([9]) Véase el informe del PCLOB en 111.

electrónico o los números de teléfono que el personal de inteligencia estadounidense haya determinado que es probable que se usen para la comunicación de información en materia de inteligencia exterior del tipo contemplado en la certificación presentada al tribunal ([1]). La base para la selección del objetivo debe estar documentada, y la documentación de cada selector será posteriormente revisada por el Departamento de Justicia ([2]). El Gobierno de EE.U.U. ha publicado información que demuestra que en 2014 había aproximadamente 90 000 individuos afectados en virtud del artículo 702, una cantidad minúscula si la comparamos con los más de 3 000 millones de usuarios de internet que existen en todo el mundo ([3]).

La información recopilada en virtud del artículo 702 está sujeta a los procedimientos de minimización aprobados por el tribunal, que ofrecen protecciones a ciudadanos no estadounidenses, así como a ciudadanos estadounidenses, y que han sido dados a conocer públicamente ([4]). Por ejemplo, las comunicaciones obtenidas en virtud del artículo 702, independientemente de que sean ciudadanos estadounidenses o no, se almacenan en bases de datos con unos controles de acceso estrictos. Solo podrán ser revisadas por personal de inteligencia que haya recibido formación sobre los procedimientos de minimización de la protección de privacidad y que haya sido específicamente autorizado para acceder con el objeto de llevar a cabo sus funciones autorizadas ([5]). El uso de los datos se limita a la identificación de la información en materia de inteligencia exterior o de la prueba de un delito ([6]). De conformidad con la PPD-28, esta información solo podrá divulgarse si existe una finalidad válida de inteligencia exterior o de aplicación de la ley; no basta el mero hecho de que una parte de la comunicación sea un ciudadano no estadounidense ([7]). Asimismo, los procedimientos de minimización y la PPD-28 establecen límites sobre cuánto tiempo pueden conservarse los datos obtenidos en virtud del artículo 702 ([8]).

La supervisión del artículo 702 es exhaustiva y es llevada a cabo por los tres órganos de nuestro Gobierno. Los organismos que implementan la ley tienen revisiones internas a varios niveles, incluidos inspectores generales independientes y controles tecnológicos del acceso a los datos. El Departamento de Justicia y la ODNI revisan y analizan estrechamente el uso del artículo 702 para verificar la observancia de las normas legales; los organismos están sometidos también a una obligación independiente de comunicar los posibles incidentes de incumplimiento. Estos incidentes son investigados, y todos los incumplimientos se remiten al Tribunal de Vigilancia de la Inteligencia Exterior, al Consejo Supervisor de Inteligencia del presidente y al Congreso, y son debidamente subsanados ([9]). Hasta la fecha no se han producido intentos deliberados de violación de la ley ni de elusión de los requisitos legales ([10]).

El Tribunal de la FISA desempeña un papel importante en la implantación del artículo 702. Está compuesto por jueces federales independientes que ocupan su cargo en el Tribunal de la FISA durante un período de siete años pero que, al igual que todos los jueces federales, son jueces con carácter vitalicio. Tal como se ha mencionado antes, el Tribunal deberá revisar las certificaciones anuales y los procedimientos de segmentación y minimización para dar cumplimiento a la ley. Asimismo, y tal como se ha mencionado antes, el Gobierno deberá notificar de inmediato al Tribunal cualquier incumplimiento ([11]) y se han desclasificado y publicado diversos dictámenes del Tribunal que demuestran el excepcional grado de control judicial e independencia que este ejerce en la revisión de estos incumplimientos.

Los rigurosos procedimientos del Tribunal han sido descritos por el antiguo presidente del Tribunal en una carta al Congreso hecha pública ([12]). Y tal como se desprende de la Ley de Libertad de EE. UU., descrita a continuación, el Tribunal está ahora explícitamente autorizado a nombrar un letrado externo como defensor independiente de la privacidad en casos que planteen cuestiones jurídicas novedosas o importantes ([13]). Este grado de implicación por parte de un poder judicial independiente en las actividades de inteligencia exterior destinadas a personas que no son ciudadanos de este país ni residentes en el país, es excepcional por no decir inaudito y permite garantizar la recopilación del artículo 702 dentro de unos límites legales adecuados.

([1]) *Id*.

([2]) *Íd*. en 8; USC, título 50, artículo 1881a(l); véase también el informe del Director de Privacidad y Libertades Civiles de la NSA, «NSA's Implementation of Foreign Intelligence Surveillance Act Section 702» (en lo sucesivo, el «Informe NSA») en 4, disponible en http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Informe de Transparencia de 2014 del Director de Inteligencia Nacional, *disponible en* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014

([4]) Procedimientos de minimización disponibles en: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf («Procedimientos de minimización de la NSA»); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf *y* http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf

([5]) Véase el informe de la NSA en 4.

([6]) Véase, por ejemplo, «Procedimientos de minimización de la NSA» en 6.

([7]) Procedimientos de la PPD-28 de la Agencia de Inteligencia, disponibles en http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties

([8]) Véase «Procedimientos de minimización de la NSA»; PPD-28, artículo 4.

([9]) Véase USC, título 50, artículo 1881(l); véase también el informe del PCLOB en 66-76.

([10]) Véase la «Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act» («Valoración semestral del cumplimiento de los procedimientos y de las directrices estipuladas en el artículo 702 de la Ley de Vigilancia de la Inteligencia Exterior»), presentada por el Fiscal General y el Director de Inteligencia Nacional, en 2-3, disponible en http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf

([11]) Regla 13 de las Reglas de Procedimientos del Tribunal de Vigilancia de la Inteligencia Exterior, disponible en http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf

([12]) Carta del 29 de julio de 2013 del Honorable Reggie B. Walton al Honorable Patrick J. Leahy, disponible en http://fas.org/irp/news/2013/07/fisc-leahy.pdf

([13]) Véase el artículo 401 de la Ley de Libertad de EE. UU., P.L. 114-23.

El Congreso ejerce la supervisión a través de los informes exigidos por la ley para las Comisiones de Inteligencia y Judicial, y de las sesiones informativas y audiencias celebradas con carácter regular. Estas incluyen un informe semestral del Fiscal General que documenta el uso del artículo 702 y los incidentes de incumplimiento ([1]); una valoración semestral del Fiscal General y del DNI que documenta la observancia de los procedimientos de segmentación y minimización, incluida la observancia de los procedimientos diseñados para garantizar que esta recopilación es para una finalidad de inteligencia exterior válida ([2]); y un informe anual de los responsables de los elementos de inteligencia que incluye una certificación de que la recopilación realizada en virtud del artículo 702 continúa produciendo información en materia de inteligencia exterior ([3]).

En resumen, la recopilación en virtud del artículo 702 está autorizada por la ley; está sujeta a diversos niveles de revisión y de control y supervisión judicial; y, tal como afirmó el Tribunal de la FISA en un dictamen recientemente desclasificado, «no se realiza en bloque ni indiscriminadamente», sino a través de […] decisiones de segmentación discretas para servicios [de comunicación] individuales» ([4]).

III. LEY DE LIBERTAD DE EE. UU. (USA FREEDOM ACT)

La Ley de Libertad de EE. UU., promulgada en junio de 2015, modificó considerablemente las competencias de vigilancia y otras competencias sobre seguridad nacional de los Estados Unidos, y aumentó la transparencia pública sobre el uso de estas competencias y sobre las decisiones del Tribunal de la FISA, tal como se describe a continuación ([5]). La Ley garantiza la competencia que necesitan nuestros profesionales de inteligencia y de aplicación de la ley para proteger la nación, a la vez que garantiza también la correcta protección de la privacidad de las personas cuando se recurre al empleo de estas competencias. Incrementa la privacidad y las libertades civiles y aumenta la transparencia.

La Ley prohíbe la recopilación en bloque de los registros, incluidos los de los ciudadanos estadounidenses y los de los no estadounidenses, de conformidad con las disposiciones de la FISA o mediante el uso de las Cartas de Seguridad Nacional, una forma de citaciones administrativas autorizadas por ley ([6]). Esta prohibición incluye específicamente metadatos telefónicos relacionados con las llamadas entre personas situadas en EE. UU. y personas situadas fuera de EE. UU., y también deberían incluir la recopilación de la información relacionada con el Escudo de la privacidad contemplada por estas autoridades. La Ley exige que el Gobierno base cualquier solicitud de registros contemplada por estas autoridades en un «criterio de selección concreto», un término que identifica específicamente a una persona, una cuenta, una dirección o un dispositivo personal, con el objeto de limitar el alcance de la información buscada de la manera más razonable posible ([7]). Esto garantiza además que la recopilación de la información para fines de inteligencia está perfectamente centrada y focalizada.

La Ley también hizo importantes modificaciones en los procedimientos ante el Tribunal de la FISA, que incrementan la transparencia y ofrecen otras garantías de protección de la privacidad. Tal como se ha observado antes, autorizó la creación de un panel permanente de habilitación de la seguridad con abogados expertos en privacidad y libertades colectivas, recopilación de inteligencia, tecnología de la información u otras áreas pertinentes, que pueden ser citados para declarar ante el tribunal en calidad de *amicus curiae* en los casos que comporten interpretaciones novedosas o importantes de la ley. Estos abogados están autorizados a exponer argumentos jurídicos que supongan un avance en la protección de la privacidad y de las libertades civiles individuales, y tendrán acceso a cualquier información, incluida la información confidencial, que el tribunal considere necesaria para sus atribuciones ([8]).

La Ley se basa asimismo en la transparencia sin precedentes del Gobierno de los EE. UU. sobre las actividades de inteligencia al exigir al DNI, en consulta con el Fiscal General, que desclasifique o publique un resumen confidencial de cada resolución, orden o dictamen emitido por el Tribunal de la FISA o el Tribunal de Revisión de la Vigilancia de la Inteligencia Exterior que implique una interpretación importante de una disposición legislativa.

([1]) Véase USC, título 50, artículo 1881f.
([2]) Véase id. artículo 1881a(l)(1).
([3]) Véase id. artículo 1881a(l)(3). Algunos de estos informes son confidenciales.
([4]) Mem. Dictamen y Orden, en 26 (FISC 2014), disponible en http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf
([5]) Véase Ley de Libertad de EE. UU., Pub. L. n.º 114-23, § 401, 129 Stat. 268.
([6]) Véase *íd*. artículos 103, 201, 501. Las cartas de seguridad nacional son autorizadas por varias leyes y permiten que el FBI obtenga información contenida en informes crediticios, registros financieros y registros electrónicos de abonados y de operaciones de determinados tipos de empresas, con el único propósito de protegerse contra el terrorismo internacional o las actividades de inteligencia clandestinas. Véase USC, título 12, artículo 3414; USC, título 15, artículos 1681u-1681v; USC, título 18, artículo 2709. Las cartas de seguridad nacional son utilizadas normalmente por el FBI para reunir información de contenido no crítico en las primeras fases de las investigaciones antiterroristas y de contraespionaje, como la identidad del abonado a una cuenta que se haya puesto en comunicación con agentes de un grupo terrorista como ISIL. Los destinatarios de la Carta Nacional de Seguridad tienen derecho a impugnarla ante un tribunal. Véase USC, título 18, artículo 3511.
([7]) Véase *íd*.
([8]) Véase *íd*. artículo 401.

Además, la Ley contempla revelaciones extensivas sobre los requisitos de recopilación de la FISA y de la Carta de Seguridad Nacional. Los Estados Unidos deberán revelar cada año al Congreso y al público en general el número de órdenes y certificaciones del FISA solicitadas y recibidas; la estimación del número de personas estadounidenses y no estadounidenses afectadas por la vigilancia; y el número de citaciones de *amici curiae*, entre otros elementos de información ([1]). La Ley también exige la presentación de otros informes públicos por parte del Gobierno sobre el número de solicitudes de una Carta de Seguridad Nacional sobre ciudadanos estadounidenses y ciudadanos no estadounidenses ([2]).

Con respecto a la transparencia corporativa, la Ley ofrece a las empresas una serie de opciones para dar a conocer públicamente el número total de órdenes y directivas de la FISA o de Cartas de Seguridad Nacional que han recibido del Gobierno, así como el número de cuentas de clientes contempladas por estas órdenes ([3]). Varias empresas han comunicado ya estas informaciones, que han revelado que las solicitudes de información afectaban a un reducido número de clientes.

Estos informes de transparencia corporativa demuestran que las solicitudes estadounidenses de inteligencia afectan únicamente a una minúscula fracción de datos. Por ejemplo, un informe reciente de transparencia de una importante empresa demuestra que las solicitudes de seguridad nacional recibidas (relacionadas con la FISA o con las Cartas de Seguridad Nacional) afectaron a menos de 20 000 de sus cuentas en un momento en que tenía como mínimo 400 millones de abonados. En otras palabras, todas las solicitudes estadounidenses de seguridad nacional notificadas por esta empresa afectaron a menos del 0,005 % de sus abonados. Aun cuando todas estas peticiones hubieran estado relacionadas con los datos del puerto seguro, lo que obviamente no es el caso, es obvio que las solicitudes son selectivas y su alcance es apropiado, ni tampoco son en bloque o indiscriminadas.

Por último, aunque las leyes que autorizan las Cartas de Seguridad Nacional ya restringen las circunstancias en las que el destinatario de una de estas cartas podría estar obligado a no divulgarlas, la Ley establece además que estos requisitos de no divulgación deberán revisarse periódicamente; exige que los destinatarios de las Cartas de Seguridad Nacional reciban notificación cuando los hechos ya no impongan el requisito de no divulgación; y establece procedimientos para la impugnación de los requisitos de no divulgación por parte de los destinatarios ([4]).

En síntesis, las importantes modificaciones que aporta la Ley de Libertad de EE. UU. A las competencias de los organismos de inteligencia americanos es una prueba evidente del enorme esfuerzo realizado por los Estados Unidos para colocar la protección de la información personal, la privacidad, las libertades civiles y la transparencia en la vanguardia de todas las prácticas de inteligencia estadounidenses.

IV. TRANSPARENCIA

Aparte de la transparencia dictada por la Ley de Libertad de EE. UU., los servicios de inteligencia de EE. UU. da a conocer públicamente mucha más información, estableciendo así un sólido ejemplo con respecto a la transparencia en sus actividades de inteligencia. Los servicios de inteligencia han publicado muchas de sus políticas, procedimientos, resoluciones del Tribunal de Vigilancia de la Inteligencia Exterior y otros materiales desclasificados con un grado de transparencia excepcional. Asimismo, los servicios de inteligencia han aumentado sustancialmente la divulgación de sus estadísticas sobre el uso gubernamental de las autoridades de recopilación de la seguridad nacional. El 22 de abril de 2015, los servicios de inteligencia publicaron su segundo informe anual sobre la frecuencia con que el Gobierno utiliza estas importantes autoridades. La ODNI también publicó, en su web y en *IC On the Record*, una serie de principios de transparencia ([5]) especiales y un plan de implantación que traduce los principios en iniciativas concretas y medibles ([6]). En octubre de 2015, el Director de Inteligencia Nacional ordenó que todas las agencias de inteligencia designaran un Director de Transparencia de la Inteligencia para fomentar la transparencia e impulsar iniciativas de transparencia ([7]). El Director de Transparencia colaborará estrechamente con el Director de Privacidad y Libertades Civiles de cada servicio de inteligencia para garantizar que la transparencia, la privacidad y las libertades civiles continúen siendo las máximas prioridades.

([1]) Véase *íd*. artículo 602.
([2]) Véase *id*.
([3]) Véase *íd*. artículo 603.
([4]) Véase *íd*. artículo 502(f)-503.
([5]) Disponible en: http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles
([6]) Disponible en: http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf
([7]) Véase *id*.

Como ejemplo de estos esfuerzos, el director de privacidad y libertades civiles de la NSA ha publicado varios informes desclasificados durante los últimos años, incluidos los informes sobre actividades previstos en el artículo 702, la Orden Ejecutiva 12333 y la Ley de Libertad de EE. UU. ([1]). Asimismo, los servicios de inteligencia colaboran estrechamente con el PCLOB, el Congreso y la comunidad estadounidense de defensa de la privacidad para ofrecer una mayor transparencia en las actividades de inteligencia estadounidenses, en la medida en que sea factible y de conformidad con la protección de la confidencialidad de las fuentes y los métodos de inteligencia. En su conjunto, las actividades de inteligencia estadounidenses son tan transparentes o más transparentes que las de cualquier otro país del mundo y son tan transparentes como lo permita la necesidad de proteger la confidencialidad de las fuentes y los métodos.

Para resumir la enorme transparencia que existe sobre las actividades de inteligencia estadounidenses:

— los servicios de inteligencia han publicado y colgado en Internet miles de páginas de dictámenes judiciales y procedimientos de los servicios que destacan los procedimientos y requisitos concretos de nuestras actividades de inteligencia. También hemos publicado informes sobre el cumplimiento de las restricciones aplicables por parte de los servicios de inteligencia,

— los altos cargos en materia de inteligencia hablan en público con regularidad de las funciones y actividades de sus organizaciones e incluyen descripciones de los regímenes de cumplimiento y de las protecciones que disciplinan su trabajo,

— los servicios de inteligencia publicaron muchos otros documentos sobre las actividades de inteligencia relacionadas con nuestra Ley de Libertad de Información,

— el presidente promulgó la PPD-28 y estableció públicamente nuevas restricciones para nuestras actividades de inteligencia, y la ODNI dio a conocer dos informes públicos sobre la implantación de estas restricciones,

— los servicios de inteligencia están obligados ahora por ley a publicar los dictámenes jurídicos emitidos por el Tribunal de la FISA, o resúmenes de estos dictámenes,

— el Gobierno está obligado a informar anualmente sobre el alcance de su uso de determinados servicios de inteligencia, y las empresas están también autorizadas a hacerlo,

— el PCLOB ha publicado diversos informes públicos detallados sobre las actividades de inteligencia y continuará haciéndolo,

— los servicios de inteligencia proporcionan información confidencial exhaustiva a las comisiones de supervisión del Congreso,

— el DNI publicó los principios de transparencia que rigen las actividades de los servicios de inteligencia.

Continuaremos aplicando esta transparencia generalizada. Obviamente, cualquier información que sea públicamente divulgada estará disponible tanto en el Departamento de Comercio como en la Comisión Europea. La revisión anual entre el Departamento de Comercio y la Comisión Europea sobre la implantación del Escudo de la privacidad ofrecerá la posibilidad de que la Comisión Europea pueda discutir las cuestiones planteadas por cualquier nueva información divulgada, así como otras cuestiones referentes al Escudo de la privacidad y su funcionamiento, y entendemos que el Departamento, por decisión propia, podrá invitar a representantes de otros organismos, incluida los servicios de inteligencia, a participar en esta revisión. Obviamente, en calidad de añadido al mecanismo proporcionado en la PPD-28 a los Estados miembros de la UE para plantear cuestiones relacionadas con la vigilancia al funcionario del Departamento de Estado designado.

V. RECURSO

La legislación estadounidense ofrece diversas posibilidades de recurso a los individuos que han sido objeto de una vigilancia electrónica ilícita a efectos de la seguridad nacional. De conformidad con la FISA, el derecho a recurrir ante un tribunal estadounidense no está limitado a los ciudadanos estadounidenses. En virtud de la FISA, un individuo que pueda establecer la legitimación para la presentación de una demanda podría recurrir para impugnar los actos de vigilancia

([1]) Disponible en: https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf, https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf, https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf

electrónica ilícita. Por ejemplo, la FISA permite a las personas sometidas a una vigilancia electrónica ilícita a demandar a los funcionarios públicos estadounidenses a título personal a fin de obtener una reparación monetaria, incluidos daños y los honorarios de los abogados. Véase USC, título 50, artículo 1810. Los individuos que puedan establecer su legitimación para la presentación de una demanda, también pueden incoar un proceso civil para obtener una reparación monetaria, incluidas las costas del juicio, contra los Estados Unidos cuando la información relacionada con ellos obtenida con la ayuda de la vigilancia electrónica contemplada en la FISA sea ilícita y deliberadamente utilizada o divulgada. Véase USC, título 18, artículo 2712. En caso de que el Gobierno pretenda utilizar o divulgar cualquier información obtenida o derivada de la vigilancia electrónica relativa a una persona perjudicada con arreglo a la FISA, o utilizarla contra esa persona en un procedimiento judicial o administrativo en los Estados Unidos, deberá notificar con antelación su intención al tribunal y a la persona en cuestión, la cual podrá impugnar la legalidad de la vigilancia y reclamar la eliminación de la información. Véase USC, título 50, artículo 1806. Por último, la FISA establece sanciones penales para los individuos que intencionadamente ejerzan una vigilancia electrónica ilícita con apariencia de legalidad o que intencionadamente utilicen o divulguen la información obtenida con la vigilancia ilícita. Véase USC, título 50, artículo 1809.

Los ciudadanos estadounidenses tienen otras vías de buscar recursos legales contra los funcionarios públicos estadounidenses por un uso público ilícito de los datos o el acceso ilícito a los datos, incluidos los funcionarios públicos que infrinjan la ley en el transcurso de un acceso ilícito a la información o un uso ilícito de la información a los supuestos efectos de la seguridad nacional. La Ley de Fraude y Abuso Informático prohíbe el acceso intencionado no autorizado (o que sobrepase el acceso autorizado) para obtener información de una institución financiera, de un sistema informático del Gobierno de los EE. UU. o el acceso a un ordenador a través de Internet, así como las amenazas de daños en ordenadores protegidos con fines de extorsión o fraude. Véase USC, título 18, artículo 1030. Cualquier persona, independientemente de su nacionalidad, que sufra daños o pérdidas por la violación de esta ley podrá demandar al infractor (incluido as un funcionario público) para obtener daños compensatorios y medidas cautelares u otra reparación equitativa en virtud del artículo 1030(g), independientemente de que se haya entablado un proceso penal, siempre que la conducta comporte al menos una de las circunstancias indicadas en la ley. La Ley de Privacidad de las Comunicaciones Electrónicas (ECPA) regula el acceso del Gobierno a las comunicaciones electrónicas guardadas, a los registros de las operaciones y a la información relativa al abonado que obra en manos de proveedores externos de comunicaciones. Véase USC, título 18, artículos 2701-2712. La ECPA autoriza a un individuo agraviado a demandar a funcionarios públicos por el acceso deliberado e ilícito a los datos almacenados. La ECPA se aplica a todas las personas, independientemente de la ciudadanía y de que las personas agraviadas tengan derecho a una indemnización por daños perjuicios y a los honorarios de los abogados. El Derecho a la Ley de Privacidad Financiera (RFPA) limita el acceso del Gobierno de los EE. UU. a los registros bancarios y bursátiles de los clientes individuales. Véase USC, título 12, artículos 3401-3422. En virtud de la RFPA, el cliente de un banco o de un agente bursátil podrá demandar al Gobierno de los EE. UU. la indemnización legal, los daños reales y los daños punitivos por el acceso obtenido ilegalmente a los registros del cliente, y la comprobación de la ilegalidad de este acceso activó deliberada y automáticamente una investigación de una posible medida disciplinaria contra los empleados públicos pertinentes. Véase USC, título 12, artículo 3417.

Por último, la Ley para la Libertad de Información (FOIA) establece un medio para cualquier persona que pretenda acceder a los registros federales existentes sobre un tema sujeto a unas determinadas categorías de excepciones. Véase USC, título 5, artículo 552(b). Este medio incluye límites en el acceso a información confidencial de la seguridad nacional, información personal de terceros e información referente a las investigaciones sobre la aplicación de la ley, y son comparables a las limitaciones impuestas por los países con su propia legislación de acceso a la información. Estas limitaciones se aplican tanto a los estadounidenses como a los ciudadanos de otras nacionalidades. Las controversias sobre la divulgación de los registros solicitada en virtud de la FOIA podrá ser recurrida administrativamente y posteriormente en un tribunal federal. El tribunal está obligado a determinar *de novo* si los registros han sido debidamente denegados —USC, título 5, artículo 552(a)(4)(B) — y podrá obligar al Gobierno a facilitar el acceso a los registros. En determinados casos, los tribunales han revocado las alegaciones del Gobierno de que la información debería ser considerada como clasificada ([1]). Aunque no existen daños monetarios, los tribunales podrán adjudicar los honorarios de los abogados.

VI. CONCLUSIÓN

Los Estados Unidos reconocen que nuestra inteligencia de señales y otras actividades de inteligencia deben tener en cuenta que todas las personas deberían ser tratadas con dignidad y respeto, independientemente de su nacionalidad o lugar de residencia, y que todas las personas tienen intereses legítimos de privacidad en el tratamiento de su información personal. Los Estados Unidos solo utilizan inteligencia de señales para garantizar su seguridad nacional y defender sus intereses de política exterior, y para proteger del peligro a sus ciudadanos y a los ciudadanos de sus aliados y socios. En pocas palabras, los servicios de inteligencia no realizan una vigilancia indiscriminada de nadie, ni tampoco de los ciudadanos europeos. La recopilación de inteligencia de señales solo se realiza cuando está debidamente autorizada y cumpliendo estrictamente las limitaciones mencionadas, únicamente después de estudiar la disponibilidad

([1]) Véase, por ejemplo, New York Times v. Departamento de Justicia, 756 F.3d 100 (2d Cir. 2014); American Civil Liberties Union v. CIA, 710 F.3d 422 (D.C. Cir. 2014).

de fuentes alternativas, en particular diplomáticas y públicas, y dando prioridad a alternativas adecuadas y factibles. Y cuando sea factible, la recopilación de inteligencia de señales solo se centrará en objetivos o temas específicos de inteligencia exterior mediante el uso de discriminantes.

La política de EE. UU. al respecto se confirmó en la PPD-28. Dentro de este contexto, los servicios de inteligencia estadounidenses no tienen la competencia legal, los recursos, la capacidad técnica o el deseo de interceptar todas las comunicaciones del mundo. Estos organismos no leen los correos electrónicos de todos los ciudadanos de los Estados Unidos, ni del resto del mundo. De acuerdo con la PPD-28, los Estados Unidos ofrecen una firme protección de la información personal de ciudadanos no estadounidenses que se recopile a través de las actividades de inteligencia exterior. En la medida de lo posible y de acuerdo con la seguridad nacional, estas protecciones incluyen políticas y procedimientos destinados a minimizar la conservación y divulgación de información personal relativa a ciudadanos no estadounidenses, comparables a la protección de que disfrutan los ciudadanos estadounidenses. Además, tal como se ha debatido antes, el régimen de vigilancia en profundidad de los poderes conferidos por el artículo 702 de la FISA es único en el mundo. Por último, las importantes modificaciones realizadas a la ley de inteligencia estadounidense por la Ley de Libertad de EE. UU. y las iniciativas lideradas por la ODNI para la promoción de la transparencia en los servicios de inteligencia mejora enormemente el respeto de la privacidad y de las libertades civiles de todos los individuos, independientemente de su nacionalidad.

Atentamente,

Robert S. Litt

21 de junio de 2016

Sr. Justin S. Antonipillai
Consejero
Departamento de Comercio de los Estados Unidos
1401 Constitution Avenue, N.W.
Washington, DC 20230

Sr. Ted Dean
Subsecretario
Administración del Comercio Internacional
1401 Constitution Avenue, N.W.
Washington, DC 20230

Estimados Sr. Antonipillai y Sr. Dean:

Les escribo para proporcionarles más información sobre la manera en la que los Estados Unidos llevan a cabo la recopilación en bloque de inteligencia de señales. Tal como se explica en la nota 5 de la Directiva de Política Presidencial 28 (PPD-28), la recopilación «en bloque» hace referencia a la adquisición de una cantidad relativamente grande de información o datos de inteligencia de señales en circunstancias en las que los servicios de inteligencia no puedan utilizar un identificador asociado a un criterio de selección específico (como la dirección de correo electrónico o el número de teléfono del criterio de selección) para orientar la recopilación. Sin embargo, esto no implica que este tipo de recopilación sea «masiva» o «indiscriminada». De hecho, la PPD-28 también requiere que «las actividades de inteligencia de señales sean tan específicas como sea posible». Para apoyar esta obligación, los servicios de inteligencia toman medidas para garantizar que, incluso cuando no sea posible utilizar identificadores específicos para orientar la recopilación, los datos que se recopilen sean susceptibles de contener información extranjera que cumpla los requisitos estipulados por los responsables políticos estadounidenses según el proceso explicado en mi carta anterior, y se minimice la cantidad de información no pertinente recopilada.

Por ejemplo, puede solicitarse a los servicios de inteligencia que adquieran inteligencia de señales sobre las actividades de un grupo terrorista que opera en una región de un país de Oriente Medio y que se considere que está planeando ataques contra países de Europa Occidental, pero es posible que los servicios de inteligencia no conozcan nombres, números de teléfono, direcciones de correo electrónico u otros identificadores específicos de las personas asociadas a dicho grupo terrorista. Podríamos decidir que, para detectar a este grupo, se recopilaran las comunicaciones que entran y salen de esa región, para su posterior revisión y análisis, con el fin de identificar las comunicaciones relacionadas con el grupo. De este modo, los servicios de inteligencia intentarían reducir la recopilación tanto como fuera posible. Esto se consideraría una recopilación «en bloque» porque no es factible utilizar discriminantes pero tampoco es una recopilación «en masa» o «indiscrimiada»; es más bien una recopilación focalizada con la mayor precisión posible.

Por tanto, incluso cuando no es posible establecer objetivos mediante el uso de selectores específicos, EE. UU. no recopila todas las comunicaciones de todas las instalaciones de comunicaciones de todas partes del mundo, sino que aplica filtros y otras herramientas técnicas para centrar la recopilación en las instalaciones que pueden contener comunicaciones con valor para la inteligencia internacional. De este modo, las actividades de inteligencia de señales de EE. UU. interceptan únicamente una pequeña parte de las comunicaciones que tienen lugar a través de Internet.

Además, tal como indiqué en mi carta anterior, dado que la recopilación «en bloque» comporta una mayor riesgo de recopilar comunicaciones no pertinentes, la PPD-28 limita el uso que los servicios de inteligencia pueden hacer de la inteligencia de señales recopilada en bloque a seis finalidades específicas. La PPD-28, así como las políticas de organismos que aplican la PPD-28, también establecen restricciones a la conservación y la difusión de la información personal adquirida a través de la inteligencia de señales, independientemente de si la información se ha recopilado en bloque o mediante un criterio de selección y sea cual sea la nacionalidad de las personas.

Así pues, la recopilación «en bloque» de los servicios de inteligencia no es una recopilación «en masa» o «indiscriminada», sino que implica la aplicación de métodos y herramientas para filtrar la recopilación a fin de centrarla en materiales que cumplan los requisitos de inteligencia internacional estipulados por los responsables políticos y, al mismo tiempo, se

minimice la recopilación de información no pertinente y se proporcionen reglas estrictas para proteger la información no pertinente que pueda obtenerse. Las políticas y los procedimientos descritos en esta carta se aplican a todas las recopilaciones en bloque de inteligencia de señales, incluyendo cualquier recopilación en bloque de comunicaciones hacia Europa y desde Europa, sin confirmar ni negar si tal recopilación se produce o no.

Asimismo, usted ha solicitado más información sobre el Consejo de Supervisión de la Privacidad y de las Libertades Civiles (PCLOB) y los inspectores generales, y sus respectivas competencias. El PCLOB es una agencia independiente del poder ejecutivo. El Consejo es bipartidista y está formado por cinco miembros que son nombrados por el presidente y confirmados por el Senado ([1]). Cada miembro del Consejo tiene un mandato de seis años. Los miembros y el personal del Consejo reciben las autorizaciones de seguridad adecuadas para que puedan llevar a cabo plenamente sus funciones y responsabilidades legales ([2]).

La misión del PCLOB es garantizar el equilibrio entre las actividades del Gobierno Federal para la prevención del terrorismo y la necesidad de proteger la privacidad y las libertades civiles. El Consejo tiene dos responsabilidades fundamentales: la supervisión y el asesoramiento. El PCLOB establece su propio plan de trabajo y determina qué actividades de supervisión o asesoramiento desea llevar a cabo.

En su función de *supervisión*, el PCLOB revisa y analiza las acciones que efectúa el poder ejecutivo para proteger a la nación contra el terrorismo, asegurando que la necesidad de tales acciones mantenga el equilibrio con la necesidad de proteger la privacidad y las libertades civiles. ([3]) La supervisión que el PCLOB ha finalizado más recientemente se ha centrado en los programas de vigilancia aplicados conforme al artículo 702 de la FISA ([4]). En la actualidad está llevando a cabo una revisión de las actividades de inteligencia realizadas con arreglo a la Orden Ejecutiva 12333 ([5]).

En su función de *asesoramiento*, el PCLOB garantiza que los aspectos relativos a la libertad se tengan debidamente en cuenta en la elaboración y la aplicación de las leyes, los reglamentos y las políticas relacionadas con las tareas de protección de la nación contra el terrorismo ([6]).

Para llevar a cabo su misión, el Consejo está legalmente autorizado a tener acceso a todos los registros, informes, auditorías, revisiones, documentos, papeles y recomendaciones relevantes de las agencias, así como a cualquier otro material pertinente, incluyendo información clasificada de conformidad con la ley ([7]). Además, el Consejo puede entrevistar, tomar declaración o tomar testimonio público a cualquier funcionario o empleado del poder ejecutivo ([8]). Asimismo, el Consejo puede solicitar por escrito que el Fiscal General, en nombre del Consejo, emita citaciones que obliguen a partes externas al poder ejecutivo a proporcionar información pertinente ([9]).

Finalmente, el PCLOB está sujeto a los requisitos legales de transparencia pública. Esto incluye mantener al público informado de sus actividades mediante la celebración de audiencias públicas y la publicación de sus informes, en la medida que ello sea compatible con la protección de la información clasificada ([10]). Además, el PCLOB debe informar de la negativa de una agencia del poder ejecutivo a seguir su asesoramiento.

Los inspectores generales (IG) de los servicios de inteligencia realizan auditorías, inspecciones y revisiones de los programas y actividades de los servicios de inteligencia para identificar y abordar los riesgos sistémicos, las vulnerabilidades y las deficiencias. Además, los IG se encargan de investigar las reclamaciones o información de acusaciones de

([1]) USC, título 42, artículo 2000ee(a), (h).
([2]) USC, título 42, artículo 2000ee(k).
([3]) USC, título 42, artículo 2000ee(d)(2).
([4]) Véase, en general, https://www.pclob.gov/library.html#oversightreports
([5]) Véase, en general, https://www.pclob.gov/events/2015/may13.html
([6]) USC, título 42, artículo 2000ee(d)(1); véase también PCLOB Advisory Function Policy and Procedure, Policy 2015-004, disponible en: https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf
([7]) USC, título 42, artículo 2000ee(g)(1)(A).
([8]) USC, título 42, artículo 2000ee(g)(1)(B).
([9]) USC, título 42, artículo 2000ee(g)(1)(D).
([10]) USC, título 42, artículo 2000eee(f).

incumplimientos de las leyes, las normas o los reglamentos, así como su gestión indebida; del despilfarro de fondos; del abuso de autoridad o de un peligro sustancial y específico para la salud y la seguridad públicas en los programas y actividades de los servicios de inteligencia. La independencia del IG es un elemento fundamental para la objetividad y la integridad de todos los informes, resultados y recomendaciones. Algunos de los elementos más esenciales para el mantenimiento de la independencia del IG son el nombramiento y el proceso de destitución del IG; la separación de las autoridades operativas, presupuestarias y de personal; y los requisitos de doble notificación a los directores de las agencias del poder ejecutivo y al Congreso.

El Congreso creó una oficina del IG independiente en cada agencia del poder ejecutivo, incluyendo todos los elementos de los servicios de inteligencia. ([1]) Con la aprobación de la Ley de Autorización de Inteligencia del Ejercicio Fiscal 2015, casi todos los IG que realizan supervisión de un elemento de los servicios de inteligencia son nombrados por el presidente y confirmados por el Senado, incluyendo el Departamento de Justicia, la Agencia Central de Inteligencia, la Agencia de Seguridad Nacional y los servicios de inteligencia. ([2]) Además, estos IG son funcionarios permanentes y no partidistas que solo pueden ser destituidos por el presidente. Aunque la Constitución de EE. UU. otorga al presidente la competencia para destituir a los IG, esta competencia rara vez se ha ejercido y requiere que el presidente envíe al Congreso una justificación por escrito 30 días antes de la destitución de un IG ([3]). Este proceso de nombramiento del IG asegura que no haya influencias indebidas por parte de funcionarios del poder ejecutivo en la selección, el nombramiento o la destitución de un IG.

En segundo lugar, los IG tienen importantes competencias legales para realizar auditorías, investigaciones y revisiones de los programas y las operaciones del poder ejecutivo. Además de las investigaciones de supervisión y de las revisiones exigidas por ley, los IG tienen una amplia capacidad para ejercer autoridad de supervisión en la revisión de los programas y actividades que elijan ([4]). En el ejercicio de esta autoridad, la ley asegura que los IG dispongan de recursos independientes para llevar a cabo sus responsabilidades, incluyendo la autoridad para contratar a su propio personal y documentar por separado sus solicitudes presupuestarias al Congreso ([5]). La ley garantiza a los IG el acceso a la información necesaria para llevar a cabo sus responsabilidades. Esto incluye la capacidad de acceder directamente a todos los registros de las agencias y a la información que detalla los programas y operaciones de las agencias, independientemente de la clasificación; la autoridad sobre información y documentos de citaciones; y la autoridad para tomar juramento ([6]). En casos excepcionales, el director de una agencia del poder ejecutivo podrá prohibir la actividad de un IG cuando, por ejemplo, una auditoría o investigación de un IG pueda perjudicar significativamente los intereses estadounidenses en materia de seguridad nacional. Asimismo, el ejercicio de esta competencia es extremadamente inusual y requiere que el director de la agencia notifique al Congreso en un plazo de 30 días las razones para el ejercicio de la misma ([7]). De hecho, el director de inteligencia nacional no ha aplicado nunca esta competencia de limitación a las actividades de ningún IG.

En tercer lugar, los IG tienen la responsabilidad de mantener completa y puntualmente informados a los directores de las agencias del poder ejecutivo y al Congreso mediante informes de fraude y otros problemas graves, usos indebidos y deficiencias relativos a los programas y actividades del poder ejecutivo ([8]). El doble informe refuerza la independencia del IG aportando transparencia al proceso de supervisión del IG y ofreciendo a los directores de las agencias la oportunidad para poner en práctica las recomendaciones del IG antes de que el Congreso pueda adoptar medidas legislativas. Por ejemplo, los IG están legalmente obligados a elaborar informes semestrales que describan este tipo de problemas, así como las acciones correctoras aplicadas hasta la fecha ([9]). Las agencias del poder ejecutivo tienen en cuenta seriamente los resultados y las recomendaciones de los IG y, a menudo, los IG pueden incluir la aceptación y la

([1]) Artículos 2 y 4 de la Ley relativa a los inspectores generales (*Inspector General Act*) de 1978, y sus enmiendas; artículo 103H(b) y (e) de la Ley de Seguridad Nacional (National Security Act) de 1947, y sus enmiendas; artículo 17(a) de la Ley relativa a la Agencia Central de Inteligencia (en adelante, «Central Intelligence Act»).

([2]) Véase Pub. L. n.º 113-293, 128 Stat. 3990, (19 de diciembre de 2014). Solo los IG de la Agencia de Inteligencia de Defensa y de la Agencia Nacional de Inteligencia Geoespacial no son nombrados por el presidente; sin embargo, el IG del Departamento de Defensa y el IG de los servicios de inteligencia tienen jurisdicción concurrente sobre estas agencias.

([3]) Artículo 3 de la Ley IG de 1978, y sus enmiendas; artículo 103H(c) de la Ley de Seguridad Nacional; y artículo 17(b) de la Central Intelligence Act.

([4]) Véanse los artículos 4(a) y 6(a)(2) de la Ley IG; artículo 103H(e) y (g)(2)(A) de la Ley de Seguridad Nacional de 1947; artículo 17(a) y (c) de la Central Intelligence Act.

([5]) Artículos 3(d), 6(a)(7) y 6(f) de la Ley IG; artículo 103H(d), (i), (j) y (m) de la Ley de Seguridad Nacional; artículos 17(e)(7) y (f) de la Central Intelligence Act.

([6]) Artículo 6(a)(1), (3), (4), (5) y (6) de la Ley IG; artículo 103H(g)(2) de la Ley de Seguridad Nacional; artículo 17(e)(1), (2), (4) y (5) de la Ley IG;

([7]) Véanse, por ejemplo, los artículos 8(b) y 8E(a) de la Ley IG; artículo 103H(f) de la Ley de Seguridad Nacional; artículo 17(b) de la Central Intelligence Act.

([8]) Artículo 4, letra a), punto 5, de la Ley IG; artículo 103H(a)(b)(3) y (4) de la Ley de Seguridad Nacional; artículo 17(a)(2) y (4) de la Central Intelligence Act.

([9]) Artículo 2(3), 4(a) y 5 de la Ley IG; artículo 103H(k) de la Ley de Seguridad Nacional; artículo 17(d) de la Central Intelligence Act. El inspector general del Departamento de Justicia publica en internet los informes que hace públicos, que están disponibles en: http://oig.justice.gov/reports/all.htm. Asimismo, el inspector general de los servicios de inteligencia publica sus informes semestrales en https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig

aplicación de sus recomendaciones por parte de las agencias en dichos informes y en otros informes presentados al Congreso y, a veces, al público ([1]). Además de esta estructura de doble informe de los IG, los IG también son responsables de guiar a los denunciantes del poder ejecutivo hasta los comités de supervisión del Congreso pertinentes para efectuar revelaciones de presunto fraude, despilfarro o uso abusivo en los programas y actividades del poder ejecutivo. Las identidades de los comparecientes están protegidas contra la revelación al poder ejecutivo, que protege a los denunciantes de posibles acciones personales prohibidas o acciones de autorización de seguridad adoptadas en represalia a la información a los IG ([2]). Dado que los denunciantes son a menudo las fuentes de las investigaciones de los IG, la capacidad de notificar sus sospechas al Congreso sin recibir influencia del poder ejecutivo aumenta la eficacia de la supervisión de los IG. Debido a esta independencia, los IG pueden promover la economía, la eficacia y la rendición de cuentas en las agencias del poder ejecutivo con objetividad e integridad.

Finalmente, el Congreso ha creado el Consejo de inspectores generales sobre Integridad y Eficiencia. Este Consejo, entre otras cosas, desarrolla normas de los IG para auditorías, investigaciones y revisiones; promueve la formación; y tiene la competencia para revisar las alegaciones de mala conducta de los IG, lo que sirve como mecanismo de vigilancia de los IG, quienes tienen la responsabilidad de vigilar a todos los demás ([3]).

Espero que esta información le resulte de utilidad.

Atentamente,
Robert S. Litt
Director Jurídico

([1]) Artículos 2(3), 4(a) y 5 de la Ley IG; artículo 103H(k) de la Ley de Seguridad Nacional; artículo 17(d) de la Central Intelligence Act. El inspector general del Departamento de Justicia publica en Internet los informes que hace públicos, que están disponibles en: http://oig.justice.gov/reports/all.htm. Asimismo, el inspector general de los servicios de inteligencia publica sus informes semestrales en https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig

([2]) Artículo 7 de la Ley IG; artículo 103H(g)(3) de la Ley de Seguridad Nacional; artículo 17(e)(3) de la Central Intelligence Act.

([3]) Artículo 11 de la Ley IG.

ANEXO VII

Carta del Asistente del Fiscal General y Consejero de Asuntos Internacionales, Bruce Swartz, Departamento estadounidense de Justicia

19 de febrero de 2016

Sr. Justin S. Antonipillai
Consejero
Departamento de Comercio de los Estados Unidos
1401 Constitution Ave., NW
Washington, DC 20230

Sr. Ted Dean
Subsecretario
Administración del Comercio Internacional
1401 Constitution Ave., NW
Washington, DC 20230

Estimado Sr. Antonipillai y Sr. Dean:

Esta carta ofrece una breve visión general de las principales herramientas de investigación utilizadas para la obtención de datos comerciales y otra información de registros de empresas en los Estados Unidos a efectos de la aplicación del Derecho penal o en aras del interés público (civil y reglamentario), incluidas las limitaciones de acceso que acompañan a estas competencias ([1]). Estos procedimientos legales no son discriminatorios, en la medida en que se utilizan para obtener información de empresas de los Estados Unidos, en particular las empresas que se autocertifican a través del marco del Escudo de la privacidad UE-EE. UU., independientemente de la nacionalidad del interesado. Además, las empresas que sean objeto de un tratamiento legal de sus datos en los Estados Unidos podrán impugnarlo ante un tribunal, tal como se explica a continuación ([2]).

Especial atención con respecto a la incautación de datos por parte de las autoridades públicas es la Cuarta Enmienda de la Constitución de los Estados Unidos que contempla que «no se violará el derecho de las personas a proteger sus personas, casas, documentos y efectos de investigaciones y embargos irrazonables, y no se expedirán Órdenes, salvo que exista una causa razonable, respaldada por un juramento o afirmación, y que describa en particular el lugar a ser investigado y las personas u objetos a embargar». IV enmienda de la Const. IV. Tal como declaró el Tribunal Supremo de los Estados Unidos en el caso Berger v. Estado de Nueva York, «el propósito fundamental de esta Enmienda, tal como se reconoce en las innumerables sentencias de este Tribunal, es salvaguardar la privacidad y la seguridad de las personas contra las invasiones arbitrarias por parte de funcionarios públicos». 388 U.S. 41, 53 (1967) [que cita el caso Camara v. Mun. Tribunal de San Francisco, 387 U.S. 523, 528 (1967)]. En las investigaciones nacionales en materia de derecho penal, la Cuarta Enmienda exige generalmente que los agentes con funciones coercitivas obtengan una orden judicial antes de iniciar una investigación. Véase Katz v. Estados Unidos, 389 U.S. 347, 357 (1967). Cuando no se aplique el requisito de la orden, la actividad gubernamental estará sujeta a una prueba de «razonabilidad» prevista en la Cuarta Enmienda. Por consiguiente, la propia Constitución garantiza que el Gobierno de los EE. UU. no tiene un poder ilimitado o arbitrario para la incautación de información privada.

Autoridades con funciones coercitivas en materia penal:

Los fiscales federales, que son funcionarios del Departamento de Justicia (DOJ), y los agentes de investigación federales, incluidos los agentes de la Oficina Federal de Investigación (FBI), un organismo de seguridad del DOJ, podrán exigir la presentación de documentos y otra información de registros a las empresas estadounidenses a efectos de una investigación penal utilizando varios tipos de procesos jurídicos vinculantes, entre ellos citaciones para comparecer ante un

([1]) Esta visión general no describe las herramientas de investigación de la seguridad nacional utilizadas por los organismos con funciones coercitivas en investigaciones sobre terrorismo y otras investigaciones de seguridad nacional, incluidas las cartas de seguridad nacional enviadas para obtener determinada información que figura en los informes de solvencia, estados financieros y registros de transacciones y de abonos electrónicos; véase USC, título 12, artículo 3414; USC, título 15, artículo 1681u; USC, título 15, artículo 1681v; USC, título 18, artículo 2709; y, para la vigilancia electrónica, las órdenes de registro, los registros comerciales y otra recopilación de comunicaciones en virtud de la Ley de Vigilancia de la Inteligencia Exterior; véase USC, título 50, artículo 1801 *et seq*.

([2]) Este documento examina la aplicación de la ley federal y las autoridades reguladoras; las violaciones de la ley estatal son investigadas por los Estados y son juzgadas por tribunales estatales. Las autoridades de aplicación de la ley estatal utilizan las órdenes y las citaciones expedidas en virtud de la ley estatal, básicamente tal como se describe en este documento, pero con la posibilidad de que el proceso legal estatal pueda estar sujeto a unas protecciones proporcionadas por las Constituciones estatales que superen las de la Constitución de EE. UU. Las protecciones de la legislación estatal deben ser como mínimo equivalentes a las de la Constitución de EE. UU., incluida aunque no limitada a la Cuarta Enmienda.

gran jurado, citaciones administrativas y órdenes de investigación, y podrán obtener otras comunicaciones gracias a las competencias penales federales relativas al registro de llamadas y las escuchas telefónicas.

Citaciones del Gran Jurado o del Tribunal: Las citaciones penales se utilizan para respaldar las investigaciones de aplicación de la ley. Un requerimiento del gran jurado es una petición oficial expedida por un gran jurado (generalmente a instancias de un fiscal federal) para apoyar la investigación de un gran jurado en una determinada presunta violación del derecho penal. Los grandes jurados son un órgano de investigación del tribunal compuesto por un juez o un magistrado. El requerimiento podrá exigir el testimonio de una persona en el proceso, la elaboración o presentación de registros comerciales, de la información almacenada electrónicamente o de otros elementos tangibles. La información debe ser relevante para la investigación y el requerimiento no podrá considerarse irrazonable por ser excesivo o por ser opresivo u oneroso. El destinatario podrá presentar una moción para impugnar un requerimiento basado en estos fundamentos. Véase Fed. R. Crim. P. 17. En determinadas circunstancias, podrán utilizarse requerimientos de documentos una vez el caso haya sido procesado por el gran jurado.

Autoridad de requerimiento administrativo: Las autoridades de requerimiento administrativo podrán ejercer investigaciones civiles o penales. En el contexto de la aplicación del derecho penal, son varias las leyes federales que autorizan el uso de citaciones administrativas para la elaboración o presentación de registros comerciales, de información almacenada electrónicamente o de otros elementos tangibles en las investigaciones relacionadas con el fraude en la asistencia sanitaria, el abuso de menores, la protección de los Servicios Secretos, los casos de sustancias controladas y las investigaciones del Fiscal General relacionadas con organismos públicos. En caso de que el Gobierno intente imponer un requerimiento administrativo al tribunal, el destinatario del requerimiento administrativo, al igual que el destinatario de un requerimiento del gran jurado, podrá argumentar la irracionalidad del requerimiento por considerarlo excesivo, opresivo u oneroso.

Órdenes judiciales para registro de llamadas entrantes y salientes: De conformidad con las disposiciones relativas al registro de llamadas entrantes y salientes, los organismos con funciones coercitivas aplicación de la ley podrá obtener una orden judicial para conseguir, en tiempo real, información sobre el marcado, el enrutamiento, el direccionamiento y la señalización de un número de teléfono o de una dirección de correo electrónico tras la certificación de que la información proporcionada es relevante para una investigación criminal pendiente. Véase USC, título 18, artículos 3121-3127. El uso o instalación de un dispositivo tal fuera de la ley es un delito federal.

Ley de Privacidad de las Comunicaciones Electrónicas (ECPA): Existen otras normas que rigen el acceso del Gobierno a la información del abonado, los datos de tráfico y el contenido almacenado de las comunicaciones mantenidos por las compañías de teléfono ISP y otros proveedores externos de servicios, de conformidad con el título II de la ECPA, también llamada Ley de Comunicaciones Almacenadas (SCA), USC, título 18, artículos 2701-2712. La SCA establece un sistema estatutario de derechos de privacidad que limita el acceso del orden público a los datos que van más allá de los requeridos por la ley constitucional a los clientes y abonados de los proveedores de servicios Internet. La SCA ofrece unos mayores niveles de protección de la privacidad en función del intrusismo de la recopilación. Para obtener información del registro de abonados, las direcciones IP, las fechas correspondientes y la información de la facturación, las autoridades judiciales penales deberán obtener un requerimiento. Para la mayoría de la demás información almacenada sin contenido, como los encabezados de los correos electrónicos sin el asunto, el orden público deberá presentar al juez unos hechos concretos que demuestren que la información exigida es relevante y sustancial para una investigación penal en curso. Para obtener el contenido almacenado de las comunicaciones electrónicas, generalmente las autoridades judiciales obtendrán una orden de un juez basada en la existencia de razones para pensar que la cuenta en cuestión contiene pruebas de un delito. La SCA ofrece también responsabilidad civil y sanciones penales.

Órdenes judiciales para la vigilancia de conformidad con la Ley Federal de escuchas telefónicas: Además, el orden público podrá interceptar en tiempo real comunicaciones por cable, orales o electrónicas a efectos de la investigación criminal en virtud de la ley federal de escuchas telefónicas. Véase USC, título 18, artículos 2510-2522. Esta competencia solo se encuentra disponible en virtud de una orden judicial en la que el juez considere, *inter alia*, que existe una causa

probable para creer que la escucha telefónica o la interceptación electrónica proporcionará las pruebas de un delito federal, o el paradero de un fugitivo de la justicia. La ley contempla la responsabilidad civil y sanciones penales para las violaciones de las disposiciones de escuchas telefónicas.

Orden de registro — Regla 41: El orden público podrá registrar físicamente locales en los Estados Unidos cuando así se lo autorice un juez. El orden público deberá demostrar al juez una «causa probable» de que se ha cometido un delito o se va a cometer un delito y que los elementos relacionados con el delito es probable que se encuentren en el lugar especificado por la orden. Esta potestad se utiliza generalmente cuando se requiere un registro físico de un local por parte de la policía debido al peligro de destrucción de las pruebas en caso de entrega de un requerimiento u otra orden a la sociedad. Véase la cuarta enmienda de la Constitución estadounidense (antes descrita con más detalle), Fed. R. Crim. P. 41. El sujeto de una orden de registro podrá intentar anular la orden si es excesiva, abusiva o se ha obtenido incorrectamente y las partes agraviadas con legitimación podrán suprimir cualquier prueba obtenida en un registro ilegal. Véase Mapp v. Ohio, 367 U.S. 643 (1961).

Directrices y políticas del DOJ: Además de estas limitaciones constitucionales, estatutarias y normativas sobre el acceso del Gobierno a los datos, el Fiscal General ha emitido directrices que colocan nuevos límites para el acceso del orden público a los datos, y también contiene protecciones para la privacidad y las libertades civiles. Por ejemplo, la Directrices del Fiscal General para las operaciones de la Oficina Nacional de Investigación (FBI) (septiembre de 2008) (en lo sucesivo, «Directrices del FG para el FBI»), disponibles en http://www.justice.gov/archive/opa/docs/guidelines.pdf, establecen los límites sobre el uso de los medios de investigación para la búsqueda de información relacionada con las investigaciones de delitos federales. Estas directrices exigen que el FBI utilice unos métodos de investigación lo menos invasivos posible, teniendo en cuenta el efecto en la privacidad y en las libertades civiles y el posible daño para la reputación. Además, señalan que «es axiomático que el FBI lleve a cabo investigaciones y otras actividades de una manera legal y responsable que respete la libertad y la privacidad y evite intrusiones innecesarias en las vidas de las personas respetuosas con la ley». *Véanse* las Directrices del FG para el FBI en 5. El FBI ha implantado estas directrices a través de la Guía Nacional de Investigaciones y Operaciones del FBI (DIOG), disponible en https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), un manual exhaustivo que incluye los límites detallados sobre el uso de las herramientas de investigación y una guía para garantizar la protección de las libertades civiles y de la privacidad en todas las investigaciones. Se incluyen otras normas y políticas que prescriben limitaciones a las actividades de investigación de los fiscales federales en el **Manual de los Fiscales de los Estados Unidos** (USAM), también disponible en línea en http://www.justice.gov/usam/united-states-attorneys-manual

Organismos civiles y reglamentarios (Interés Público):

Existen también importantes límites para el acceso civil o reglamentario (por ejemplo, «el interés público») a los datos mantenidos por sociedades estadounidenses. Los organismos con responsabilidades civiles y reglamentarias podrán expedir requerimientos a las sociedades para la obtención de registros comerciales, información almacenada electrónicamente u otros elementos tangibles. Estos organismos están limitados en su ejercicio de requerimientos administrativos o civiles no tan solo por sus estatutos orgánicos, sino también por la revisión judicial independiente de los requerimientos anteriores a la posible ejecución judicial. *Véase, por ejemplo*, Fed. R. Civ. P. 45. Los organismos solo podrán acceder a los datos relevantes para las cuestiones que recaigan dentro de su ámbito de competencia para la regulación. Además, el destinatario de un requerimiento administrativo podrá impugnar la aplicación de un requerimiento ante el tribunal mediante la presentación de pruebas de que el organismo no ha actuado de conformidad con las normas básicas de razonabilidad, tal como se ha mencionado con anterioridad.

Existen otras bases jurídicas para que las sociedades puedan impugnar las solicitudes de datos de los órganos administrativos sobre la base de sus sectores concretos y de los tipos de datos que posean. Por ejemplo, las instituciones financieras podrán impugnar los requerimientos administrativos que contemplen determinados tipos de información como violaciones de la Ley de Secreto Bancario y sus normativas para la implantación. Véase USC, título 31, artículo 5318; 31 C.F.R., parte X. Otras empresas pueden basarse en la Ley sobre Informes de Crédito Justos; véase USC, título 15, artículo 1681b, o numerosas leyes específicas del sector. El uso indebido de la potestad del requerimiento de un organismo puede comportar la responsabilidad del organismo, o la responsabilidad personal de los funcionarios del organismo. Véase, por ejemplo, el Derecho a la Ley de Privacidad Financiera, USC, título 12, artículos 3401-3422. Los tribunales de los Estados Unidos son, por consiguiente, los guardianes contra los requisitos reglamentarios impropios y ofrecen un control independiente de las acciones de los organismos federales.

Por último, cualquier competencia estatutaria que tengan las autoridades administrativas para una incautación física de los registros de una sociedad estadounidense en virtud de un registro administrativo deberá satisfacer los requisitos de la Cuarta Enmienda. Véase See v. Ciudad de Seattle, 387 U.S. 541 (1967).

Conclusión

Todas las actividades de aplicación de la ley y reglamentarias realizadas en los Estados Unidos deben ajustarse a la legislación vigente, incluida la Constitución americana, las leyes, las normas y los reglamentos. Estas actividades deberán cumplir también las políticas aplicables, incluidas las directrices del Fiscal General que rigen las actividades represivas de las autoridades federales. El marco jurídico antes descrito limita la capacidad de los organismos reguladores y con funciones coercitivas estadounidenses para obtener información de empresas estadounidenses, independientemente de que la información se refiera a ciudadanos estadounidenses o a ciudadanos de países extranjeros, y permite el control judicial de las solicitudes de datos efectuadas por el Gobierno en virtud de estas competencias.

Atentamente,

Bruce C. Swartz

Asistente del Fiscal General y Consejero de Asuntos Internacionales