DECISIÓN DE EJECUCIÓN (UE) 2023/1795 DE LA COMISIÓN

de 10 de julio de 2023

relativa a la adecuación del nivel de protección de los datos personales en el Marco de Privacidad de Datos UE-EE. UU. con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

[notificada con el número C(2023) 4745]

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) ([1]), y en particular su artículo 45, apartado 3,

Considerando lo siguiente:

1. INTRODUCCIÓN

(1) El Reglamento (UE) 2016/679 ([2]) establece las normas que regulan la transferencia de datos personales de los responsables o encargados del tratamiento en la Unión a terceros países y organizaciones internacionales, en la medida en que tales transferencias se encuentren comprendidas dentro de su ámbito de aplicación. Las normas sobre las transferencias internacionales de datos se establecen en el capítulo V de dicho Reglamento. Si bien la circulación de datos personales hacia y desde países no pertenecientes a la UE es esencial para la expansión del comercio transfronterizo y la cooperación internacional, el nivel de protección de los datos personales en la Unión no debe verse menoscabado por las transferencias a terceros países u organizaciones internacionales ([3]).

(2) De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, la Comisión puede decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país garantizan un nivel de protección adecuado. En tal caso, la transferencia de datos personales a un tercer país puede realizarse sin necesidad de obtener ninguna otra autorización, de conformidad con lo dispuesto en el artículo 45, apartado 1, y el considerando 103 de dicho Reglamento.

(3) Tal como se especifica en el artículo 45, apartado 2, del Reglamento (UE) 2016/679, la adopción de una decisión de adecuación ha de basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, que contemple tanto las normas aplicables a los importadores de datos como las limitaciones y garantías en lo que respecta al acceso a los datos personales por parte de las autoridades públicas. En su evaluación, la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección «equivalente en lo esencial» al ofrecido en la Unión [considerando 104 del Reglamento (UE) 2016/679], con arreglo a la normativa de la Unión, en concreto el Reglamento (UE) 2016/679, así como a la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, el «TJUE») ([4]).

([1]) DO L 119 de 4.5.2016, p. 1.
([2]) Se incluye en el anexo VIII, para facilitar la lectura, una lista de las abreviaciones utilizadas en la presente Decisión.
([3]) Véase el considerando 101 del Reglamento (UE) 2016/679.
([4]) Véase la reciente sentencia en el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximillian Schrems («Schrems II»), ECLI:EU:C:2020:559.

(4) Como ya aclaró el TJUE en su sentencia de 6 de octubre de 2015, en el asunto C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems») ([5]), esta exigencia no supone tener que garantizar un nivel de protección idéntico. En particular, los medios de que se sirve el tercer país en cuestión para la protección de los datos personales pueden ser diferentes de los aplicados en la Unión, siempre que, en la práctica, sean eficaces para garantizar un nivel de protección adecuado ([6]). Por consiguiente, el principio de adecuación no exige que se reproduzcan al pie de la letra las normas de la Unión, sino que el criterio radica en si, a través de la esencia de los derechos de privacidad y su aplicación, fuerza ejecutiva y supervisión efectivas, el ordenamiento en cuestión ofrece, en su conjunto, el nivel de protección exigido ([7]). Además, según dicha sentencia, al aplicar este criterio, la Comisión debe evaluar, en particular, si el marco jurídico del tercer país en cuestión establece reglas destinadas a limitar las injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional, y proporciona una protección jurídica eficaz contra injerencias de esa naturaleza ([8]). Las Referencias sobre adecuación del Comité Europeo de Protección de Datos, que pretenden aclarar este criterio, también proporcionan claves interpretativas a este respecto ([9]).

(5) El criterio aplicable con respecto a dicha injerencia en los derechos fundamentales a la privacidad y a la protección de datos fue aclarado con mayor detalle por el TJUE en su sentencia de 16 de julio de 2020, en el asunto C-311/18, Data Protection Commissioner/Facebook Ireland Ltd y Maximillian Schrems («Schrems II»), por la que se invalidó la Decisión de Ejecución (UE) 2016/1250 de la Comisión ([10]), sobre el anterior marco transatlántico aplicable a la circulación de datos, el Escudo de la privacidad UE-EE. UU. (en lo sucesivo, «Escudo de la privacidad»). El TJUE consideró que las limitaciones de la protección de los datos personales que se derivan de la normativa interna de los Estados Unidos relativa al acceso y la utilización, por las autoridades estadounidenses, de los datos transferidos desde la Unión a los Estados Unidos con fines de seguridad nacional no están reguladas conforme a exigencias sustancialmente equivalentes a las requeridas en el Derecho de la UE, en lo que respecta a la necesidad y proporcionalidad de tales injerencias en el derecho a la protección de datos ([11]). También interpretó que no cabía interponer recurso ante un órgano que ofrezca a las personas cuyos datos se transfieren a los Estados Unidos garantías sustancialmente equivalentes a las exigidas en el artículo 47 de la Carta, sobre el derecho a la tutela judicial efectiva ([12]).

(6) A raíz de la sentencia Schrems II, la Comisión entabló negociaciones con los Estados Unidos para poder adoptar una nueva decisión de adecuación que cumpliera los requisitos del artículo 45, apartado 2, del Reglamento (UE) 2016/679, conforme a la interpretación del TJUE. Como resultado de estas negociaciones, el 7 de octubre de 2022 se aprobó en los Estados Unidos (en lo sucesivo, «EE. UU.») el Decreto Presidencial n.º 14086, titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos» (Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities') (en lo sucesivo, «Decreto Presidencial n.º 14086»), al que complementa el Reglamento sobre el Tribunal de Recurso en Materia de Protección de Datos (Regulation on the Data Protection Review Court) (en lo sucesivo, «Reglamento sobre el Tribunal de Recurso»), aprobado por el secretario de Justicia (Attorney General) de los EE. UU. ([13]). Además, se ha actualizado el marco aplicable a las entidades mercantiles que traten datos transferidos desde la Unión en virtud de la presente Decisión (en lo sucesivo, «Marco de Privacidad de Datos UE-EE. UU.»).

(7) La Comisión ha analizado con detenimiento la normativa y las prácticas vigentes en los EE. UU. y, en particular, el Decreto Presidencial n.º 14086 y el Reglamento sobre el Tribunal de Recurso. Basándose en las averiguaciones reflejadas en los considerandos 9 a 200, la Comisión llega a la conclusión de que los EE. UU. garantizan un nivel de protección adecuado de los datos personales que los responsables o encargados del tratamiento en la UE ([14]) transfieran con arreglo al Marco de Privacidad de Datos UE-EE. UU. a entidades certificadas estadounidenses.

([5]) Asunto C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems»), ECLI:EU:C:2015:650, apartado 73.

([6]) Schrems, apartado 74.

([7]) Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo, «Intercambio y protección de los datos personales en un mundo globalizado», COM(2017) 7, de 10.1.2017, sección 3.1, pp. 6 y 7.

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

([9]) Referencias sobre adecuación, Comité Europeo de Protección de Datos, WP 254, rev. 01, disponible en el siguiente enlace: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. (DO L 207 de 1.8.2016, p. 1).

([11]) Schrems II, apartado 185.

([12]) Schrems II, apartado 197.

([13]) Título 28, parte 302, del Código de Reglamentos Federales (Code of Federal Regulations).

([14]) La presente Decisión es pertinente a efectos del EEE. El Acuerdo sobre el Espacio Económico Europeo dispone la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE (Islandia, Liechtenstein y Noruega). La Decisión del Comité Mixto por la que se incorpora el Reglamento (UE) 2016/679 al anexo XI del Acuerdo EEE fue adoptada por el Comité Mixto del EEE el 6 de julio de 2018 y entró en vigor el 20 de julio de 2018. El Reglamento está cubierto pues por dicho Acuerdo. A efectos de la presente Decisión, debe entenderse, por tanto, que las referencias a la UE y a los Estados miembros de la UE también incluyen a los Estados del EEE.

(8) La presente Decisión tiene como efecto que las transferencias de datos personales que los responsables y encargados del tratamiento en la UE ([15]) realicen a entidades certificadas estadounidenses no requieran ningún tipo de autorización. No tiene ninguna incidencia en la aplicación directa del Reglamento (UE) 2016/679 a dichas entidades cuando se cumplan las condiciones relativas al ámbito territorial de dicho Reglamento, establecidas en su artículo 3.

2. MARCO DE PRIVACIDAD DE DATOS UE-EE. UU.

2.1. Ámbito de aplicación objetivo y subjetivo

2.1.1. *Entidades certificadas*

(9) El Marco de Privacidad de Datos UE-EE. UU. se basa en un sistema de certificación por el que las entidades estadounidenses se comprometen a cumplir una serie de principios, a saber, los principios del Marco de Privacidad de Datos UE-EE. UU. y los principios complementarios (en conjunto, «los principios en materia de privacidad»), aprobados por el Departamento de Comercio (Department of Commerce) de los EE. UU. y recogidos en el anexo I de la presente Decisión ([16]). Para recibir la certificación del Marco de Privacidad de Datos UE-EE. UU., las entidades deben someterse a las competencias de investigación y ejecución forzosa de la Comisión Federal de Comercio (Federal Trade Commission) o del Departamento de Transporte (Department of Transportation) de los EE. UU. ([17]). Los principios en materia de privacidad son de aplicación inmediatamente después de la certificación. Como se explica con mayor detalle en los considerandos 48 a 52, las entidades que participen en el Marco de Privacidad de Datos UE-EE. UU. tienen que revalidar cada año la certificación de su cumplimiento de los principios ([18]).

2.1.2. *Definición de «datos personales» y concepto de «responsable» y de «agente»*

(10) La protección concedida en el Marco de Privacidad de Datos UE-EE. UU. se extiende a todos los datos personales transferidos desde la UE a las entidades estadounidenses a las que el Departamento de Comercio de los EE. UU. haya concedido el certificado de que cumplen los principios en materia de privacidad, con excepción de los datos recogidos para su publicación, retransmisión u otras formas de comunicación pública de material periodístico, así como la información contenida en material de archivo publicado previamente a partir de archivos de medios de comunicación ([19]). Por lo tanto, dicha información no puede transferirse con arreglo al Marco de Privacidad de Datos UE-EE. UU.

(11) Los principios en materia de privacidad definen los datos personales y la información personal de la misma manera que el Reglamento (UE) 2016/679, es decir, como «los datos sobre un particular identificado o identificable a los que es de aplicación el RGPD, que los recibe de la UE una entidad estadounidense y que quedan registrados de alguna forma» ([20]). En consecuencia, también están comprendidos los datos de investigación seudonimizados (o «codificados»), incluso cuando la clave de ese código no se comparte con la entidad estadounidense receptora ([21]). De modo análogo, el tratamiento se define como «cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación, difusión y supresión o destrucción» ([22]).

(12) El Marco de Privacidad de Datos UE-EE. UU. es de aplicación a las entidades estadounidenses que se consideran responsables (es decir, persona física o jurídica que, sola o junto con otros, determina las finalidades y medios del tratamiento de datos personales) ([23]) o encargadas (es decir, agente que actúa por cuenta del responsable del tratamiento) del tratamiento ([24]). Los encargados estadounidenses deben estar obligados contractualmente a actuar

([15]) La presente Decisión no afecta a las obligaciones del Reglamento (UE) 2016/679 que se aplican a las entidades (responsables y encargados del tratamiento) de la Unión que transfieren los datos, por ejemplo, en materia de limitación de la finalidad, minimización de los datos, transparencia y seguridad de los datos [véase también el artículo 44 del Reglamento (UE) 2016/679].

([16]) Véase a este respecto la sentencia Schrems, apartado 81, en la que el Tribunal de Justicia confirmó que un sistema de autocertificación puede garantizar un nivel de protección adecuado.

([17]) Anexo I, sección I, punto 2. La Comisión Federal de Comercio tiene amplias competencias sobre las actividades comerciales (con contadas excepciones), en particular relacionadas con los bancos, las aerolíneas, el sector de los seguros y las actividades de mero transportista de las empresas de servicios de telecomunicaciones (aunque la resolución de la Corte de Apelaciones del Noveno Distrito de los EE. UU. de 26 de febrero de 2018 en el asunto FTC c. AT&T ha confirmado que la Comisión Federal de Comercio tiene competencia sobre las actividades de dichas entidades distintas de las de mero transportista). Véase también el anexo IV, nota a pie de página 2. El Departamento de Transporte tiene competencias de ejecución respecto de las aerolíneas y los agentes de venta de billetes (respecto del transporte aéreo); véase el anexo V, sección A.

([18]) Anexo I, sección III, punto 6.

([19]) Anexo I, sección III, punto 2.

([20]) Anexo I, sección I, punto 8, letra a.

([21]) Anexo I, sección III, punto 14, letra g.

([22]) Anexo I, sección I, punto 8, letra b.

([23]) Anexo I, sección I, punto 8, letra c.

([24]) Véase el anexo I, sección II, punto 2, letra b, punto 3, letra b, y punto 7, letra d, donde se aclara que los agentes actúan por cuenta del responsable del tratamiento, con sujeción a las instrucciones de este último y con arreglo a obligaciones contractuales específicas.

únicamente siguiendo instrucciones del responsable del tratamiento de la UE y a ayudar a este último a responder a los particulares que ejerzan los derechos que le reconocen los principios en materia de privacidad ([25]). Además, en caso de subtratamiento, el encargado del tratamiento debe celebrar un contrato con el subencargado por el que se garantice el mismo nivel de protección que el conferido por los principios en materia de privacidad y tomar medidas para asegurar su cumplimiento ([26]).

2.2. **Principios del Marco de Privacidad de Datos UE-EE. UU.**

2.2.1. ***Limitación de la finalidad y opción***

(13) Los datos personales deben tratarse de manera lícita y leal. Deben recogerse para una finalidad específica y, posteriormente, solo deben utilizarse en la medida en que ello no sea incompatible con la finalidad del tratamiento.

(14) En el Marco de Privacidad de Datos UE-EE. UU., esto se garantiza por medio de varios principios. En primer lugar, en virtud del principio de integridad de los datos y limitación de la finalidad, al igual que en virtud del artículo 5, apartado 1, letra b), del Reglamento (UE) 2016/679, las entidades no pueden tratar datos personales de manera incompatible con la finalidad para la que fueron recogidos inicialmente o que autorizó posteriormente el interesado ([27]).

(15) En segundo lugar, antes de utilizar datos personales con una nueva finalidad que sea sustancialmente distinta de la finalidad original, pero aun así compatible con esta, o de comunicarlos a un tercero, la entidad debe ofrecer a los interesados la oportunidad de oponerse, de conformidad con el principio de opción ([28]), a través de un mecanismo claro, bien visible e inmediatamente utilizable. Es importante recalcar que dicho principio no deja sin efecto la prohibición expresa de realizar operaciones de tratamiento incompatibles ([29]).

([25]) Anexo I, sección III, punto 10, letra a. Véanse también las instrucciones elaboradas por el Departamento de Comercio, con la colaboración del Comité Europeo de Protección de Datos, para el Escudo de la privacidad, en las que se aclaraban las obligaciones de los encargados del tratamiento estadounidenses que recibiesen datos personales de la UE en ese marco. Dado que este régimen no ha variado, las instrucciones y las respuestas a las preguntas frecuentes siguen siendo válidas para el Marco de Privacidad de Datos UE-EE. UU. (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Anexo I, sección II, punto 3, letra b.

([27]) Anexo I, sección II, punto 5, letra a. Pueden ser finalidades compatibles una auditoría, la prevención del fraude u otras finalidades que se ajusten a las expectativas de una persona razonable dadas las circunstancias de la recogida de los datos (véase el anexo I, nota a pie de página 6).

([28]) Anexo I, sección II, punto 2, letra a. Este régimen no es de aplicación cuando la entidad transfiera datos personales a un encargado que actúe por cuenta de esta y siguiendo sus instrucciones (anexo I, sección II, punto 2, letra b). Ahora bien, en este supuesto la entidad debe haber celebrado un contrato y garantizar el cumplimiento del principio de responsabilidad proactiva por las transferencias ulteriores, tal como se describe pormenorizadamente en el considerando 43. Además, el principio de opción (así como el principio de notificación) puede limitarse cuando se traten datos personales en ejercicio de la diligencia debida (como parte de una posible fusión o absorción) o en procesos de auditoría, en la medida y durante el tiempo que sea necesario para cumplir obligaciones legales o de interés público o en la medida y durante el tiempo que la aplicación de dichos principios perjudique los intereses legítimos de la entidad en el contexto específico de las comprobaciones que exige la diligencia debida o los procesos de auditoría (anexo I, sección III, punto 4). El principio complementario n.º 15 (anexo I, sección III, punto 15, letras a y b) también contempla una excepción al principio de opción (así como a los principios de notificación y de responsabilidad proactiva por las transferencias ulteriores) respecto de los datos personales procedentes de fuentes de acceso público (a menos que el exportador de datos de la UE indique que la información está sujeta a limitaciones que impongan la aplicación de dichos principios) o de los datos personales extraídos de registros de consulta pública (siempre que no se combinen con información de registros no públicos y se cumplan las condiciones para la consulta). Del mismo modo, el principio complementario n.º 14 (anexo I, sección III, punto 14, letra f) establece una excepción al principio de opción (así como a los principios de notificación y de responsabilidad proactiva por las transferencias ulteriores) respecto del tratamiento de datos personales por parte de productos farmacéuticos y sanitarios en relación con las actividades de control de la eficacia y la seguridad de los productos, en la medida en que el cumplimiento de dichos principios afecte al cumplimiento de los requisitos regulatorios.

([29]) Esta regla se aplica a todas las transferencias de datos en el Marco de Privacidad de Datos UE-EE. UU., incluso cuando estas se refieran a los datos recogidos en el marco de relaciones laborales. Si bien las entidades estadounidenses certificadas pueden, en principio, utilizar los datos de recursos humanos para finalidades distintas no laborales (por ejemplo, determinadas comunicaciones publicitarias), deben respetar la prohibición de realizar operaciones de tratamiento incompatibles y, además, únicamente pueden utilizarlos de conformidad con los principios de notificación y opción. Excepcionalmente, las entidades pueden utilizar los datos personales para una finalidad adicional compatible sin notificarlo ni ofrecer el derecho de opción, pero solo en la medida necesaria y durante el tiempo necesario para evitar comprometer la capacidad de la entidad para tomar decisiones de ascenso, de nombramiento o laborales de otro tipo (véase el anexo I, sección III, punto 9, letra b, inciso iv). La prohibición de las entidades estadounidenses de emprender medidas punitivas contra el empleado por ejercer este derecho de opción, en particular cualquier limitación de las oportunidades laborales, garantiza que, a pesar de la relación de subordinación y dependencia inherente, el empleado esté libre de presión y, por tanto, tenga auténtica libertad de elección. Véase el anexo I, sección III, punto 9, letra b, inciso i.

2.2.2. ***Tratamiento de categorías especiales de datos personales***

(16) Deben aplicarse garantías específicas cuando se traten «categorías especiales» de datos.

(17) De conformidad con el principio de opción, se aplican garantías específicas al tratamiento de «información delicada», es decir, datos personales que indiquen el estado de salud, el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical, la información sobre la vida sexual del particular o cualquier otra información recibida de un tercero y que este considere y trate como delicada ([30]). Esto significa que cualquier dato que se considere delicado con arreglo a la normativa de la Unión en materia de protección de datos (especialmente los datos sobre la orientación sexual, los datos genéticos y los datos biométricos) debe ser tratado como delicado en el Marco de Privacidad de Datos UE-EE. UU. por las entidades certificadas.

(18) Como norma general, las entidades deben obtener el consentimiento expreso de los particulares para utilizar información delicada con finalidades distintas de la finalidad para la que fue recogida inicialmente o que autorizó posteriormente el particular (con su consentimiento expreso), o para comunicarla a terceros ([31]).

(19) No es necesario obtener dicho consentimiento en supuestos específicos, comparables a las excepciones contempladas en la normativa de la Unión en materia de protección de datos, por ejemplo, cuando el tratamiento de datos delicados sea de interés vital para una persona o necesario para un proceso judicial o para proporcionar cuidados médicos o establecer un diagnóstico ([32]).

2.2.3. ***Seguridad, minimización y exactitud de los datos***

(20) Los datos deben ser exactos y, si fuera necesario, estar actualizados. También deben ser adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados y, en principio, no deben conservarse más tiempo del necesario en relación con los fines para los que se tratan los datos personales.

(21) En virtud del principio de integridad de los datos y limitación de la finalidad ([33]), los datos personales deben limitarse a lo pertinente para la finalidad del tratamiento. Además, las entidades deben, en la medida necesaria para lograr dicha finalidad del tratamiento, tomar medidas razonables para que los datos personales sean fiables en relación con el uso previsto, exactos y actuales y estén completos.

(22) Por otra parte, la información personal puede conservarse de forma que identifique o haga identificable al particular (esto es, en forma de datos personales) ([34]) únicamente en la medida en que ello contribuya a la finalidad para la que fue recogida inicialmente o que autorizó posteriormente el particular de conformidad con el principio de opción. Esta obligación no impide a las entidades continuar tratando información personal por períodos más largos, pero únicamente por el tiempo y en la medida en que dicho tratamiento contribuya razonablemente a una o varias de las finalidades siguientes, comparables a las excepciones contempladas en la normativa de la Unión en materia de protección de datos: archivamiento en interés público, periodismo, literatura y arte, investigación científica e histórica y análisis estadístico ([35]). Cuando los datos personales se conserven para una de estas finalidades, su tratamiento queda sujeto a las garantías que establecen los principios en materia de privacidad ([36]).

(23) Los datos personales también deben ser tratados de tal manera que se garantice su seguridad, especialmente la protección contra su tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental. A tal fin, los responsables y encargados del tratamiento deben tomar las medidas técnicas u organizativas apropiadas para proteger los datos personales frente a posibles amenazas. Estas medidas deben evaluarse teniendo en cuenta el estado de la técnica, los costes conexos y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos de los particulares.

([30]) Anexo I, sección II, punto 2, letra c.
([31]) Anexo I, sección II, punto 2, letra c.
([32]) Anexo I, sección III, punto 1.
([33]) Anexo I, sección II, punto 5.
([34]) Véase el anexo I, nota a pie de página 7, en la que se aclara que una persona se considera «identificable» siempre que una entidad o un tercero pueda identificarla razonablemente, teniendo en cuenta los medios de identificación que es razonablemente probable que se utilicen (valorando, entre otras cosas, el coste y el tiempo necesarios para la identificación y la tecnología disponible en el momento del tratamiento).
([35]) Anexo I, sección II, punto 5, letra b.
([36]) *Véase la nota anterior.*

(24) En el Marco de Privacidad de Datos UE-EE. UU., esto está garantizado por el principio de seguridad, que exige, al igual que el artículo 32 del Reglamento (UE) 2016/679, que se tomen medidas de seguridad razonables y apropiadas, teniendo en cuenta los riesgos que entraña el tratamiento y la naturaleza de los datos ([37]).

2.2.4. ***Transparencia***

(25) Los interesados deben ser informados de las principales características del tratamiento de sus datos personales.

(26) Esto se garantiza con el principio de notificación ([38]), que, al igual que las exigencias de transparencia del Reglamento (UE) 2016/679, obliga a las entidades a informar a los interesados sobre, entre otros aspectos, i) la participación de la entidad en el Marco de Privacidad de Datos UE-EE. UU., ii) el tipo de datos recogidos, iii) la finalidad del tratamiento, iv) el tipo de terceros, o su identidad, a los que pueden comunicarse los datos personales y las finalidades para hacerlo, v) sus derechos individuales, vi) cómo ponerse en contacto con la entidad y vii) las vías de reparación disponibles.

(27) Esta notificación debe hacerse en un lenguaje claro y evidente cuando se solicite por primera vez a los particulares que proporcionen los datos personales o tan pronto como sea posible después, pero, en cualquier caso, antes de que los datos se utilicen para una finalidad sustancialmente distinta (pero compatible) de aquella para la que fueron recogidos o antes de que se comuniquen a terceros ([39]).

(28) Además, las entidades deben publicar sus directrices en materia privacidad, que deben ajustarse a los principios en materia de privacidad (o, en el caso de los datos de recursos humanos, ponerlas a disposición fácil de los particulares), y proporcionar enlaces al sitio web del Departamento de Comercio (con información pormenorizada sobre la certificación, los derechos de los interesados y las vías de impugnación disponibles), a la lista del Marco de Privacidad de Datos (lista de entidades participantes) y al sitio web de un organismo alternativo de resolución de controversias adecuado ([40]).

2.2.5. ***Derechos individuales***

(29) Los interesados deben tener ciertos derechos que puedan hacer valer ante el responsable o el encargado del tratamiento, en concreto el derecho de acceso a los datos, el derecho a oponerse al tratamiento y el derecho de rectificación o supresión de datos.

(30) El principio de acceso ([41]) del Marco de Privacidad de Datos UE-EE. UU. otorga a los particulares tales derechos. En particular, el interesado tiene derecho, sin necesidad de justificación, a: que la entidad le confirme si trata datos personales relacionados con él; que le proporcione los datos; y recibir información sobre la finalidad del tratamiento, las categorías de datos personales tratados y las categorías de destinatarios a quienes se comunican los datos ([42]). Las entidades deben responder a las solicitudes de acceso en un plazo razonable ([43]). La entidad puede fijar

([37]) Anexo I, sección II, punto 4, letra a. Además, en lo que respecta a los datos de recursos humanos, el Marco de Privacidad de Datos UE-EE. UU. obliga a los empleadores a adaptarse a las preferencias de privacidad de sus empleados limitando el acceso a los datos personales, anonimizando determinados datos o asignando códigos o seudónimos (anexo I, sección III, punto 9, letra b, inciso iii).

([38]) Anexo I, sección II, punto 1.

([39]) Anexo I, sección II, punto 1, letra b. El principio complementario n.º 14 (anexo I, sección III, punto 14, letras b y c) contiene disposiciones específicas para el tratamiento de datos personales en el contexto de la investigación médica y los ensayos clínicos. En particular, este principio permite a las entidades tratar los datos de los ensayos clínicos, incluso después de que el particular deje de participar en el ensayo, si así se dejó claro en la notificación cuando el particular aceptó participar. Del mismo modo, si las entidades que participan en el Marco de Privacidad de Datos UE-EE. UU. reciben datos personales con fines de investigación médica, solo pueden utilizarlos para una nueva actividad de investigación de conformidad con los principios de notificación y opción. En este caso, la notificación al particular debe, en principio, proporcionar información sobre cualquier uso específico futuro de los datos (por ejemplo, estudios relacionados). Si no es posible enumerar desde el principio todos los usos futuros de los datos (porque los nuevos usos con fines investigativos podrían derivarse de nuevos conocimientos o avances médicos o de investigación), debe explicarse que los datos pueden ser utilizados en futuras actividades de investigación médica y farmacéutica imprevistas. Si este uso posterior no es coherente con la finalidad general de investigación para la que se recogieron los datos (por ejemplo, si la nueva finalidad es sustancialmente diferente, pero todavía compatible con la finalidad original; véanse los considerandos 14 y 15), debe obtenerse un nuevo consentimiento expreso. Véanse, además, las limitaciones o excepciones específicas al principio de notificación descritas en la nota a pie de página 28.

([40]) Anexo I, sección III, punto 6, letra d.

([41]) Véase también el principio complementario sobre el acceso (anexo I, sección III, punto 8).

([42]) Anexo I, sección III, punto 8, letra a, incisos i y ii.

([43]) Anexo I, sección III, punto 8, letra i.

límites razonables al número de veces que satisfará las solicitudes de acceso de un particular concreto dentro de un período determinado y puede cobrar una tasa que no sea excesiva, por ejemplo, cuando las solicitudes sean manifiestamente abusivas, en particular por su carácter repetitivo ([44]).

(31) El derecho de acceso solo puede limitarse en circunstancias excepcionales, similares a las contempladas en la normativa de la Unión en materia de protección de datos, en particular: cuando ello vulnere los derechos legítimos de terceros; cuando el trabajo o el gasto de conceder el acceso sean desproporcionados en relación con los riesgos para la privacidad del particular dadas las circunstancias del caso (aunque los gastos y el trabajo no sean criterios que se deban valorar al determinar si conceder el acceso es razonable); en la medida en que sea probable que la comunicación de los datos afecte a la protección de intereses públicos preponderantes, como la seguridad nacional, la seguridad pública o la defensa; cuando la información contenga información comercial confidencial; cuando la información se trate únicamente con fines de investigación o estadísticos ([45]). Cualquier denegación o limitación de un derecho del interesado tiene que ser necesaria y estar debidamente justificada, y corresponde a la entidad demostrar el cumplimiento de tales requisitos ([46]). Al realizar este análisis, la entidad debe tener especialmente en consideración los intereses del particular ([47]). Si es posible separar la información de otros datos a los que se aplique una limitación, la entidad debe expurgar la información protegida y comunicar la información restante ([48]).

(32) Además, los interesados tienen derecho a que se rectifiquen o modifiquen los datos inexactos y a que se supriman los datos tratados en vulneración de los principios en materia de privacidad ([49]). Por otra parte, como se explica en el considerando 15, los particulares tienen derecho a oponerse al tratamiento de sus datos con finalidades sustancialmente distintas (pero compatibles) de aquellas para las que se recogieron y a la comunicación de sus datos a terceros. Si los datos personales se utilizan con fines de mercadotecnia directa, los particulares tienen un derecho general a oponerse en todo momento al tratamiento ([50]).

(33) Los principios en materia de privacidad no tratan específicamente la cuestión de las decisiones que afectan al interesado basadas únicamente en el tratamiento automatizado de datos personales. Sin embargo, en lo que respecta a los datos personales que hayan sido recogidos en la Unión, las decisiones basadas en el tratamiento automatizado las debe tomar normalmente el responsable del tratamiento de los datos en la Unión (que tiene una relación directa con el interesado de que se trate) y están, por tanto, sujetas directamente al Reglamento (UE) 2016/679 ([51]). Se trata, por ejemplo, de los supuestos de transferencia en los que el tratamiento lo lleva a cabo un operador económico extranjero (por ejemplo, estadounidense) que actúa como agente (encargado) del responsable de la Unión (o como subencargado que actúa por cuenta del encargado de la Unión que ha recibido los datos del responsable de la Unión que los recogió) que, por ello, toma la decisión.

(34) Así se confirmó en el estudio encargado por la Comisión en 2018 en el marco de la segunda revisión anual del funcionamiento del Escudo de la privacidad ([52]), en el que se llegaba a la conclusión de que, en aquel momento, no había indicios de que las entidades participantes en el Escudo de la privacidad estuvieran tomando, de forma generalizada, decisiones automatizadas basadas en los datos personales transferidos en el marco del Escudo de la privacidad.

([44]) Anexo I, sección III, punto 8, letra f, inciso i y ii, y letra g.
([45]) Anexo I, sección III, punto 4, punto 8, letras b, c y e, punto 14, letras e y f, y punto 15, letra d.
([46]) Anexo I, sección III, punto 8, letra e, inciso ii. La entidad debe explicar al particular los motivos de la denegación o limitación e indicar el punto de contacto al que plantear consultas ulteriores (sección III, punto 8, letra a, inciso iii).
([47]) Anexo I, sección III, punto 8, letra a, incisos ii y iii.
([48]) Anexo I, sección III, punto 8, letra a, inciso i.
([49]) Anexo I, sección II, punto 6, y sección III, punto 8, letra a, inciso i.
([50]) Anexo I, sección III, puntos 8 y 12.
([51]) Sin embargo, puede darse excepcionalmente el caso de que haya una relación directa entre la entidad estadounidense y el interesado de la UE, lo que suele ser consecuencia de que dicha entidad se dirige específicamente al particular en la UE ofreciéndole bienes o servicios o haciendo un seguimiento de su conducta. En tal supuesto, la propia entidad estadounidense está comprendida en el ámbito de aplicación del Reglamento (UE) 2016/679 (artículo 3, apartado 2) y, por lo tanto, debe ella cumplir directamente la normativa de la Unión en materia de protección de datos.
([52]) SWD(2018) 497 final, sección 4.1.5. El estudio se concentró en i) la medida en que las entidades estadounidenses participantes en el Escudo de la privacidad toman decisiones que afectan a los interesados basadas en el tratamiento automatizado de los datos personales transferidos por empresas de la UE en el marco del Escudo de la privacidad y ii) las garantías que la normativa federal estadounidense contempla para los particulares en este tipo de supuestos y las condiciones para su aplicación.

(35) En cualquier caso, en los ámbitos en que es más probable que las empresas recurran al tratamiento automatizado de los datos personales para tomar decisiones que afectan al particular (por ejemplo, préstamos, hipotecas, empleo o seguros), las leyes estadounidense contemplan garantías específicas contra las decisiones que les perjudiquen ([53]). En dichas leyes se suele disponer que los particulares tienen derecho a ser informados de los motivos específicos de la decisión (por ejemplo, la denegación de un préstamo), a impugnar el carácter incompleto o inexacto de la información (así como el hecho de que concurran circunstancias que la hagan ilícita) y a pedir reparación. En el ámbito de los créditos al consumo, la Ley sobre la imparcialidad de las fichas de información crediticia y la Ley de igualdad de oportunidades de crédito establecen garantías que otorgan a los consumidores una suerte de derecho a pedir explicaciones y de derecho a impugnar la decisión. Estas Leyes son de aplicación a un amplio conjunto de ámbitos, como los préstamos, el empleo, la vivienda y los seguros. Además, determinadas normas contra la discriminación, como el título VII de la Ley de derechos civiles (Civil Rights Act) y la Ley de vivienda justa, brindan a los particulares protección frente a los modelos utilizados en las decisiones automatizadas que puedan dar lugar a discriminación por determinadas características, y confieren a los particulares derechos para impugnar tales decisiones, especialmente las automatizadas. Con respecto a la información sanitaria, la disposición en materia de privacidad de la Ley de portabilidad de los seguros de enfermedad y de responsabilidad respecto de estos (Health Insurance Portability and Accountability Act) crea determinados derechos similares a los del Reglamento (UE) 2016/679 con respecto al acceso a la información personal sanitaria. Además, las directrices de las autoridades estadounidenses exigen a quienes presten servicios médicos que reciban la información con la que puedan informar a los particulares de los sistemas de decisiones automatizadas utilizados en el sector médico ([54]).

(36) Por lo tanto, estas reglas confieren garantías similares a las contempladas en la normativa de la Unión en materia de protección de datos en el supuesto improbable de que las propias entidades participantes tomaran decisiones automatizadas.

2.2.6. ***Limitaciones de las transferencias ulteriores***

(37) El nivel de protección de los datos personales que se transfieren desde la UE a entidades estadounidenses no debe verse comprometido por la transferencia ulterior de dichos datos a destinatarios estadounidenses o de terceros países.

(38) En virtud del principio de responsabilidad proactiva por las transferencias ulteriores ([55]), serán de aplicación reglas especiales a las transferencias ulteriores, es decir, las transferencias de datos personales de una entidad participante a un tercero que ejerza de responsable o encargado, con independencia de si este último está establecido en los EE. UU. o en un tercer país distinto de los EE. UU. (y no comprendido en la UE). Las transferencias ulteriores solo puede tener lugar i) para fines limitados y especificados, ii) sobre la base de un contrato entre la entidad participante y el tercero ([56]) (o un acuerdo equivalente dentro de un grupo de sociedades de capital ([57])) y iii) solo si dicho contrato exige al tercero que confiera el mismo nivel de protección que el garantizado por los principios en materia de privacidad.

(39) Esta obligación de conferir el mismo nivel de protección que el garantizado por los principios en materia de privacidad, que debe leerse junto con el principio de principio de integridad de los datos y limitación de la finalidad, significa, en particular, que el tercero solo puede tratar la información personal que le haya sido transferida para fines que no sean incompatibles con los fines para los que fueron recogidos inicialmente o que autorizó posteriormente por el particular (de conformidad con el principio de opción).

([53]) Véase, por ejemplo, la Ley de igualdad de oportunidades de crédito [Equal Credit Opportunity Act; título 15, artículos 1691 y ss., del Código de Estados Unidos (United States Code)], la Ley sobre la imparcialidad de las fichas de información crediticia (Fair Credit Reporting Act; título 15, artículos 1681 y ss., del Código de Estados Unidos) o la Ley de vivienda justa (Fair Housing Act; título 42, artículos 3601 y ss., del Código de Estados Unidos). Además, los EE. UU. se han comprometido a cumplir los principios de la OCDE en materia de inteligencia artificial, que incluyen, por ejemplo, principios en materia de transparencia y detallan el régimen de capacidad, seguridad y rendición de cuentas.

([54]) Véanse, por ejemplo, las directrices disponibles en inglés en el sitio web del Departamento de Salud y Servicios Humanos (Department of Health and Human Services) sobre la información personal sanitaria de sus prestadores de asistencia sanitaria y sus seguros de salud a la que tienen derecho de acceso los particulares, en virtud de la Ley de portabilidad de los seguros de enfermedad y de responsabilidad respecto de estos.

([55]) Véase el anexo I, sección II, punto 3, y el principio complementario sobre los contratos obligatorios para las transferencias ulteriores (anexo I, sección III, punto 10).

([56]) Como excepción a este principio general, las entidades pueden realizar la transferencia ulterior de datos personales de un pequeño número de empleados sin suscribir un contrato con el destinatario si se trata de necesidades operativas ocasionales relacionadas con el trabajo, por ejemplo, la reserva de un vuelo o de una habitación de hotel o la contratación de un seguro. Sin embargo, también en este supuesto, la entidad sigue teniendo que cumplir los principios de notificación y de opción (véase el anexo I, sección III, punto 9, letra e).

([57]) Véase el principio complementario sobre los contratos obligatorios para las transferencias ulteriores (anexo I, sección III, punto 10, letra b). Si bien este principio permite que se realicen las transferencias también con arreglo a 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 la información personal de conformidad con los principios en materia de privacidad». Además, dado que las entidades estadounidenses certificadas siguen siendo responsables del cumplimiento de los principios en materia de privacidad, tienen un fuerte incentivo para utilizar instrumentos que sean realmente eficaces en la práctica.

(40) El principio de responsabilidad proactiva por las transferencias ulteriores también debe leerse junto con el principio de notificación y, en el caso de las transferencias ulteriores a terceros responsables del tratamiento ([58]), con el principio de opción, según el cual los interesados deben ser informados de, entre otros aspectos, el tipo o la identidad del tercero destinatario, la finalidad de la transferencia ulterior y la opción ofrecida y pueden oponerse o, en el caso de datos delicados, tienen que dar su «consentimiento expreso» a la transferencia ulterior.

(41) La obligación de conferir el mismo nivel de protección que el garantizado por los principios en materia de privacidad es de aplicación a todos los terceros implicados 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 su subtratamiento.

(42) En todos los casos, el contrato celebrado con el tercero receptor debe disponer que este notificará a la entidad participante si ya no puede cumplir esta obligación. Cuando se llegue a esta conclusión, el tratamiento por el tercero debe cesar o deben tomarse otras medidas razonables y adecuadas para corregir la situación ([59]).

(43) Son de aplicación garantías adicionales en caso de transferencia ulterior a un tercero agente (encargado). En tal caso, la entidad estadounidense debe asegurarse de que el agente solo actúa siguiendo sus instrucciones y tomar medidas razonables y adecuadas para i) garantizar que el agente efectivamente trate los datos personales transferidos cumpliendo las obligaciones que los principios en materia de privacidad imponen a la entidad y ii) detener el tratamiento no autorizado y tomar las oportunas medidas de reparación, previa notificación ([60]). El Departamento de Comercio puede exigir a la entidad que aporte un resumen o una copia representativa de las cláusulas en materia de privacidad del contrato ([61]). Cuando se planteen problemas de cumplimiento en una cadena de (sub)tratamiento, la entidad que sea responsable del tratamiento de los datos personales es, en principio, responsable, tal como se especifica en el principio de impugnación, ejecución forzosa y responsabilidad, excepto si demuestra que no es responsable del hecho generador del perjuicio ([62]).

2.2.7. ***Responsabilidad proactiva***

(44) En virtud del principio de responsabilidad proactiva, las entidades que traten datos están obligadas a tomar medidas técnicas u organizativas apropiadas para cumplir efectivamente sus obligaciones en materia de protección de datos y deben poder demostrar el cumplimiento de estas obligaciones, en particular ante la autoridad de supervisión competente.

(45) Cuando la entidad decide voluntariamente certificarse ([63]) en el Marco de Privacidad de Datos UE-EE. UU., contrae la obligación de cumplir plenamente los principios, que será exigible por la vía de la ejecución forzosa. En virtud del principio de impugnación, ejecución forzosa y responsabilidad ([64]), las entidades participantes deben establecer mecanismos eficaces para garantizar el cumplimiento de los principios en materia de privacidad. Asimismo, las entidades deben tomar medidas para verificar ([65]) que sus directrices en materia privacidad se ajustan a los principios en materia de privacidad y se aplican en consecuencia. Dicha verificación puede llevarse a cabo, bien mediante un sistema de autoevaluación, que debe constar de una serie de procedimientos internos que garanticen que los empleados reciben formación sobre la aplicación de las directrices en materia privacidad de la entidad y que se efectúen verificaciones objetivas periódicas del cumplimiento, bien mediante verificaciones externas, entre cuyos métodos pueden figurar las auditorías, las comprobaciones aleatorias o el uso de herramientas tecnológicas.

([58]) Los particulares no tendrán derecho a oponerse cuando los datos personales se transfieran a un tercero que actúe como agente de la entidad estadounidense, esto es, por su cuenta y siguiendo sus instrucciones. Sin embargo, para ello es necesario un contrato con el agente, y la entidad estadounidense asume la responsabilidad de hacer efectivas las garantías que ofrecen los principios en materia de privacidad, mediante el ejercicio de sus competencias de instrucción.

([59]) La situación varía según el tercero sea responsable o encargado (agente) del tratamiento. En la primera hipótesis, el contrato celebrado con el tercero debe disponer que este cese el tratamiento o tome otras medidas razonables y adecuadas para corregir la situación. En la segunda hipótesis, corresponde a la entidad participante —como responsable del tratamiento con cuyas instrucciones opera el agente — tomar estas medidas. Véase el anexo I, sección III, punto 3.

([60]) Anexo I, sección II, punto 3, letra b.

([61]) *Véase la nota anterior.*

([62]) Anexo I, sección II, punto 7, letra d.

([63]) Véase también el principio complementario sobre la autocertificación (anexo I, sección III, punto 6).

([64]) Véase también el principio complementario sobre la resolución de controversias y la ejecución forzosa (anexo I, sección III, punto 11).

([65]) Véase también el principio complementario sobre la verificación (anexo I, sección III, punto 7).

(46) Además, las entidades deben conservar los documentos que prueben por escrito la implantación de sus prácticas respecto del Marco de Privacidad de Datos UE-EE. UU. y proporcionarlos previa petición, en el contexto de investigaciones o reclamaciones por incumplimiento, al organismo independiente de resolución de controversias o al organismo de garantía del cumplimiento competente ([66]).

2.3. **Administración, supervisión y garantía del cumplimiento**

(47) El Departamento de Comercio se encarga de la administración y la supervisión del Marco de Privacidad de Datos UE-EE. UU. El Marco contempla mecanismos de supervisión y garantía del cumplimiento para verificar y garantizar que las entidades participantes cumplen los principios en materia de privacidad y que se trata de resolver los incumplimientos. Estos mecanismos se establecen en los principios en materia de privacidad (anexo I) y los compromisos asumidos por el Departamento de Comercio (anexo III), la Comisión Federal de Comercio (anexo IV) y el Departamento de Transporte (anexo V).

2.3.1. ***Certificación y revalidación de la certificación***

(48) Para certificarse en el Marco de Privacidad de Datos UE-EE. UU. (o revalidar anualmente su certificación), las entidades están obligadas a declarar públicamente su compromiso de cumplir los principios en materia de privacidad, publicar sus directrices en materia privacidad y aplicarlas plenamente ([67]). Como parte de su solicitud de revalidación de la certificación, las entidades deben presentar información al Departamento de Comercio sobre, entre otros aspectos, el nombre de la entidad pertinente, la descripción de los fines para los que tratará los datos personales, los datos personales cubiertos por la certificación, así como el método de verificación elegido, el órgano independiente de impugnación pertinente y el organismo legal que tenga competencia para hacer cumplir los principios en materia de privacidad ([68]).

(49) Las entidades pueden recibir datos personales en el Marco de Privacidad de Datos UE-EE. UU. desde la fecha en que sean inscritas en la lista del Marco por el Departamento de Comercio. Para preservar la seguridad jurídica y evitar las declaraciones falsas, se prohíbe a las entidades que se autocertifiquen por primera vez indicar públicamente que cumplen los principios en materia de privacidad hasta que el Departamento de Comercio haya determinado que el expediente inicial de autocertificación que ha presentado la entidad está completo y haya inscrito a la entidad en la lista del Marco de Privacidad de Datos ([69]). Al objeto de poder seguir acogiéndose al Marco de Privacidad de Datos UE-EE. UU. para recibir datos personales de la UE, las entidades deben revalidar cada año su certificación de participación en el Marco. Cuando la entidad deje de estar amparada por el Marco de Privacidad de Datos UE-EE. UU. por el motivo que sea, debe eliminar todas las declaraciones que den a entender que continúa participando en el Marco ([70]).

(50) Como se refleja en los compromisos mencionados en el anexo III, el Departamento de Comercio debe verificar si las entidades cumplen todos los requisitos para la certificación y han aprobado directrices (públicas) en materia de privacidad con la información exigida por el principio de notificación ([71]). Basándose en la experiencia adquirida con el proceso de certificación (o de revalidación de la certificación) en el Escudo de la privacidad, el Departamento de Comercio debe llevar a cabo una serie de comprobaciones, en particular para verificar si las directrices en materia privacidad de las entidades incluyen un enlace al formulario de reclamación correcto en el sitio web del órgano de resolución de controversias pertinente y, cuando el expediente de certificación comprenda a varias filiales y sucursales de la entidad, si las directrices en materia privacidad de cada una de esas filiales cumplen los requisitos para la certificación y están a disposición de los interesados ([72]). Además, el Departamento de Comercio debe llevar a cabo, cuando sea necesario, comprobaciones concertadas con la Comisión Federal de Comercio y el Departamento de Transporte para verificar que las entidades están realmente sujetas al organismo de supervisión indicado en el expediente de certificación (o de revalidación de la certificación), y colaborará con los organismos de resolución alternativa de controversias para verificar que las entidades están dadas de alta realmente ante el órgano independiente de impugnación indicado en el expediente de certificación (o de revalidación de la certificación) ([73]).

([66]) Anexo I, sección III, punto 7.
([67]) Anexo I, sección I, punto 2.
([68]) Anexo I, sección III, punto 6, letra b, y anexo III, sección «Verificar los requisitos para la autocertificación».
([69]) Anexo I, nota a pie de página 12.
([70]) Anexo I, sección III, punto 6, letra h.
([71]) Anexo I, sección III, punto 6, letra a, y nota a pie de página 12, así el anexo III, sección «Verificar los requisitos para la autocertificación».
([72]) Anexo III, sección «Verificar los requisitos para la autocertificación».
([73]) Del mismo modo, el Departamento de Comercio colaborará con el tercero que actúe como depositario de los fondos recaudados a través de la tasa para el panel de las APD (véase el considerando 73) para verificar que las entidades que hayan indicado a las APD como órgano independiente de impugnación han pagado la tasa del año correspondiente. Véase el anexo III, sección «Verificar los requisitos para la autocertificación».

(51) El Departamento de Comercio debe informar a las entidades de que, para completar la certificación (o la revalidación de la certificación), deben resolver todos los problemas detectados durante su revisión. Si la entidad no responde en el plazo fijado por el Departamento de Comercio (por ejemplo, en lo que respecta a la revalidación de la certificación, se espera que el proceso se complete en un plazo de cuarenta y cinco días) ([74]) o de algún otro modo no completa su certificación, la certificación se considera desistida. En ese caso, cualquier engaño sobre la participación en el Marco de Privacidad de Datos UE-EE. UU., o sobre su cumplimiento, puede desencadenar actuaciones de ejecución forzosa por parte de la Comisión Federal de Comercio o Departamento de Transporte ([75]).

(52) Para garantizar la correcta aplicación del Marco de Privacidad de Datos UE-EE. UU., las partes interesadas, como los particulares afectados, los exportadores de datos y las APD nacionales, deben poder identificar a las entidades que se comprometen a cumplir los principios en materia de privacidad. Para garantizar la transparencia desde el comienzo, el Departamento de Comercio se ha comprometido a publicar y mantener actualizada la lista de las entidades que han certificado su cumplimiento de los principios en materia de privacidad y están sujetas a la competencia de, como mínimo, uno de los organismos de garantía del cumplimiento mencionados en los anexos IV y V de la presente Decisión ([76]). El Departamento de Comercio debe actualizar dicha lista en función de las revalidaciones anuales de las autocertificaciones de las entidades y cada vez que una entidad se dé de baja o sea eliminada del Marco de Privacidad de Datos UE-EE. UU. Por otra parte y para garantizar la transparencia también al final, debe publicar y mantener actualizado el registro de las entidades que ya no formen parte de la lista, con indicación en cada caso del motivo de dicha eliminación ([77]). Por último, debe proporcionar un enlace al sitio web de la Comisión Federal de Comercio sobre el Marco de Privacidad de Datos UE-EE. UU. en el que se enumerarán las competencias de la Comisión Federal de Comercio de garantía del cumplimiento respecto del Marco ([78]).

2.3.2. ***Control del cumplimiento***

(53) El Departamento de Comercio debe controlar de forma continuada el cumplimiento efectivo de los principios en materia de privacidad por parte de las entidades participantes a través de diferentes mecanismos ([79]). En particular, debe llevar a cabo inspecciones sin aviso de entidades seleccionadas aleatoriamente, así como inspecciones sin aviso *ad hoc* de entidades específicas cuando se detecten posibles deficiencias en el cumplimiento (por ejemplo, las puestas en conocimiento del Departamento de Comercio por terceros) para verificar si: i) el punto o puntos de contacto responsables de la tramitación de las reclamaciones y las solicitudes de los interesados están disponibles y dan respuesta; ii) las directrices en materia de privacidad de la entidad se pueden visualizar sin restricciones tanto en su sitio web como a través de un enlace en el sitio web del Departamento de Comercio; iii) las directrices en materia de privacidad de la entidad siguen cumpliendo los requisitos para la certificación; y iv) el organismo independiente de resolución de controversias indicado por la entidad está disponible para conocer de las reclamaciones ([80]).

(54) Si hay indicios creíbles de que la entidad no cumple sus compromisos a efectos del Marco de Privacidad de Datos UE-EE. UU. (en particular, si el Departamento de Comercio recibe reclamaciones o si la entidad no responde satisfactoriamente a las solicitudes del Departamento), este debe exigir a la entidad que cumplimente y envíe el cuestionario pormenorizado correspondiente ([81]). Si la entidad no responde oportuna y satisfactoriamente, se remite el asunto a la autoridad competente (Comisión Federal de Comercio o Departamento de Transporte) para que tome las medidas necesarias para garantizar el cumplimiento ([82]). Como parte de sus actividades de control del

([74]) Anexo III, nota a pie de página 2.
([75]) Véase el anexo III, sección «Verificar los requisitos para la autocertificación».
([76]) La información sobre la administración de la lista del Marco de Privacidad de Datos puede consultarse en el anexo III (véase la introducción en el epígrafe «Administración y supervisión del programa del Marco de Privacidad de Datos por parte del Departamento de Comercio») y en el anexo I (sección I, puntos 3 y 4, y sección III, punto 6, letra d, y punto 11, letra g).
([77]) Anexo III, véase la introducción en el epígrafe «Administración y supervisión del programa del Marco de Privacidad de Datos por parte del Departamento de Comercio».
([78]) Véase el anexo III, epígrafe «Adaptar el sitio web del Marco de Privacidad de Datos al público destinatario».
([79]) Véase el anexo III, epígrafe «Realizar de oficio revisiones y evaluaciones periódicas del cumplimiento del programa del Marco de Privacidad de Datos».
([80]) Como parte de sus actividades de control, el Departamento de Comercio puede utilizar diferentes herramientas, en particular para comprobar si han dejado de funcionar los enlaces a las directrices en materia de privacidad o para hacer un seguimiento proactivo de las noticias para buscar denuncias de las que se desprendan indicios creíbles de incumplimiento.
([81]) Véase el anexo III, epígrafe «Realizar de oficio revisiones y evaluaciones periódicas del cumplimiento del programa del Marco de Privacidad de Datos».
([82]) Véase el anexo III, epígrafe «Realizar de oficio revisiones y evaluaciones periódicas del cumplimiento del programa del Marco de Privacidad de Datos».

cumplimiento en el Escudo de la privacidad, el Departamento de Comercio llevó a cabo periódicamente las inspecciones sin aviso mencionadas en el considerando 53 e hizo un seguimiento constante de los informes públicos, lo que le permitió detectar, tratar y resolver los problemas de cumplimiento ([83]). Las entidades que incumplan sistemáticamente los principios en materia de privacidad son eliminadas de la lista del Marco de Privacidad de Datos y deben devolver o suprimir la información personal que hubiesen recibido con arreglo al Marco ([84]).

(55) En los demás casos de eliminación de la lista, como la baja voluntaria o la falta de revalidación de la certificación, la entidad debe suprimir o devolver los datos, pero también puede conservarlos si revalida cada año ante el Departamento de Comercio su compromiso de continuar aplicando los principios en materia de privacidad o confiere una protección adecuada a los datos personales por otros medios autorizados (por ejemplo, con un contrato que contenga todos los requisitos de las cláusulas contractuales tipo adoptadas por la Comisión) ([85]). En este caso, la entidad también tiene que nombrar un punto de contacto, dentro de la entidad, para todas las cuestiones relacionadas con el Marco de Privacidad de Datos UE-EE. UU.

2.3.3. ***Detección y corrección de las declaraciones falsas de participación***

(56) El Departamento de Comercio debe hacer un seguimiento de las posibles declaraciones falsas de participación en el Marco de Privacidad de Datos UE-EE. UU. y del uso indebido de la marca de certificación del Marco, tanto de oficio como previa reclamación (por ejemplo, recibidas de las APD) ([86]). En particular, debe verificar de forma continuada que las entidades que i) se den de baja en el Marco de Privacidad de Datos UE-EE. UU., ii) no hayan completado la revalidación anual de la certificación (es decir, bien porque iniciaron el trámite, pero no lo completaron a su debido tiempo, bien porque nunca lo iniciaron), iii) no hayan sido eliminadas como participantes, en particular por «incumplimiento sistemático», o iv) no hayan completado la certificación inicial (es decir, porque iniciaron el trámite, pero no lo completaron a su debido tiempo), eliminen toda referencia de las directrices en materia de publicidad pertinentes que implique que participan activamente en el Marco ([87]). El Departamento de Comercio también debe realizar búsquedas en internet para hallar referencias al Marco de Privacidad de Datos UE-EE. UU. en las directrices en materia privacidad de las entidades, incluida la detección de declaraciones falsas de entidades que nunca hayan participado en el Marco ([88]).

(57) Cuando el Departamento de Comercio constate que las referencias al Marco de Privacidad de Datos UE-EE. UU. no se han eliminado o se utilizan indebidamente, informará a la entidad de que, si no se subsana la situación, puede remitir el asunto a la Comisión Federal de Comercio o al Departamento de Transporte ([89]). Si la entidad no responde satisfactoriamente, el Departamento de Comercio debe remitir el asunto al organismo competente para que tome las medidas oportunas ([90]). Todo engaño en la información dada a conocer al público en lo referente al cumplimiento por parte de la entidad de los principios en materia de privacidad en forma de declaraciones o prácticas engañosas puede ser objeto de medidas de ejecución forzosa de la Comisión Federal de Comercio, del Departamento de Transporte u otros organismos de garantía del cumplimiento pertinentes estadounidenses. Los engaños en la información transmitida al Departamento pueden castigarse en el marco de la Ley de declaraciones falsas (False Statements Act; título 18, artículo 1001, del Código de Estados Unidos).

([83]) Durante la segunda revisión anual del Escudo de la privacidad, el Departamento de Comercio informó de que había llevado a cabo inspecciones sin aviso de cien entidades y envió cuestionarios sobre cumplimiento en veintiún casos (tras lo cual se subsanaron los problemas detectados); véase el documento de la Comisión SWD(2018) 497 final, p. 9. Del mismo modo, el Departamento de Comercio informó durante la tercera revisión anual del Escudo de la privacidad de que había detectado tres incidentes, gracias a su labor de seguimiento de los informes públicos, y comenzó la práctica de realizar inspecciones sin aviso a treinta empresas cada mes, lo que dio lugar al envío del cuestionario sobre cumplimiento en el 28 % de los casos (tras lo cual, los problemas detectados se subsanaron inmediatamente o, en tres casos, se resolvieron tras una carta de advertencia); véase el documento de la Comisión SWD(2019) 495 final, p. 8.

([84]) Anexo I, sección III, punto 11, letra g. Se considera que se produce incumplimiento sistemático cuando la entidad se niegue a cumplir la resolución del organismo del ámbito autorregulatorio en materia de privacidad, del organismo de resolución de controversias independiente o del organismo de garantía del cumplimiento.

([85]) Anexo I, sección III, punto 6, letra f.

([86]) Véase el anexo III, epígrafe «Detectar y corregir las declaraciones falsas de participación».

([87]) *Véase la nota anterior.*

([88]) *Véase la nota anterior.*

([89]) *Véase la nota anterior.*

([90]) En el marco del Escudo de la privacidad, el Departamento de Comercio informó, durante la tercera revisión anual del marco, de que había detectado 669 casos de declaraciones falsas de participación (entre octubre de 2018 y octubre de 2019), la mayoría de los cuales se resolvieron después de la carta de advertencia del Departamento de Comercio; 143 casos fueron remitidos a la Comisión Federal de Comercio (véase el considerando 62). Véase el documento de la Comisión SWD(2019) 495 final, página 10.

2.3.4. ***Garantía del cumplimiento***

(58) Con el fin de garantizar un nivel de protección adecuado de los datos en la práctica, debe haber una autoridad de control independiente encargada de supervisar el cumplimiento de la normativa en materia de protección de datos y hacerla cumplir en caso necesario.

(59) Las entidades participantes deben estar sujetas a la competencia de las autoridades estadounidenses competentes (la Comisión Federal de Comercio y el Departamento de Transporte), que disponen de las competencias de investigación y ejecución forzosa necesarias para garantizar el cumplimiento efectivo de los principios en materia de privacidad ([91]).

(60) La Comisión Federal de Comercio es una autoridad independiente compuesta por cinco comisarios, nombrados por el presidente con el asesoramiento y la autorización del Senado ([92]). Los comisarios son nombrados por un mandato de siete años y solo pueden ser destituidos por el presidente por ineficiencia, incumplimiento de deberes o delitos contra la Administración pública. La Comisión Federal de Comercio no puede tener más de tres comisarios del mismo partido político y los comisarios no pueden ejercer, mientras ocupen este cargo, ninguna otro actividad empresarial, profesional o laboral.

(61) La Comisión Federal de Comercio puede realizar investigaciones sobre el cumplimiento de los principios en materia de privacidad, así como sobre las declaraciones falsas de cumplimiento de los principios o de participación en el Marco de Privacidad de Datos UE-EE. UU. por parte de las entidades que ya no figuren en la lista del Marco o que nunca se hayan certificado ([93]). También puede exigir coercitivamente el cumplimiento solicitando que se dicten resoluciones administrativas o resoluciones judiciales federales (como las resoluciones de constatación de la avenencia, dictadas para homologar los convenios transaccionales) ([94]) con las que imponer medidas cautelares o permanentes u otras medidas de reparación, y hace un seguimiento sistemático del cumplimiento de dichas resoluciones ([95]). Si las entidades incumplen dichas resoluciones, la Comisión Federal de Comercio puede solicitar la imposición de multas y otras medidas de reparación, incluida la indemnización por cualquier perjuicio ocasionado por la conducta infractora. Las resoluciones de constatación de la avenencia dictadas respecto de entidades participantes contienen obligaciones de información ([96]) y las entidades tienen que publicar todas las secciones pertinentes relacionadas con el Marco de Privacidad de Datos UE-EE. UU. de todo informe de cumplimiento o evaluación presentados a la Comisión Federal de Comercio. Por último, la Comisión Federal de Comercio publica en línea la lista de las entidades objeto de las resoluciones judiciales o dictadas por la Comisión Federal de Comercio en los asuntos relativos al Marco de Privacidad de Datos UE-EE. UU. ([97]).

(62) Con respecto al Escudo de la privacidad, la Comisión Federal de Comercio emprendió medidas de ejecución forzosa en unos veintidós casos, tanto en relación con la vulneración de requisitos específicos del marco (por ejemplo, que la entidad no declarase al Departamento de Comercio que siguió aplicando las garantías del Escudo de la privacidad después de que se diese de baja en este; que no verificase, mediante una autoevaluación o una verificación externa del cumplimiento, que cumplía el marco) ([98]) como con declaraciones falsas de participación en el marco (por ejemplo, por parte de entidades que no completaron el proceso de certificación o que no renovaron anualmente su certificación, pero seguían afirmando participar en el marco) ([99]). Estas medidas de ejecución forzosa se debieron, entre otras cosas, al uso proactivo de los requerimientos administrativos para obtener información de determinados participantes en el Escudo de la privacidad para comprobar si se habían producido vulneraciones sustanciales de las obligaciones del Escudo de la privacidad ([100]).

([91]) Las entidades participantes tienen que declarar públicamente su compromiso de cumplir los principios en materia de privacidad, publicar sus directrices en materia privacidad de conformidad con estos principios y ponerlos en práctica en su totalidad. Se puede obligar a cesar el incumplimiento; primero, con arreglo al artículo 5 de la Ley de la Comisión Federal de Comercio (Federal Trade Commission Act), por el que se prohíben los actos desleales o engañosos en el comercio o que afectan al mismo (título 15, artículo 45, del Código de Estados Unidos), y, segundo, con arreglo al título 49, artículo 41712, del Código de Estados Unidos, por el que se prohíbe a los transportistas y los agentes de venta de billetes participar en prácticas desleales o engañosas en el transporte aéreo o en la comercialización de este tipo de transporte.

([92]) Título 15, artículo 41, del Código de Estados Unidos.

([93]) Anexo IV.

([94]) Según información de la Comisión Federal de Comercio, esta no tiene competencia para llevar a cabo inspecciones sobre el terreno en el ámbito de la protección de la privacidad. No obstante, tiene competencia para obligar a las entidades a presentar documentos y declaraciones de testigos (véase el artículo 20 de la Ley de la Comisión Federal de Comercio) y puede recurrir al sistema judicial para hacer ejecutar tales órdenes en caso de incumplimiento.

([95]) Véase el anexo IV, epígrafe «Solicitar órdenes y hacer un seguimiento».

([96]) Las resoluciones de la Comisión Federal de Comercio o las judiciales pueden exigir a las empresas que introduzcan programas de protección de la privacidad y que presenten periódicamente a la Comisión Federal de Comercio informes de cumplimiento o evaluaciones de terceros independientes sobre dichos programas.

([97]) Anexo IV, epígrafe «Solicitar órdenes y hacer un seguimiento».

([98]) Documento de la Comisión SWD(2019) 495 final, página 11.

([99]) Véase la lista de asuntos en el sitio web de la Comisión Federal de Comercio, disponible en inglés en https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Véanse también los documentos de la Comisión SWD (2017) 344 final, p. 17, SWD(2018) 497 final, p. 12, y SWD(2019) 495 final, p. 11.

([100]) Véanse, por ejemplo, las observaciones escritas del presidente Joseph Simons respecto de la segunda revisión anual del Escudo de la privacidad.

(63) Con carácter más general, la Comisión Federal de Comercio ha emprendido en los últimos años medidas de ejecución forzosa en una serie de casos relativos al cumplimiento de las exigencias específicas en materia de protección de datos que también están contempladas en el Marco de Privacidad de Datos UE-EE. UU., como, por ejemplo, los principios de limitación de la finalidad y conservación de los datos ([101]), de minimización de los datos ([102]), de seguridad de los datos ([103]) y de exactitud de los datos ([104]).

(64) El Departamento de Transporte tiene competencia exclusiva para regular las prácticas en materia de privacidad de las aerolíneas y tiene competencia compartida con la Comisión Federal de Comercio con respecto a las prácticas en materia de privacidad de los agentes de venta de billetes en la comercialización de este tipo de transporte. Los funcionarios del Departamento de Transporte tratan en primer lugar de lograr un convenio transaccional y, si esto no es posible, pueden iniciar un proceso de ejecución, con audiencia probatoria ante un juez de lo contencioso-administrativo del Departamento de Transporte, que tiene potestad para dictar órdenes de cese de actividad e imponer sanciones pecuniarias ([105]). Los jueces de lo contencioso-administrativo gozan de varias prerrogativas en virtud de la Ley de lo contencioso-administrativo (Administrative Procedure Act) para garantizar su independencia e imparcialidad. Por ejemplo, solo pueden ser separados del servicio por causa justificada; se asignan los asuntos mediante turno de reparto; no pueden desempeñar funciones incompatibles con sus deberes y responsabilidades como jueces de lo contencioso-administrativo; no están sujetos a la supervisión de la unidad de investigación de la autoridad para la que trabajan (en este caso, el Departamento de Transporte); y deben desempeñar su función jurisdiccional y de ejecución con imparcialidad ([106]). El Departamento de Transporte se ha comprometido a hacer un seguimiento de las resoluciones de ejecución forzosa y a garantizar que las que se deriven de los casos relacionados con los principios del Marco de Privacidad de Datos UE-EE. UU. se puedan consultar en su sitio web ([107]).

2.4. **Reparación**

(65) Para que exista una protección adecuada y, en particular, que se puedan tutelar los derechos individuales por la vía coercitiva, el interesado debe poder ejercitar acciones judiciales y solicitar medidas administrativas con fines reparatorios.

(66) El Marco de Privacidad de Datos UE-EE. UU. obliga, a través del principio de impugnación, ejecución forzosa y responsabilidad, a las entidades a ofrecer vías de reparación a los particulares afectados por incumplimientos y, por tanto, a darles la posibilidad de presentar reclamaciones en relación con el incumplimiento de las entidades participantes; estas reclamaciones deben resolverse, en su caso, con una resolución que disponga medidas reparatorias eficaces ([108]). Como parte de su certificación, las entidades deben cumplir las exigencias de dicho principio estableciendo vías de reparación que se puedan activar inmediatamente y creando órganos independientes de impugnación eficaces que puedan investigar y resolver rápidamente las reclamaciones y controversias sin coste alguno para el interesado ([109]).

([101]) Véase, por ejemplo, la resolución de la Comisión Federal de Comercio contra Drizly, LLC., en la que exige a esta sociedad, entre otras cosas, que 1) destruya los datos personales que recogió que no sean necesarios para ofrecer sus bienes y servicios a los consumidores y 2) deje de recoger y almacenar información personal a menos que sea necesario para finalidades específicas explicitadas en el correspondiente cronograma de conservación de datos.

([102]) Véase, por ejemplo, la resolución de la Comisión Federal de Comercio contra CafePress (24 de marzo de 2022), en la que exige a esta empresa, entre otras cosas, que minimice la cantidad de datos que recoge.

([103]) Véase, por ejemplo, las medidas de ejecución forzosa de la Comisión Federal de Comercio contra Drizzly, LLC., y contra CafePress, con las que exigía a las empresas en cuestión que establecieran un programa de seguridad específico o que tomaran medidas de seguridad específicas. Además, por lo que se refiere a las violaciones de la seguridad de los datos, véase también la resolución de la Comisión Federal de Comercio de 27 de enero de 2023 contra Chegg y el convenio transaccional con Equifax de 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Véase, por ejemplo, el caso RealPage, Inc. (16 de octubre de 2018), en el que la Comisión Federal de Comercio emprendió medidas de ejecución forzosa con arreglo a la Ley sobre la imparcialidad de las fichas de información crediticia contra una empresa de escrutinio de futuros arrendatarios que elaboraba informes de antecedentes para los arrendadores y las sociedades de administración de fincas basándose en el historial de arrendamientos, información de registros públicos (como los antecedentes penales y los desahucios) y la información crediticia, que servían como factor para valorar la idoneidad para el arrendamiento. La Comisión Federal de Comercio constató que la empresa no había tomado medidas razonables para garantizar la exactitud de la información que proporcionaba, basada en su herramienta de automatizada.

([105]) Véase el anexo V, epígrafe «Prácticas de garantía del cumplimiento».

([106]) Véase el título 5, artículo 3105, artículo 7521, letra a), artículo 554, letra d), y artículo 556, letra b), punto 3, del Código de Estados Unidos.

([107]) Anexo V, sección titulada «Seguimiento y publicidad de las resoluciones de ejecución forzosa por vulneración de los principios del Marco de Privacidad de Datos UE-EE. UU.».

([108]) Anexo I, sección II, punto 7.

([109]) Anexo I, sección III, punto 11.

(67) Las entidades pueden optar por órganos independientes de impugnación en la UE o en los EE. UU. Como se explica con más detalle en el considerando 73, esto incluye la posibilidad de comprometerse voluntariamente a cooperar con las APD de la UE. Cuando las entidades traten datos de recursos humanos, dicho compromiso de cooperar con las APD de la UE es obligatorio. Otras opciones son la resolución alternativa de controversias independiente o los programas de protección de la privacidad concebidos por el sector privado que incorporen los principios en materia de privacidad en sus reglas. Estos últimos deben incluir mecanismos de ejecución eficaces de conformidad con los requisitos del principio de impugnación, ejecución forzosa y responsabilidad.

(68) Por consiguiente, el Marco de Privacidad de Datos UE-EE. UU. otorga a los interesados una serie de posibilidades para hacer valer sus derechos y presentar reclamaciones en relación con el incumplimiento de las entidades participantes; asimismo, contempla que se resuelvan sus reclamaciones, en su caso, con una resolución que imponga medidas reparatorias eficaces. Los particulares pueden presentar su reclamación directamente a la entidad, al organismo independiente de resolución de controversias designado por la entidad, a las APD nacionales, al Departamento de Comercio o a la Comisión Federal de Comercio. Cuando sus reclamaciones no sean resueltas por ninguna de estas vías, los particulares tienen derecho a solicitar la incoación de un proceso arbitral vinculante (anexo I del anexo I de la presente Decisión). Excepto por lo que se refiere al tribunal arbitral, que exige que se agoten ciertas vías de impugnación antes de acudir a él, los particulares tienen la posibilidad de seguir alguna o todas las vías de su elección y no están obligados a elegir una vía antes que otra ni a seguir una secuencia específica.

(69) En primer lugar, los interesados de la UE pueden buscar una solución en caso de incumplimiento de los principios en materia de privacidad poniéndose en contacto directamente con la entidad participante en cuestión ([110]). Al objeto de facilitar la resolución, la entidad deberá establecer una vía reparatoria eficaz para tales reclamaciones. Las directrices en materia de privacidad de la entidad han de indicar por tanto claramente cuál es el punto de contacto, ya sea interno o externo, que se encarga de tramitar las reclamaciones (incluido cualquier establecimiento pertinente en la UE que pueda atender las consultas o reclamaciones), e informar asimismo del organismo independiente de resolución de controversias designado por la entidad (véase el considerando 70). Cuando reciba la reclamación del particular, directamente de este o a través del Departamento de Comercio tras haber sido remitida por una APD, la entidad debe responder al interesado de la UE en un plazo de cuarenta y cinco días ([111]). 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 ([112]) (en el supuesto de que la entidad se haya comprometido a cooperar con las APD), con respecto a su cumplimiento de los principios en materia de privacidad.

(70) En segundo lugar, los particulares también pueden presentar su reclamación directamente al organismo independiente de resolución de controversias (de los EE. UU. o de la UE) designado por la entidad que se encargue de investigar y resolver las reclamaciones de los particulares (salvo que sean manifiestamente infundadas o insustanciales) y ofrecer al particular una vía de impugnación adecuada y gratuita ([113]). Las sanciones y medidas reparatorias impuestas por dicho organismo han de ser lo suficientemente severas para garantizar el cumplimiento de los principios en materia de privacidad por parte de las entidades, y debe poder exigirse la anulación o reparación por estas últimas de los efectos del incumplimiento y, según el caso, el cese del tratamiento de los datos personales en cuestión y/o la supresión de estos, así como la publicidad de los incumplimientos constatados ([114]). Los organismos independientes de resolución de controversias designados por las entidades tienen que incluir en sus sitios web públicos información pertinente sobre el Marco de Privacidad de Datos UE-EE. UU. y los servicios que prestan en este sentido ([115]). Todos los años deben publicar un informe anual con estadísticas agregadas sobre estos servicios ([116]).

([110]) Anexo I, sección III, punto 11, letra d, inciso i.

([111]) Anexo I, sección III, punto 11, letra d, inciso i.

([112]) Es la autoridad encargada de la tramitación designada por el panel de las APD contemplado en el principio complementario sobre la función de las autoridades de protección de datos (anexo I, sección III, punto 5).

([113]) Anexo I, sección III, punto 11, letra d.

([114]) Anexo I, sección II, punto 7, y sección III, punto 11, letra e.

([115]) Anexo I, sección III, punto 11, letra d, inciso ii.

([116]) Dicho informe anual expondrá: 1) el número total de reclamaciones relacionadas con el Marco de Privacidad de Datos UE-EE. UU. que se hayan recibido durante el año de referencia; 2) la naturaleza de las reclamaciones recibidas; 3) las medidas tomadas respecto de la calidad de la solución de controversias, como, por ejemplo, la duración de la tramitación de las reclamaciones; y 4) el resultado de las reclamaciones tramitadas, a saber, el número y el tipo de medidas reparatorias dictadas o de sanciones impuestas.

(71) Como parte de sus procedimientos de control del cumplimiento, el Departamento de Comercio puede verificar que las entidades participantes estén dadas de alta realmente ante los órganos independientes de impugnación que ellas mismas han especificado ([117]). Las entidades y los órganos independientes de impugnación competentes deben responder rápidamente a las consultas y solicitudes de información del Departamento de Comercio relacionadas con el Marco de Privacidad de Datos UE-EE. UU. El Departamento de Comercio debe colaborar con los órganos independientes de impugnación para verificar que incluyen en sus sitios web información sobre los principios en materia de privacidad y los servicios que prestan en el Marco de Privacidad de Datos UE-EE. UU. y que publican informes anuales ([118]).

(72) Cuando la entidad incumpla la resolución del organismo de resolución de controversias o del organismo del ámbito autorregulatorio, este debe notificar dicho incumplimiento al Departamento de Comercio y a la Comisión Federal de Comercio (o a otra autoridad estadounidense competente para investigar el incumplimiento de la entidad) o al órgano jurisdiccional competente ([119]). Si la entidad se niega a cumplir la resolución firme del organismo del ámbito autorregulatorio en materia de privacidad, del organismo independiente de resolución de controversias o de un organismo público competente o si dicho organismo determina que la entidad incumple frecuentemente los principios en materia de privacidad, tal circunstancia se puede considerar un incumplimiento sistemático, lo que tiene como consecuencia que el Departamento de Comercio, tras notificar a la entidad con treinta días de antelación y brindarle la oportunidad de responder, elimina a dicha entidad de la lista del Marco de Privacidad de Datos ([120]). Si, una vez eliminada de la lista, la entidad sigue afirmando participar en el Marco de Privacidad de Datos UE-EE. UU., el Departamento de Comercio debe remitir el asunto a la Comisión Federal de Comercio u otro organismo de garantía del cumplimiento ([121]).

(73) En tercer lugar, los particulares también pueden presentar sus reclamaciones a las APD nacionales de la UE, que pueden ejercer las competencias investigativas y correctivas que les atribuye el Reglamento (UE) 2016/679. Las entidades están obligadas a cooperar en la investigación y la resolución de las reclamaciones por parte de las APD por lo que respecta al tratamiento de datos de recursos humanos recogidos en el marco de la relación laboral o cuando la entidad en cuestión se haya sometido voluntariamente a la supervisión por parte de las APD ([122]). En concreto, las entidades deben responder a las consultas, acatar los dictámenes de las APD, en particular las medidas reparatorias o indemnizatorias, y comunicar por escrito a las APD la toma de las medidas correspondientes ([123]). En caso de incumplimiento de los dictámenes de las APD, estas remitirán el asunto al Departamento de Comercio (que puede eliminar a las entidades correspondientes de la lista del Marco de Privacidad de Datos) o, con fines coercitivos, a la Comisión Federal de Comercio o al Departamento de Transporte (el incumplimiento del compromiso de cooperar con las APD, así como de los principios en materia de privacidad, puede ser objeto de acciones de ejecución forzosa en virtud del Derecho estadounidense) ([124]).

(74) Para facilitar la cooperación a efectos de una tramitación eficaz de las reclamaciones, tanto el Departamento de Comercio como la Comisión Federal de Comercio han nombrado un punto de contacto específico responsable del contacto directo con las APD ([125]). Estos puntos de contacto ayudan a resolver las consultas de las APD sobre el cumplimiento de los principios en materia de privacidad por parte de una entidad en concreto.

(75) Las APD emiten el dictamen ([126]) una vez que las partes enfrentadas hayan dispuesto de tiempo razonable para formular sus observaciones y aportar las pruebas que deseen. El panel trata de pronunciarse 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 ([127]). Si la entidad no cumple transcurridos veinticinco días desde que se recibió el dictamen y no ha dado una explicación satisfactoria sobre el retraso, el panel puede notificar su intención ya sea de remitir la reclamación a la Comisión Federal de Comercio (u otro organismo de garantía del cumplimiento estadounidense),

([117]) Anexo I, sección «Verificar los requisitos para la autocertificación».
([118]) Véase el anexo III, sección «Facilitar la cooperación con los organismos de resolución alternativa de controversias que prestan servicios relacionados con los principios en materia de privacidad». Véase también el anexo I, sección III, punto 11, letra d, incisos ii) a iii).
([119]) Véase el anexo I, sección III, punto 11, letra e.
([120]) Véase el anexo I, sección III, punto 11, letra g, en particular los incisos ii y iii.
([121]) Véase el anexo I, epígrafe «Detectar y corregir las declaraciones falsas de participación».
([122]) Anexo I, sección II, punto 7, letra b.
([123]) Anexo I, sección III, punto 5.
([124]) Anexo I, sección III, punto 5, letra c, inciso ii.
([125]) Anexo III (véase el epígrafe «Facilitar la cooperación con las APD») y anexo IV (véanse los epígrafes «Investigaciones y priorización de las reclamaciones remitidas» y «Cooperación con las APD de la UE para la garantía del cumplimiento»).
([126]) El reglamento interno del panel informal de las APD deben aprobarlo las APD en virtud de su competencia para organizar su trabajo y cooperar entre sí.
([127]) Anexo I, sección III, punto 5, letra c, inciso i.

ya sea de certificar que se ha vulnerado gravemente el compromiso de cooperar. El primer supuesto puede desencadenar un procedimiento de garantía del cumplimiento con arreglo al artículo 5 de la Ley de la Comisión Federal de Comercio (u otra ley equivalente) ([128]). En el segundo supuesto, el panel informa al Departamento de Comercio, que debe considerar que la negativa de la entidad a cumplir el dictamen del panel de la APD constituye un incumplimiento sistemático y, por tanto, eliminarla de la lista del Marco de Privacidad de Datos.

(76) Si la APD a la que se ha dirigido la reclamación no toma medidas al respecto o estas son insuficientes, el reclamante puede impugnar judicialmente esta situación en el Estado miembro de la UE de que se trate.

(77) Los particulares también pueden presentar reclamaciones a las APD, incluso cuando el panel de las APD no haya sido designado como organismo de resolución de controversias de la entidad. En estos casos, la APD puede remitir dichas reclamaciones al Departamento de Comercio o a la Comisión Federal de Comercio. Con el fin de facilitar y mejorar la cooperación en lo relativo a las reclamaciones de particulares y al incumplimiento por parte de las entidades participantes, el Departamento de Comercio debe nombrar un punto de contacto específico que servirá de enlace y ayudará a resolver las consultas de las APD sobre el cumplimiento de los principios en materia de privacidad por parte de una entidad en concreto ([129]). Asimismo, la Comisión Federal de Comercio se ha comprometido a nombrar un punto de contacto específico ([130]).

(78) 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 en materia de privacidad por parte de las entidades ([131]). A tal efecto, ha establecido procedimientos especiales para que las APD puedan remitir las reclamaciones al punto de contacto específico, realizar un seguimiento de las mismas y cooperar con las entidades interesadas para facilitar su resolución ([132]). Con objeto de agilizar la tramitación de las reclamaciones de los particulares, el punto de contacto trata directamente con la APD pertinente las cuestiones relacionadas con el cumplimiento y, en particular, la pone al tanto del estado de las reclamaciones en un plazo no superior a los noventa días siguientes a la remisión de estas ([133]). De este modo, los interesados pueden presentar las reclamaciones por incumplimiento de las entidades participantes directamente ante su APD nacional, y esta puede remitirlas al Departamento de Comercio, que es la autoridad estadounidense encargada de la administración del Marco de Privacidad de Datos UE-EE. UU.

(79) Si, a partir de sus verificaciones de oficio, de las reclamaciones recibidas o de cualquier otra información, el Departamento de Comercio llega a la conclusión de que una entidad ha incumplido de forma sistemática los principios en materia de privacidad, puede eliminarla de la lista del Marco de Privacidad de Datos ([134]). Se considera incumplimiento sistemático la negativa a cumplir la resolución firme del organismo del ámbito autorregulatorio en materia de privacidad, del organismo independiente de resolución de controversias o de un organismo público competente, incluidas las APD ([135]).

(80) En quinto lugar, las entidades participantes deben estar sujetas a la competencia de las autoridades estadounidenses, en particular de la Comisión Federal de Comercio ([136]), que disponen de las competencias de investigación y ejecución forzosa necesarias para garantizar efectivamente el cumplimiento de los principios en materia de privacidad. La Comisión Federal de Comercio da prioridad a las reclamaciones por incumplimiento de los principios en materia de privacidad remitidas por los organismos independientes de resolución de controversias o los organismos del ámbito autorregulatorio, el Departamento de Comercio y las APD (de oficio o previa reclamación) para determinar si se ha vulnerado el artículo 5 de la Ley de la Comisión Federal de Comercio ([137]). La Comisión Federal de Comercio se ha comprometido a crear un procedimiento normalizado de remisión, a nombrar un punto de contacto de entre su personal al que las APD puedan remitir las reclamaciones y a intercambiar información sobre las reclamaciones remitidas. Asimismo, puede admitir a trámite las reclamaciones que presenten directamente los particulares y emprender investigaciones de oficio en relación con el Marco de Privacidad de Datos UE-EE. UU., en particular como parte de su actividad de investigación más amplia de cuestiones relacionadas con la privacidad.

([128]) Anexo I, sección III, punto 5, letra c, inciso ii.

([129]) Véase el anexo III, epígrafe «Facilitar la cooperación con las APD».

([130]) Véase el anexo IV, epígrafes «Investigaciones y priorización de las reclamaciones remitidas» y «Cooperación con las APD de la UE para la garantía del cumplimiento».

([131]) Anexo III, véase, por ejemplo, el epígrafe «Facilitar la cooperación con las APD».

([132]) Anexo I, sección II, punto 7, letra e, y anexo III, epígrafe «Facilitar la cooperación con las APD».

([133]) *Véase la nota anterior.*

([134]) Anexo I, sección III, punto 11, letra g.

([135]) Anexo I, sección III, punto 11, letra g.

([136]) Las entidades participantes tienen que declarar públicamente su compromiso de cumplir los principios en materia de privacidad, publicar sus directrices en materia privacidad de conformidad con estos principios y ponerlos en práctica en su totalidad. El incumplimiento puede perseguirse con arreglo al artículo 5 de la Ley de la Comisión Federal de Comercio, por el que se prohíben los actos desleales o engañosos en el comercio o que afectan al mismo.

([137]) Véanse también los compromisos similares asumidos por el Departamento de Transporte en el anexo V.

(81) 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 del particular, el interesado de la UE puede solicitar la incoación de un proceso arbitral vinculante al Panel del Marco de Privacidad de Datos UE-EE. UU. ([138]). Las entidades deben informar a los particulares sobre la posibilidad de solicitar la incoación de un proceso arbitral vinculante y están obligadas a dar respuesta cuando el particular presente dicha solicitud ([139]).

(82) El Panel del Marco de Privacidad de Datos UE-EE. UU. está integrado por un grupo mínimo de diez árbitros nombrados por el Departamento de Comercio y la Comisión Europea por su destacada independencia, integridad y experiencia con la normativa estadounidense en materia de privacidad y la normativa de la Unión en materia de protección de datos. En cada litigio, las partes seleccionan de este grupo un tribunal arbitral compuesto por uno o tres árbitros ([140]).

(83) El Centro Internacional de Resolución de Controversias (International Centre for Dispute Resolution), que es la división internacional de la Asociación Estadounidense de Arbitraje (American Arbitration Association) (denominadas conjuntamente en lo sucesivo «el CIRC y la AEA»), fue seleccionado por el Departamento de Comercio para gestionar los arbitrajes. Los procesos de los que conozca el Panel del Marco de Privacidad de Datos UE-EE. UU. se rigen por un conjunto pactado de reglas de arbitraje y un código de conducta para los árbitros. El sitio web del CIRC y la AEA ofrece información clara y concisa a los particulares sobre el arbitraje y el procedimiento para solicitar la incoación del proceso arbitral.

(84) Las reglas de arbitraje acordadas por el Departamento de Comercio y la Comisión Europea complementan el Marco de Privacidad de Datos UE-EE. UU., que cuenta con varios elementos que facilitan el recurso a esta vía por parte de los interesados de la UE: i) en la preparación de sus alegaciones ante el tribunal arbitral, el interesado puede recibir ayuda de su APD nacional; ii) si bien el arbitraje se debe celebrar en los EE. UU., los interesados de la UE pueden participar, si lo desean, por videoconferencia o conferencia telefónica sin coste alguno para ellos; iii) si bien el arbitraje se debe desarrollar, en principio, en inglés, previa solicitud motivada, normalmente se proporciona un servicio de traducción e interpretación en las audiencias arbitrales sin coste para el interesado; iv) por último, si bien cada parte debe pagar los honorarios de sus respectivos abogados en caso de contar con representación letrada ante el tribunal arbitral, el fondo creado por el Departamento de Comercio y financiado con las aportaciones anuales de las entidades participantes ha de sufragar los gastos del proceso arbitral hasta los importes máximos que determinen las autoridades estadounidenses tras consultarlo con la Comisión Europea ([141]).

(85) El Panel del Marco de Privacidad de Datos UE-EE. UU. tiene competencia para imponer las medidas específicas, equitativas y no monetarias ([142]) necesarias para reparar el incumplimiento de los principios en materia de privacidad. Si bien el tribunal arbitral debe tener en cuenta en su apreciación las medidas de reparación que ya se hayan dictado en las demás vías de impugnación que contempla el Marco de Privacidad de Datos UE-EE. UU., los particulares afectados pueden recurrir de todos modos al arbitraje si consideran que tales medidas son insuficientes. De este modo, los interesados de la UE pueden solicitar la incoación de un proceso arbitral en todos aquellos casos en los que, por la actuación u omisión de las entidades participantes, los órganos independientes de impugnación o las autoridades estadounidenses competentes (por ejemplo, la Comisión Federal de Comercio) no se haya resuelto de manera satisfactoria sus reclamaciones. No se puede solicitar la incoación de un proceso arbitral si la APD esté facultada para resolver la reclamación en cuestión con respecto a la entidad participante, en particular cuando la entidad tenga la obligación de cooperar y de acatar los dictámenes de las APD en relación con el tratamiento de los datos de recursos humanos recogidos en el marco de relaciones laborales o se haya comprometido voluntariamente a hacerlo. En virtud de la Ley federal de arbitraje, los particulares pueden solicitar a los órganos jurisdiccionales estadounidenses la ejecución forzosa del laudo arbitral, lo que constituye una garantía para aquellos en caso de incumplimiento por parte de la entidad.

([138]) Véase el anexo I del anexo I, «Modelo de arbitraje».
([139]) Véase el anexo I, sección II, punto 1, letra a, inciso xi, y punto 7, letra c.
([140]) El número de árbitros que integran el tribunal arbitral deben acordarlo las partes.
([141]) Anexo I del anexo I, sección G, punto 6.
([142]) Los particulares no pueden demandar una indemnización por daños y perjuicios en el proceso arbitral, pero el hecho de recurrir al arbitraje no impide demandar tal indemnización ante los órganos jurisdiccionales ordinarios estadounidenses.

(86) En séptimo lugar, si la entidad no cumple su compromiso de cumplir los principios en materia de privacidad y las directrices en materia de privacidad que ha publicado, la normativa estadounidense también contempla acciones judiciales, como la de indemnización por daños y perjuicios. Por ejemplo, en determinadas condiciones, los particulares pueden ejercitar acciones judiciales (incluida la de indemnización por daños y perjuicios) con arreglo a la legislación de los Estados federados en materia de consumo en casos de engaños fraudulentos y de actos o prácticas desleales o engañosos ([143]) y con arreglo al Derecho sobre la responsabilidad civil (en particular, la responsabilidad por violación de la privacidad ([144]), por apropiación del nombre o la imagen ([145]) y por injuria con publicidad ([146])).

(87) En conjunto, las distintas vías procesales antes descritas garantizan que las reclamaciones por incumplimiento del Marco de Privacidad de Datos UE-EE. UU. por parte de las entidades certificadas sean resueltas de forma efectiva y se tomen medidas de reparación.

3. ACCESO A LOS DATOS PERSONALES TRANSFERIDOS DESDE LA UNIÓN EUROPEA Y USO DE ESTOS POR PARTE DE LOS PODERES PÚBLICOS ESTADOUNIDENSES

(88) La Comisión ha evaluado asimismo las limitaciones y garantías previstas, incluidos los mecanismos de supervisión y las vías de impugnación para los particulares contemplados en el Derecho estadounidense en lo que respecta a la recogida y la utilización ulterior por los poderes públicos estadounidenses de los datos personales transferidos a responsables y encargados del tratamiento en los EE. UU. en aras del interés público, en particular a efectos penales y de seguridad nacional (acceso de los poderes públicos) ([147]). A la hora de evaluar si, con arreglo a la presente Decisión, las condiciones en las que el acceso de los poderes públicos a los datos transferidos a los EE. UU. superan la prueba de la equivalencia sustancial a efectos del artículo 45, apartado 1, del Reglamento (UE) 2016/679, según la interpretación del TJUE a la luz de la Carta de los Derechos Fundamentales, la Comisión tuvo en cuenta, en particular, los criterios siguientes.

(89) En particular, cualquier limitación del ejercicio del derecho a la protección de los datos personales debe ser establecida por ley, y la base legal que permita la injerencia en dicho derecho debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate ([148]). Además, para cumplir el requisito de proporcionalidad, según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario en una sociedad democrática para lograr objetivos específicos de interés general equivalentes a los reconocidos por la Unión, la base legal debe establecer reglas claras y precisas que regulen el alcance y la aplicación de las medidas en cuestión e imponer unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso ([149]). Por otra parte, estas reglas y garantías deben ser exigibles

([143]) Véase, por ejemplo, la legislación de los Estados federados de protección de los consumidores: California [Código Civil de California (Cal. Civ. Code), artículos 1750 a 1785; Ley de medidas de reparación para los consumidores (Consumers Legal Remedies Act)], Distrito de Columbia [Código del Distrito de Columbia (D.C. Code), título 28, capítulo 39, artículo 1], Florida [Legislación de Florida (Fla. Stat.), capítulo 501, artículos 201 a 213; Ley sobre las prácticas comerciales desleales y engañosas (Deceptive and Unfair Trade Practices Act)], Illinois [Repertorio de leyes de Illinois (Ill. Comp. Stat.), capítulo 815, ley 505, artículos 1 a 12; Ley sobre el fraude a los consumidores y las prácticas empresariales engañosas (Consumer Fraud and Deceptive Business Practices Act)]; Pennsylvania [Repertorio de leyes de Pennsylvania (Pa. Stat. Ann.), título 73, ley 201, artículos 1 a 9 *quater*; Ley sobre las prácticas empresariales desleales y la protección de los consumidores (Unfair Trade Practices and Consumer Protection Law)].

([144]) Es decir, la injerencia dolosa en los asuntos o negocios privados de un particular de una manera que sería muy ofensiva para una persona razonable [Compendio de principios jurisprudenciales, volumen segundo (responsabilidad civil) (Restatement of Torts, Second), artículo 652 *ter*].

([145]) Esta responsabilidad nace cuando alguien utiliza el nombre o la imagen de otro para anunciar una empresa o un producto, o para algún fin mercantil similar [Compendio de principios jurisprudenciales, volumen segundo (responsabilidad civil), artículo 652 *quater*].

([146]) Es decir, cuando se hace pública información sobre la vida privada de un particular, ello sería muy ofensivo para una persona razonable y la información no es de interés público [Compendio de principios jurisprudenciales, volumen segundo (responsabilidad civil), artículo 652 *quinquies*].

([147]) Este aspecto es importante especialmente en relación con la sección I, punto 5, del anexo I. De conformidad con dicha sección y también con el RGPD, se puede establecer limitaciones al cumplimiento y respeto de las exigencias y derechos en materia de protección de datos que forman parte de los principios en materia de privacidad. Sin embargo, esas limitaciones no son absolutas; solo pueden hacerse efectivas en ciertas condiciones, por ejemplo en la medida necesaria para dar cumplimiento a una resolución judicial o a obligaciones de interés público, policiales o de seguridad nacional. En este contexto y para mayor claridad, la sección se refiere también a las condiciones fijadas en el Decreto Presidencial n.º 14086 que se analizan, entre otros, en los considerandos 127 a 141.

([148]) Véase Schrems II, apartados 174 y 175 y la jurisprudencia citada. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véanse también el asunto C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs y otros, ECLI:EU:C:2020:790, apartado 65, y los asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros/Premier ministre y otros, ECLI:EU:C:2020:791, apartado 175.

([149]) Véase Schrems II, apartados 176 y 181 y la jurisprudencia citada. En relación con el acceso por parte de las autoridades públicas de los Estados miembros, véanse también Privacy International/Secretary of State for Foreign and Commonwealth Affairs y otros, apartado 68, y La Quadrature du Net y otros/Premier ministre y otros, apartado 132.

por los particulares y vinculantes ([150]). En concreto, los interesados han de tener la posibilidad de ejercer acciones en Derecho ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión ([151]).

3.1. **Acceso y uso por parte de los poderes públicos estadounidenses con fines penales**

(90) Por lo que se refiere a las injerencias en los datos personales transferidos en el Marco de Privacidad de Datos UE-EE. UU. con fines penales, la normativa estadounidense impone una serie de limitaciones al acceso a los datos personales y su uso y contempla mecanismos de supervisión y vías de impugnación que se ajustan a las exigencias mencionadas en el considerando 89 de la presente Decisión. Las condiciones en las que se puede tener acceso y las garantías aplicables al ejercicio de estas competencias se precisan con detalle en las secciones siguientes. A este respecto, el Ejecutivo estadounidense [a través del Departamento de Justicia (Department of Justice)] también se ha comprometido a aplicar con rigor las limitaciones y garantías contempladas (anexo VI de la presente Decisión).

3.1.1. ***Base jurídica, limitaciones y garantías***

3.1.1.1. *Limitaciones y garantías respecto de la recogida de datos personales con fines penales*

(91) Los fiscales federales y los agentes de investigación federales estadounidenses pueden acceder a los datos personales tratados por entidades estadounidenses certificadas que se transfieran desde la Unión al amparo del Marco de Privacidad de Datos UE-EE. UU. con fines penales con arreglo a procedimientos diferentes, como se explica con más detalle en los considerandos 92 a 99. Estos procedimientos se aplican también cuando la información se obtiene de cualquier entidad estadounidense, independientemente de la nacionalidad o el lugar de residencia de los interesados afectados ([152]).

(92) En primer lugar, a petición de un agente de policía federal o de un abogado del Estado, el juez puede dictar una orden de registro o incautación (incluida la información almacenada electrónicamente) ([153]). Tal orden solo puede dictarse si existe una causa probable ([154]) de que los elementos objeto de incautación (pruebas de un delito, objetos de posesión ilegal o bienes utilizados en la comisión de un delito o diseñados o destinados con tal fin) se encuentren en el lugar especificado en la orden. La orden debe especificar los bienes u objetos que deban incautarse y designar al juez al

([150]) Véase Schrems II, apartados 181 y 182.

([151]) Véase Schrems I, apartado 95, y Schrems II, apartado 194. En ese sentido, el TJUE ha destacado en particular que el cumplimiento del artículo 47 de la Carta de los Derechos Fundamentales, que garantiza el derecho a la tutela judicial efectiva ante un juez independiente e imparcial, «forma parte también del nivel de protección exigido dentro de la Unión cuyo respeto debe ser constatado por la Comisión antes de adoptar una decisión de adecuación en virtud del artículo 45, apartado 1, del RGPD» (Schrems II, apartado 186).

([152]) Véase el anexo VI. Véase, por ejemplo, con respecto a la Ley de interceptación de comunicaciones (Wiretail Act), la Ley de comunicaciones almacenadas (Stored Communications Act) y la Ley de registro de comunicaciones salientes (Pen Register Act) (mencionadas con más detalle en los considerandos 95 a 98), el asunto Suzlon Energy Ltd c. Microsoft Corp., volumen 671, tercera serie del Repertorio Jurisprudencial Federal (Federal Reporter), páginas 726 a 729 (Corte de Apelaciones del Noveno Circuito, 2011).

([153]) Código Procesal Penal Federal (Federal Rules of Criminal Procedure), artículo 41. En una sentencia de 2018, la Corte Suprema (Supreme Court) confirmó que también es necesaria una orden de registro o una dispensa de orden para que las autoridades policiales consulten el historial de ubicaciones de los móviles, que ofrecen una visión general de los movimientos del usuario y respecto del cual el usuario debe poder tener una expectativa razonable de privacidad (Timothy Ivory Carpenter c. United States of America, volumen 16-402, página 585, del Repertorio Jurisprudencial de los EE. UU., de 2018). En consecuencia, por lo general no pueden obtenerse estos datos de una empresa de telefonía móvil en virtud de una resolución judicial simplemente por existir motivos razonables para creer que la información es pertinente e importante para una investigación penal en curso, sino que es preciso demostrar la existencia de una causa probable cuando se pretende utilizar una orden judicial.

([154]) Según la Corte Suprema, la causa probable es un estándar práctico, no técnico, que va referido a las consideraciones fácticas y prácticas de la vida cotidiana en las que los hombres razonables y prudentes se basan para actuar (Illinois c. Gates; volumen 462, páginas 213 y 232, del Repertorio Jurisprudencial de los EE. UU., de 1983). Por lo que se refiere a las órdenes de registro, existe causa probable cuando sea bastante razonable creer que con el registro puedan hallarse de pruebas de un delito.

que debe devolverse la orden. La persona objeto de un registro o cuyo patrimonio sea objeto de registro puede impugnar las pruebas obtenidas o derivadas de un registro ilícito si dichas pruebas se aportan en su contra durante el proceso penal ([155]). Cuando se exija al titular de los datos (por ejemplo, una empresa) que comunique los datos en virtud de una orden judicial, este puede, en particular, impugnar la orden si esta resulta excesivamente onerosa ([156]).

(93) En segundo lugar, en la investigación de determinados delitos graves ([157]), normalmente a petición de un fiscal federal, el jurado de acusación (sección instructora del órgano jurisdiccional para la que se nombra un juez penal o un juez de paz) puede dictar un requerimiento para exigir a alguien que presente o aporte de otro modo documentos empresariales, información almacenada electrónicamente u otros elementos tangibles. Además, son varias las leyes que autorizan el uso de los requerimientos administrativos para que se presenten o aporten de otro modo documentos empresariales, información almacenada electrónicamente u otros elementos tangibles en las investigaciones relacionadas con el fraude sanitario, el maltrato infantil, la protección de los servicios secretos y las sustancias controladas, así como las investigaciones de los inspectores generales ([158]). En ambos casos, la información debe ser pertinente para la investigación y el requerimiento no puede ser irrazonable, por ser excesivo, opresivo u oneroso (y puede ser impugnado por el destinatario por estos motivos) ([159]).

(94) Condiciones muy similares se aplican a los requerimientos administrativos dictados para conseguir acceso a datos en posesión de empresas estadounidenses con fines civiles o regulatorios (interés público). La competencia de los organismos que tengan responsabilidades civiles o regulatorias para dictar requerimientos administrativos debe establecerse por ley. El empleo de los requerimientos administrativos está sujeto a una prueba de verosimilitud, según la cual es preciso que la investigación persiga una finalidad legítima, que la información solicitada con el requerimiento administrativo sea pertinente para esa finalidad, que el organismo no tenga ya la información que solicita y que se respete el procedimiento administrativo para dictar el requerimiento administrativo ([160]). La Corte Suprema ha aclarado en su jurisprudencia que es necesario hallar un equilibrio entre la importancia del interés público de la información solicitada y la importancia de los intereses privados personales y organizativos ([161]). Si bien los requerimientos administrativos no están sometidos a aprobación judicial previa, si son controlados judicialmente si los recurre el destinatario por los motivos antes mencionados o si el organismo trata de ejecutar forzosamente el requerimiento administrativo por la vía judicial ([162]). Además de estas limitaciones generales transversales, en leyes específicas pueden establecerse requisitos específicos más estrictos ([163]).

([155]) Asunto Mapp c. Ohio; volumen 367, página 643, del Repertorio Jurisprudencial de los EE. UU., de 1961.

([156]) Véase el asunto In re Application of United States, volumen 610, segunda serie del Repertorio Jurisprudencial Federal, páginas 1148 a 1157 (Corte de Apelaciones del Tercer Circuito, 1979), donde se sostiene que el respeto de las debidas garantías procesales exige resolver la cuestión de la onerosidad antes de obligar a la compañía telefónica a prestar ayuda para ejecutar la orden de registro; véase asimismo el asunto In re Application of United States, volumen 616, segunda serie del Repertorio Jurisprudencial Federal, página 1122 (Corte de Apelaciones del Noveno Circuito, 1980).

([157]) La quinta enmienda de la Constitución de los EE. UU. exige que la acusación por los delitos castigados con pena capital y los demás delitos graves la formule el jurado de acusación. El jurado de acusación está compuesto por entre dieciséis y veintitrés jurados y se pronuncia acerca de si existe causa probable para creer que se ha cometido el delito. Para llegar a este veredicto, los jurados de acusación están dotados de facultades de investigación con arreglo a las cuales pueden dictar requerimientos.

([158]) Véase el anexo VI.

([159]) Código Procesal Penal Federal, artículo 17.

([160]) Asunto United States c. Powell; volumen 379, página 48, del Repertorio Jurisprudencial de los EE. UU., de 1964.

([161]) Asunto Oklahoma Press Publishing Co. c. Walling; volumen 327, página 186, del Repertorio Jurisprudencial de los EE. UU., de 1946.

([162]) La Corte Suprema ha aclarado que, cuando se recurre un requerimiento administrativo, el órgano jurisdiccional debe valorar si 1) la investigación persigue una finalidad autorizada lícita, 2) la competencia para dictar el requerimiento administrativo en cuestión está bajo el control del Congreso y 3) los documentos solicitados son pertinentes para la investigación. La Corte también señaló que los requerimientos administrativos deben ser razonables, es decir, que deben especificar los documentos que se solicitan de forma adecuada, pero no excesiva, para las finalidades de la investigación en cuestión y deben ser detallados en cuanto a la descripción del lugar, las personas o los artículos objeto de registro.

([163]) Por ejemplo, la Ley del derecho a la privacidad financiera otorga a los organismos públicos la competencia para recabar los documentos económicos y financieros en poder de entidades financieras en virtud de un requerimiento administrativo solo si 1) existen motivos para creer que los documentos en cuestión son pertinentes para una investigación policial legítima y 2) se ha trasladado una copia del requerimiento administrativo o emplazamiento al cliente junto con una notificación en la que se especifique razonablemente la naturaleza de la investigación (título 12, artículo 3425, del Código de Estados Unidos). Otro ejemplo es la Ley sobre la imparcialidad de las fichas de información crediticia, que prohíbe a las agencias de información sobre clientes entregar las fichas de clientes al recibir un requerimiento administrativo (solo tienen la obligación de responder a los requerimientos del jurado de acusación o a las resoluciones judiciales; título 15, artículo 1681 y ss., del Código de Estados Unidos). Por lo que se refiere a comunicar información, son de aplicación las obligaciones específicas de la Ley de comunicaciones almacenadas, en particular con respecto a la posibilidad de utilizar requerimientos administrativos (en los considerandos 96 a 97 se puede encontrar una explicación más pormenorizada).

(95) En tercer lugar, hay varias bases legales que permiten a las autoridades acceder con fines penales a los datos de comunicaciones. Los órganos jurisdiccionales pueden dictar una resolución por la que se autorice la recogida, en tiempo real, de información no sustantiva sobre el marcado, el enrutamiento, el direccionamiento y la señalización de un número de teléfono o de una dirección de correo electrónico (mediante el empleo de dispositivos de registro de comunicaciones salientes y entrantes) si considera que la autoridad solicitante ha justificado que la información que probablemente se obtendrá es pertinente para una investigación penal en curso ([164]). La resolución judicial debe, entre otras cuestiones, especificar la identidad, si se conoce, del sospechoso, las características de las comunicaciones a las que se aplica y el delito al que se refiere la información que debe recogerse. El empleo de dispositivos de registro de comunicaciones salientes y entrantes puede autorizarse por un período máximo de sesenta días, que solo puede prorrogarse mediante una nueva resolución judicial.

(96) Además, el acceso con fines penales a la información de los usuarios digitales, los datos de tráfico y el contenido almacenado de las comunicaciones que obran en poder de las empresas de servicios de internet, las compañías telefónicas y otras empresas externas de servicios puede venir autorizado por la Ley de comunicaciones almacenadas ([165]). Para obtener el contenido almacenado de las comunicaciones electrónicas, las autoridades policiales deben, por lo general, solicitar una orden judicial que se fundamente en la existencia de una causa probable para considerar que la cuenta en cuestión alberga pruebas de un delito ([166]). Las autoridades policiales pueden solicitar un requerimiento para obtener información del registro de abonados, las direcciones IP, los sellos de tiempo correspondientes y la información de la facturación. Para la mayoría de la demás información almacenada no sustantiva, como los encabezados de los correos electrónicos sin el asunto, las autoridades policiales deben solicitar una resolución judicial, que solo se dicta si el juez considera que existen motivos razonables para creer que la información es pertinente e importante para una investigación penal en curso.

(97) Las empresas que reciben solicitudes en virtud de la Ley de comunicaciones almacenadas pueden notificárselo voluntariamente al cliente o usuario cuya información se solicita, salvo cuando la autoridad policial competente consiga que se dicte una medida cautelar que prohíba dicha notificación ([167]). Tal medida cautelar es una resolución judicial que obliga a la empresa de servicios de comunicaciones electrónicas o de servicios informáticos remotos a la que se dirige la orden, requerimiento o resolución judicial a no notificar a ninguna otra persona la existencia de dicha orden, requerimiento o resolución judicial mientras el órgano jurisdiccional lo considere oportuno. Esta medida cautelar se dicta si el órgano jurisdiccional considera que existen motivos para creer que la notificación pondría en grave peligro la investigación o retrasaría indebidamente el juicio, por ejemplo, porque pondría en peligro la vida o la integridad física de una persona, podría propiciar la huida del sospechoso, podría desencadenar la intimidación de posibles testigos, etc. Hay una Circular del secretario de Justicia adjunto (Deputy Attorney General) (que es vinculante para todos los funcionarios y cargos del Departamento de Justicia) que exige a los fiscales que justifiquen minuciosamente la necesidad de la medida cautelar y aclaren al órgano jurisdiccional cómo se cumplen los requisitos legales para que se dicte la medida cautelar en ese caso concreto ([168]). La Circular también exige que las solicitudes de medidas cautelares no tengan por objeto, en general, retrasar la notificación durante más de un año. Si, en circunstancias excepcionales, es necesario que la medida cautelar despliegue sus efectos durante más tiempo, ello solo puede solicitarse con la firma por escrito del supervisor designado por el secretario de Justicia de los EE. UU. o el fiscal general adjunto (Assistant Attorney General) correspondiente. Además, al archivar la investigación, el fiscal debe valorar inmediatamente si existen motivos para no dejar sin efecto las medidas cautelares relacionadas y, en caso contrario, dejarlas sin efecto y asegurarse de que se notifique a la empresa de servicios ([169]).

([164]) Título 18, artículo 3123, del Código de Estados Unidos.

([165]) Título 18, artículos 2701 a 2713, del Código de Estados Unidos.

([166]) Título 18, artículo 2701, letra a) y letra b), punto 1, subletra A), del Código de Estados Unidos. Si se notifica al usuario o cliente afectado (ya sea por anticipado o, en determinadas circunstancias, con una notificación retrasada), la información sustantiva almacenada durante más de 180 días también puede obtenerse en virtud de un requerimiento administrativo o un requerimiento del jurado de acusación [título 18, artículo 2701, letra b), punto 1, subletra B), del Código de Estados Unidos] o de una resolución judicial, si existen motivos razonables para creer que la información es pertinente e importante para una investigación penal en curso [título 18, artículo 2701, letra d), del Código de Estados Unidos]. Sin embargo, de conformidad con la sentencia de una corte federal de apelaciones, los investigadores del Ejecutivo suelen obtener órdenes judiciales de registro para obtener la parte sustantiva de las comunicaciones privadas o los datos almacenados de las empresas de servicios de comunicación. United States c. Warshak, volumen 631, tercera serie del Repertorio Jurisprudencial Federal, página 266 (Corte de Apelaciones del Sexto Circuito, 2010).

([167]) Título 18, artículo 2705, letra b), del Código de Estados Unidos.

([168]) Véase la Circular publicada el 19 de octubre de 2017 por el secretario de Justicia adjunto, Rod Rosenstein, sobre un régimen más restrictivo para las solicitudes de medidas cautelares (de no comunicación), disponible en inglés en https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Circular publicada el de 27 de mayo de 2022 por la secretaria de Justicia adjunto, Lisa Moncao, sobre directrices complementaria relativas a las solicitudes de medidas cautelares contempladas en el título 18, artículo 2705, letra b), del Código de Estados Unidos.

(98) Las autoridades policiales también pueden interceptar en tiempo real comunicaciones por cable, orales o electrónicas con arreglo a una resolución judicial en la que el juez considere, entre otros aspectos, que existe una causa probable para considerar que la escucha o la interceptación electrónica demostrará que se ha cometido un delito federal o permitirá conocer el paradero de un fugitivo de la justicia ([170]).

(99) Hay varias directrices e instrucciones del Departamento de Justicia que contemplan garantías adicionales, entre ellas, las Directrices del secretario de Justicia sobre las operaciones nacionales del Buró Federal de Investigaciones (en lo sucesivo, «FBI», por sus siglas en inglés), que, entre otros aspectos, exigen al FBI que sus métodos de investigación sean lo menos invasivos posible, teniendo en cuenta el efecto en la privacidad y en las libertades civiles ([171]).

(100) Según el Ejecutivo estadounidense, en el caso de las investigaciones policiales del ámbito de los Estados federados se aplican, como mínimo, las mismas garantías antes descritas (con respecto a las investigaciones llevadas a cabo en virtud del Derecho de los Estados federados) ([172]). En particular, hay disposiciones constitucionales, así como leyes y jurisprudencia de los Estados federados, que reafirman las garantías antes mencionadas contra los registros que no sean razonables al exigir que se dicte una orden de registro ([173]). De forma similar a las garantías establecidas en el ámbito federal, solo se puede dictar una orden de registro tras demostrar la existencia de una causa probable y se debe describir el lugar, las personas o los artículos objeto de registro ([174]).

([170]) Título 18, artículos 2510 a 2522, del Código de Estados Unidos.

([171]) Directrices del secretario de Justicia, de septiembre de 2008, sobre las operaciones nacionales del FBI («Directrices sobre el FBI»), disponibles en inglés en http://www.justice.gov/archive/opa/docs/guidelines.pdf. Figuran reglas y directrices sobre las limitaciones a las actividades de investigación de los fiscales federales en el Manual de Justicia de los Fiscales Estadounidenses (United States Attorneys' Manual); se puede consultar en inglés en http://www.justice.gov/usam/united-states-attorneys-manual. Para no seguir estas Directrices, debe obtenerse la aprobación previa del director del FBI, el director adjunto o el asistente ejecutivo designado por el director, a menos que dicha aprobación no pueda obtenerse debido a la inmediatez o la gravedad de la amenaza para la seguridad de las personas o el patrimonio o para la seguridad nacional (en cuyo caso, debe notificarse lo antes posible al director o a otra persona autorizada). Si no se siguen las Directrices, el FBI debe notificarlo al Departamento de Justicia, que a su vez informa al secretario de Justicia y al secretario de Justicia adjunto.

([172]) Anexo VI, nota a pie de página 2. Véanse también los asuntos Arnold c. City of Cleveland [67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993)] (en los ámbitos de los derechos individuales y las libertades civiles, la Constitución de los EE. UU., cuando sea aplicable a los Estados federados, fija un mínimo que las resoluciones de los órganos jurisdiccionales de los Estados federados no pueden incumplir), Cooper c. California [386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967)] (este pronunciamiento no afecta, por supuesto, a la competencia de los Estados federados de fijar estándares más garantistas para los registros e incautaciones que los establecidos por la Constitución federal si así lo desean) y Petersen c. City of Mesa [63 P.3d 309, 312 (Corte de Apelaciones de Arizona, 2003)] (si bien la Constitución de Arizona puede imponer estándares más estrictos para los registros e incautaciones que los de la Constitución federal, los órganos jurisdiccionales de Arizona no pueden brindar una protección inferior a la contemplada en la cuarta enmienda).

([173]) La mayoría de los Estados federados han reproducido las garantías de la cuarta enmienda en sus constituciones. Véase el artículo 1, apartado 5, de la Constitución de Alabama, el artículo 1, apartado 14, de la Constitución de Alaska, el artículo 2, apartado 15, de la Constitución de Arkansas, el artículo 1, apartado 13, de la Constitución de California, el artículo 2, apartado 7, de la Constitución de colorado, el artículo 1, apartado 7, de la Constitución de Connecticut, el artículo 1, apartado 6, de la Constitución de Delaware, el artículo 1, apartado 12, de la Constitución de Florida, el artículo 1, apartado 1, punto XIII, de la Constitución de Georgia, el artículo 1, apartado 7, de la Constitución de Hawái, el artículo 1, apartado 17, de la Constitución de Idaho, el artículo 1, apartado 6, de la Constitución de Illinois, el artículo 1, apartado 11, de la Constitución de Indiana, el artículo 1, apartado 8, de la Constitución de Iowa, el artículo 15 de la Carta de Derechos de la Constitución de Kansas, el artículo 10 de la Constitución de Kentucky, el artículo 1, apartado 5, de la Constitución de Luisiana, el artículo 1, apartado 5, de la Constitución de Maine, el artículo 14 de la Declaración de Derechos de la Constitución de Massachussetts, el artículo 1, apartado 11, de la Constitución de Míchigan, el artículo 1, apartado 10, de la Constitución de Minnesota, el artículo III, apartado 23, de la Constitución de Misisipi, el artículo 1, apartado 15, de la Constitución de Misuri, el artículo 2, apartado 11, de la Constitución de Montana, el artículo 1, apartado 7, de la Constitución de Nebraska, el artículo 1, apartado 18, de la Constitución de Nevada, la parte 1, artículo 19, de la Constitución de Nuevo Hampshire, el artículo 2, apartado 7, de la Constitución de Nueva Jersey, el artículo 2, apartado 10, de la Constitución de Nuevo México, el artículo 1, apartado 12, de la Constitución de Nueva York, el artículo 1, apartado 8, de la Constitución de Dakota del Norte, el artículo 1, apartado 14, de la Constitución de Ohio, el artículo 2, apartado 30, de la Constitución de Oklahoma, el artículo 1, apartado 9, de la Constitución de Oregón, el artículo 1, apartado 8, de la Constitución de Pensilvania, el artículo 1, apartado 6, de la Constitución de Rhode Island, el artículo 1, apartado 10, de la Constitución de Carolina del Sur, el artículo 6, apartado 11, de la Constitución de Dakota del Sur, el artículo 1, apartado 7, de la Constitución de Tennessee, el artículo 1, apartado 9, de la Constitución de Texas, el artículo 1, apartado 14, de la Constitución de Utah, el capítulo 1, artículo 11, de la Constitución de Vermont, el artículo 3, apartado 6, de la Constitución de Virginia Occidental, el artículo 1, apartado 11, de la Constitución de Wisconsin y el artículo 1, apartado 4, de la Constitución de Wyoming. Otros (como Maryland, Carolina del Norte y Virginia) han consagrado en sus constituciones menciones específicas para las órdenes que han sido interpretadas judicialmente en el sentido de que brindan un nivel de protección similar o mayor al de la cuarta enmienda; véanse el artículo 26 de la Declaración de Derechos de Maryland, el artículo 1, apartado 20, de la Constitución de Carolina del Norte, el artículo 1, apartado 10, de la Constitución de Virginia y la jurisprudencia pertinente [Hamel c. State, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008), State c. Johnson, 861 S.E.2d 474, 483 (N.C. 2021) y Lowe c. Commonwealth, 337 S.E.2d 273, 274 (Va. 1985)]. Por último, Arizona y Washington cuentan con preceptos constitucionales que protegen la privacidad de manera más general (el artículo 2, apartado 8, de la Constitución de Arizona y el artículo 1, apartado 7, de la Constitución de Washington), que han sido interpretadas judicialmente en el sentido de que brindan un nivel de protección mayor al de la cuarta enmienda [véanse las sentencias de los asuntos State c. Bolt, 689 P.2d 519, 523 (Ariz. 1984), State c. Ault, 759 P.2d 1320, 1324 (Ariz. 1988), State c. Myrick, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984) y State c. Young, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)].

([174]) Véanse, por ejemplo, el artículo 1524, apartado 3, letra b), del Código Penal de California (California Penal Code), el capítulo 3, artículos 6 a 13, del Código Procesal Penal de Alabama (Alabama Rules of Criminal Procedure), el título 10, capítulo 79, artículo 35, del Código de Leyes de Washington (Revised Code of Washington) y el título 19.2 (Procesal Penal), capítulo 5, artículo 59, del Código de Leyes de Virginia (Code of Virginia).

3.1.1.2. *Utilización ulterior de la información recogida*

(101) Por lo que se refiere al uso ulterior de los datos recogidos por las autoridades policiales federales, las diferentes leyes, directrices y normas imponen garantías específicas. Con la excepción de los instrumentos específicos aplicables a las actividades del FBI (las Directrices del secretario de Justicia sobre las operaciones nacionales del FBI y la Guía de Investigaciones y Operaciones Nacionales del FBI), las obligaciones descritas en esta sección se aplican con carácter general a los demás usos de los datos por las autoridades federales, en particular a los datos consultado o utilizados con fines civiles o regulatorios. Esto incluye por ejemplo las obligaciones derivadas de circulares o reglamentos de la Oficina de Gestión y Presupuesto, de la Ley de modernización de la gestión de la seguridad de la información federal (Federal Information Security Management Modernization Act), de la Ley de Administración digital y de la Ley de archivos federales.

(102) De conformidad con la competencia conferida por la Ley Clinger-Cohen [Clinger-Cohen Act; Compendio de Leyes de Derecho Público (Public Law), 104.º Congreso, Ley 106, división E] y la Ley de seguridad informática, de 1987 (Computer Security Act; Compendio de Leyes de Derecho Público, 100.º Congreso, Ley 235), la Oficina de Gestión y Presupuesto (Office of Management and Budget) publicó la Circular n.º A-130 para establecer directrices generales vinculantes de aplicación a todos los organismos federales (incluidas las autoridades policiales) cuando tratan información de identificación personal ([175]). En particular, la Circular exige que todos los organismos federales limiten la creación, la recogida, la utilización, el tratamiento, el almacenamiento, la conservación, la difusión y la comunicación de información de identificación personal a lo que estén legalmente autorizados, sea pertinente y se considere razonablemente necesario para el correcto desempeño de sus funciones ([176]). Además, en la medida de lo razonablemente posible, los organismos federales deben garantizar que la información de identificación personal sea exacta y pertinente, esté actualizada y completa y se reduzca al mínimo necesario para el correcto desempeño de sus funciones. En términos más generales, los organismos federales deben: establecer un programa integral de privacidad para garantizar el cumplimiento de los requisitos en materia de privacidad aplicables; elaborar y evaluar directrices en materia de privacidad y gestionar los riesgos en materia de privacidad; establecer procedimientos para detectar, documentar y notificar los incidentes relacionados con incumplimientos en materia de privacidad; desarrollar programas de sensibilización y formación en materia de privacidad para empleados y contratistas; y establecer directrices y procedimientos para garantizar que el personal sea responsable del cumplimiento de los requisitos y directrices en materia privacidad ([177]).

(103) Además, la Ley de Administración digital (E-Government Act) ([178]) exige que todas los organismos federales (incluidas las autoridades policiales): establezcan garantías de la seguridad de la información que sean proporcionales al riesgo y la magnitud del daño que se derivaría del acceso, uso, comunicación, perturbación, modificación o destrucción no autorizados; y cuenten con un responsable en materia de información para garantizar el cumplimiento de los requisitos en materia de seguridad de la información y lleven a cabo una evaluación anual independiente (por ejemplo, que la realice un inspector general; véase el considerando 109) de su programa y sus prácticas en materia de seguridad de la información ([179]). Del mismo modo, la Ley de archivos federales (Federal Records Act) ([180]) y los reglamentos de desarrollo ([181]) exigen que la información en poder de los organismos federales esté sujeta a salvaguardias que garanticen la integridad física de la información y la protejan de accesos no autorizados.

(104) De conformidad con las competencias otorgadas por leyes federales, como la Ley federal de modernización de la seguridad de la información (Federal Information Security Modernisation Act), de 2014, la Oficina de Gestión y Presupuesto y el Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology) han elaborado normas que son vinculantes para los organismos federales (incluidas las autoridades policiales) y que especifican con más detalle los requisitos mínimos de seguridad de la información que deben establecerse, incluidos los controles de acceso, la sensibilización y la formación, la planificación contra las contingencias, la respuesta a los incidentes, las herramientas de auditoría y rendición de cuentas, la garantía de la integridad del sistema y la información, la realización de evaluaciones de riesgos para la privacidad y la seguridad, etc. ([182]). Además, todos los organismos federales (incluidas las autoridades policiales) deben, de conformidad con las directrices de la Oficina de

([175]) Es decir, la información que puede utilizarse para identificar a una persona o llegar a conocer su identidad, ya sea por sí sola o combinada con otra información vinculada o vinculable a una persona concreta; véase la Circular n.º A-130 de la Oficina de Gestión y Presupuesto, p. 33 (definición de información de identificación personal).

([176]) Circular n.º A-130 de la Oficina de Gestión y Presupuesto, apéndice II, «Responsabilidades de la gestión de información de identificación personal» [Registro Federal (Federal Register), volumen 81, página 49,689, de 28 de julio de 2016), página 17.

([177]) Apéndice II, punto 5, letras a) a h).

([178]) Título 44, capítulo 36, del Código de Estados Unidos.

([179]) Título 44, artículos 3544 a 3545, del Código de Estados Unidos.

([180]) Ley de archivos federales, título 44, artículo 3105, del Código de Estados Unidos.

([181]) Título 36, artículos 1228,150 y siguientes y 1228,228, del Código de Reglamentos Federales, y apéndice A.

([182]) Véase, por ejemplo, la Circular n.º A-130 de la Oficina de Gestión y Presupuesto; la Publicación Especial 800-53, versión quinta, del Instituto Nacional de Normas y Tecnología, de 10 de diciembre de 2020, sobre los controles de la seguridad y la privacidad de las entidades y sistemas que manipulan información; y la Norma Federal de Tratamiento de la Información n.º 200 del Instituto Nacional de Normas y Tecnología, sobre los requisitos mínimos de seguridad de la información y los sistemas de información federales.

Gestión y Presupuesto, aprobar y aplicar un plan para gestionar las violaciones de la seguridad de los datos, especialmente en lo que respecta a la respuesta a dichas violaciones de la seguridad y la evaluación de los riesgos de daños ([183]).

(105) Por lo que se refiere a la conservación de los datos, la Ley de archivos federales ([184]) exige a los organismos federales de los EE. UU. (incluidas las autoridades policiales) que fijen períodos de conservación de la información (tras los cuales debe eliminarse dicha información), que deben ser aprobados por la Administración Nacional de Archivos y Registros (National Archives and Record Administration) ([185]). La duración de este período de conservación se fija en función de diferentes factores, como el tipo de investigación, si las pruebas siguen siendo pertinentes para la investigación, etc. Por lo que respecta al FBI, las Directrices del secretario de Justicia sobre las operaciones nacionales del FBI establece que este debe contar con un plan de conservación de información de este tipo y con un sistema en el que se pueda consultar rápidamente el estado y el fundamento de las investigaciones.

(106) Por último, la Circular n.º A-130 de la Oficina de Gestión y Presupuesto también fija determinados requisitos para la difusión de información de identificación personal. En principio, la difusión y comunicación de información de identificación personal debe limitarse a lo que esté autorizado legalmente y sea pertinente y razonablemente necesario para el correcto desempeño de las funciones propias del organismo ([186]). Al compartir información de identificación personal con otras entidades públicas, los organismos federales estadounidenses deben imponer, cuando proceda, condiciones (incluida la aplicación de controles específicos de seguridad y privacidad) para el tratamiento de la información por medio de acuerdos escritos (como convenios, los acuerdos de utilización de datos, los acuerdos de intercambio de información y los memorandos de entendimiento) ([187]). Por lo que se refiere a los motivos por los que puede difundir la información, las Directrices del secretario de Justicia sobre las operaciones nacionales del FBI y la Guía de Investigaciones y Operaciones Nacionales del FBI ([188]) disponen, por ejemplo, que el FBI puede estar obligada jurídicamente a ello (por ejemplo, en virtud de un convenio internacional) o que está autorizada a difundir información en ciertas circunstancias, por ejemplo: a otros organismos estadounidenses si la comunicación es compatible con la finalidad por la que la información fue recogida y guarda relación con sus responsabilidades; a comités del Congreso; a organismos extranjeros si la información guarda relación con sus responsabilidades y la difusión se ajusta a los intereses de los EE. UU.; si la difusión es claramente necesaria para proteger la seguridad de las personas o el patrimonio o para proteger contra un delito o amenaza para la seguridad nacional o prevenirlos y la comunicación es compatible con la finalidad por la que la información fue recogida ([189]).

3.1.2. ***Supervisión***

(107) Las actividades de las autoridades policiales federales están sujetas a la supervisión de diversos organismos ([190]). Como se explica en los considerandos 92 a 99, en la mayoría de los supuestos esto incluye el control judicial previo, para autorizar las medidas de recogida antes de que ejecutarlas. Además, otros organismos supervisan las diferentes fases de las actividades de las autoridades policiales, en particular la recogida y el tratamiento de datos personales. En conjunto, estos organismos judiciales y no judiciales garantizan que las autoridades policiales estén sometidas a una supervisión independiente.

([183]) Circular 17-12, sobre la preparación respecto de las violaciones de la seguridad de información de identificación personal y la respuesta a las mismas, disponible en inglés en https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf, y Circular n.º A-130 de la Oficina de Gestión y Presupuesto. Por ejemplo, los procedimientos para responder a las violaciones de la seguridad de los datos del Departamento de Justicia, disponible en inglés en https://www.justice.gov/file/4336/download.

([184]) Ley de archivos federales, título 44, artículo 3101 y siguientes, del Código de Estados Unidos

([185]) La Administración Nacional de Archivos y Registros está facultada para evaluar las prácticas de administración de los registros de los organismos y puede determinar si está justificada la conservación continuada de determinada información [título 44, artículo 2904, letra c), y artículo 2906, del Código de Estados Unidos].

([186]) Circular n.º A-130 de la Oficina de Gestión y Presupuesto, sección 5, letra f, punto 1, subletra d).

([187]) Circular n.º A-130 de la Oficina de Gestión y Presupuesto, apéndice I, punto 3, letra d).

([188]) Véase también la Guía de Investigaciones y Operaciones Nacionales del FBI, sección 14.

([189]) Directrices del secretario de Justicia sobre las operaciones nacionales del FBI, sección VI, letras B y C; Guía de Investigaciones y Operaciones Nacionales del FBI, sección 14.

([190]) Los mecanismos mencionados en esta sección también se aplican a la recogida y el uso de los datos por parte de las autoridades federales con fines civiles y regulatorios. Los organismos de los ámbitos civil y regulatorio federales están sujetos al control de sus respectivos inspectores generales y a la supervisión del Congreso, también al Servicio de Responsabilidad del Ejecutivo, que es el organismo de investigación y auditoría del Congreso. Salvo que el organismo en cuestión cuente con un responsable de la protección de la privacidad y de las libertades civiles —puesto que suele existir en los organismos como el Departamento de Justicia y el Departamento de Seguridad Nacional por sus competencias policiales y relativas a la seguridad nacional—, esa función recae en el responsable superior de privacidad del organismo. Todos los organismos federales están obligados legalmente a nombrar a un responsable superior de privacidad, que es el responsable de asegurarse de que el organismo cumpla la normativa en materia de privacidad y todas las obligaciones en materia de supervisión. Véase, por ejemplo, la Circular M-16-24 de la Oficina de Gestión y Presupuesto, sobre la función y el nombramiento de los responsables superiores de privacidad, de 2016.

(108) En primer lugar, existen responsables de la protección de la privacidad y de las libertades civiles en diversos Departamentos con responsabilidades penales ([191]). Aunque las facultades específicas de estos funcionarios pueden variar ligeramente en función de la ley habilitadora correspondiente, suelen incluir la supervisión de los procedimientos para garantizar que el respectivo Departamento u organismo tenga debidamente en cuenta las cuestiones relacionadas con la privacidad y las libertades civiles y haya implantado procedimientos adecuados para atender las reclamaciones de los particulares que consideren que se han vulnerado su privacidad o sus libertades civiles. Los directores de cada Departamento u organismo deben velar por que los responsables de la protección de la privacidad y de las libertades civiles dispongan de los medios y los recursos necesarios para cumplir su misión, tengan acceso a todo el material y el personal necesarios para desempeñar sus funciones y sean informados y consultados sobre los cambios propuestos en este ámbito ([192]). Los responsables de la protección de la privacidad y de las libertades civiles presentan informes periódicos al Congreso, entre otros aspectos, acerca del número y la naturaleza de las reclamaciones recibidas por el Departamento u organismo, así como un resumen del curso dado a las mismas, los controles e investigaciones llevados a cabo y las repercusiones de las actuaciones emprendidas por el funcionario ([193]).

(109) En segundo lugar, un inspector general independiente supervisa las actividades del Departamento de Justicia, incluido el FBI ([194]). Los inspectores generales son independientes por mandato legal ([195]) y se encargan de llevar a cabo investigaciones, auditorías e inspecciones independientes de los programas y operaciones del Departamento. Pueden consultar todos los registros, informes, auditorías, expedientes, documentos, escritos, recomendaciones u otro material pertinente, previo requerimiento si es preciso, y pueden tomar declaración ([196]). Aunque los inspectores generales solo pueden formular recomendaciones no vinculantes de medidas correctoras, sus informes, especialmente los relativos a las actuaciones a raíz de recomendaciones (o a su ausencia) ([197]), se publican y se transmiten asimismo al Congreso, que puede ejercer su función de supervisión a este respecto (ver considerando 111) ([198]).

([191]) Véase el título 42, artículo 2000ee-1, del Código de Estados Unidos. Por ejemplo, el Departamento de Justicia, el Departamento de Seguridad Nacional (Department of Homeland Security) y el FBI. En el Departamento de Seguridad Nacional, además, el funcionario responsable de la privacidad tiene como cometido aplicar y mejorar las garantías de la privacidad y promover la transparencia dentro de dicho Departamento (título 6, artículos 142 y 222, del Código de Estados Unidos). Todos los sistemas, la tecnología, los formularios y los programas del Departamento de Seguridad Nacional que recogen datos personales o afectan a la privacidad están sujetos a la supervisión del funcionario responsable de la privacidad, que puede consultar todos los registros, informes, auditorías, expedientes, documentos, escritos, recomendaciones u otro material pertinente del Departamento, previo requerimiento si es preciso. El funcionario responsable de la privacidad debe informar anualmente al Congreso sobre las actividades del Departamento que afecten a la privacidad, especialmente las reclamaciones por vulneraciones de la privacidad.

([192]) Título 42, artículo 2000ee-1, letra d), del Código de Estados Unidos.

([193]) Véase el título 42, artículo 2000ee-1, letra f), puntos 1 y 2, del Código de Estados Unidos. Por ejemplo, el informe de la funcionario responsable de la privacidad y las libertades civiles en el Departamento de Justicia y de la Oficina de Privacidad y Libertades Civiles (Office of Privacy and Civil Liberties) correspondiente al período comprendido entre octubre de 2020 y marzo de 2021 muestra que se llevaron a cabo 389 investigaciones en materia de privacidad, especialmente sobre los sistemas de información y otros programas (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

([194]) Del mismo modo, la Ley de seguridad nacional (National Security Act), de 2002, creó la Oficina del Inspector General (Office of Inspector General) como parte del Departamento de Seguridad Nacional.

([195]) Los inspectores generales solo pueden ser destituidos por el presidente, que deberá comunicar al Congreso por escrito los motivos de tal destitución.

([196]) Véase la Ley sobre los inspectores generales, de 1978, artículo 6.

([197]) Véase a este respecto, por ejemplo, el resumen, elaborado por la Oficina del Inspector General, adscrita al Departamento de Justicia, de sus recomendaciones y la medida en que se han cumplido gracias a acciones de seguimiento de los departamentos y organismos correspondientes (https://oig.justice.gov/sites/default/files/reports/22-043.pdf).

([198]) Véase la Ley sobre los inspectores generales, de 1978, artículo 4, apartado 5, y artículo 5. Por ejemplo, la Oficina del Inspector General, adscrita al Departamento de Justicia, publicó recientemente su informe semestral al Congreso (1 de octubre de 2021 a 31 de marzo de 2022, https://oig.justice.gov/node/23596), en el que se ofrece una visión general de sus auditorías, evaluaciones, inspecciones, revisiones especiales e investigaciones de los programas y operaciones del Departamento de Justicia. Entre estas actividades figuraba la investigación de un antiguo contratista por haber comunicado ilícitamente que se estaba realizando una vigilancia electrónica (interceptación de comunicaciones de un particular) en una investigación en curso; dicha investigación acabó con la condena del contratista. La Oficina del Inspector General también llevó a cabo una investigación de los programas y prácticas en materia de seguridad de la información de los organismos del Departamento de Justicia, entre las que se incluyen la comprobación de la eficacia de las directrices, procedimientos y prácticas en materia de seguridad de la información de un subconjunto representativo de sistemas de los organismos.

(110) En tercer lugar, en la medida en que realicen actividades de lucha contra el terrorismo, los departamentos con competencias policiales están sometidos a la supervisión de la Junta de Supervisión de la Privacidad y las Libertades Civiles, que es un organismo independiente del Ejecutivo que cuenta con una junta de cinco miembros (representativos de los dos partidos) nombrados por el presidente por un mandato fijo de seis años con la aprobación del Senado ([199]). De conformidad con la ley que la crea, la Junta de Supervisión de la Privacidad y las Libertades Civiles tiene encomendadas responsabilidades en el ámbito de las políticas de lucha contra el terrorismo y su ejecución, con el fin de proteger la privacidad y las libertades civiles. Para llevar a cabo su actividad de supervisión, puede acceder a todos los registros, informes, auditorías, expedientes, documentos, escritos y recomendaciones, incluida información clasificada, así como realizar interrogatorios y tomar declaración ([200]). También recibe informes de los responsables de la protección de las libertades civiles y la privacidad de diversos Departamentos y organismos federales ([201]), puede formular recomendaciones a los organismos públicos y a las autoridades policiales, e informa periódicamente a los comités del Congreso y al presidente de los EE. UU. ([202]). Los informes de la Junta, incluidos los dirigidos al Congreso, deben publicarse en la mayor medida posible ([203]).

(111) Por último, las actividades policiales con fines penales están sujetas a la supervisión de comités específicos del Congreso de los EE. UU. (los Comités sobre el Poder Judicial de la Cámara y del Senado). Los Comités sobre el Poder Judicial llevan a cabo su supervisión periódica de diferentes maneras, en particular a través de audiencias, investigaciones, revisiones e informes ([204]).

3.1.3. ***Reparación***

(112) Como se ha indicado, las autoridades policiales deben, en la mayoría de los casos, recabar autorización judicial antes de recoger datos personales. Si bien este requisito no se aplica a los requerimientos administrativos, estos se limitan a supuestos específicos y están sujetos a revisión judicial independiente, al menos cuando el Ejecutivo solicite la ejecución judicial forzosa. En particular, los destinatarios de requerimientos administrativos pueden impugnarlos judicialmente si consideran que son irrazonables, por ser excesivos, opresivos u onerosos ([205]).

(113) Los particulares pueden, en primer lugar, presentar sus solicitudes o reclamaciones a las autoridades policiales en relación con la manipulación de sus datos personales, lo que incluye la posibilidad de solicitar acceso a los datos personales y su corrección ([206]). En cuanto a las actividades relacionadas con la lucha contra el terrorismo, los particulares pueden presentar su reclamación a los responsables de la protección de la privacidad y de las libertades civiles (u otros funcionarios) de las autoridades policiales ([207]).

(114) Por otra parte, la normativa estadounidense establece una serie de acciones judiciales que los particulares pueden ejercitar contra las autoridades públicas o uno de sus funcionarios cuando dichas autoridades traten datos personales ([208]). Cualquier particular, con independencia de su nacionalidad y siempre que se cumplan los requisitos aplicables, está legitimado para ejercitar estas acciones judiciales, que están reguladas, en particular, en la Ley de lo contencioso-administrativo, la Ley de libertad de información (Freedom of Information Act) y la Ley de privacidad de las comunicaciones electrónicas (Electronic Communications Privacy Act).

([199]) Los miembros de la Junta deben ser escogidos únicamente sobre la base de sus cualificaciones profesionales, sus logros, su prestigio, su conocimiento en materia de libertades civiles y privacidad y su experiencia pertinente, sin tener en cuenta su afiliación política. En ningún caso puede haber más de tres miembros de la Junta que pertenezcan al mismo partido político. Para formar parte de la Junta, los miembros nombrados no pueden ser cargos públicos electos, funcionarios o empleados públicos del Gobierno Federal en activo; solo pueden ejercer de miembros de la Junta. Véase el título 42, artículo 2000ee, letra h), del Código de Estados Unidos.

([200]) Título 42, artículo 2000ee, letra g), del Código de Estados Unidos.

([201]) Véase el título 42, artículo 2000ee-1, letra f), punto 1, subletra A), inciso iii), del Código de Estados Unidos. Entre ellos figuran, como mínimo, el Departamento de Justicia, el Departamento de Defensa, el Departamento de Seguridad Nacional, así como cualquier otro Departamento, organismo o servicio del poder ejecutivo que la Junta de Supervisión de la Privacidad y las Libertades Civiles considere pertinente.

([202]) Título 42, artículo 2000ee, letra e), del Código de Estados Unidos.

([203]) Título 42, artículo 2000ee, letra f), del Código de Estados Unidos.

([204]) Por ejemplo, los comités celebran reuniones por temas (véase, por ejemplo, la audiencia reciente del Comité sobre el Poder Judicial de la Cámara sobre las redadas digitales masivas, disponible en inglés en https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), así como audiencias periódicas de supervisión, por ejemplo, de la actividad del FBI o del Departamento de Justicia (disponible en inglés en https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 y https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899).

([205]) Véase el anexo VI.

([206]) Circular n.º A-130 de la Oficina de Gestión y Presupuesto, apéndice II, sección 3, letras a) y f), que exigen que los organismos federales garanticen un acceso adecuado y la corrección que soliciten los particulares, y que establezcan procedimientos para recibir y resolver las reclamaciones y solicitudes en materia de privacidad.

([207]) Véase el título 42, artículo 2000ee-1, del Código de Estados Unidos en relación con el Departamento de Justicia y el Departamento de Seguridad Nacional. Véase también la Circular M-16-24 de la Oficina de Gestión y Presupuesto, sobre la función y el nombramiento de los responsables superiores de privacidad.

([208]) Las vías procesales mencionadas en esta sección también se aplican a la recogida y el uso de los datos por parte de las autoridades federales con fines civiles y regulatorios.

(115) En general, en virtud de las disposiciones sobre revisión judicial de la Ley de lo contencioso-administrativo ([209]), todo particular que sufra un perjuicio por actuaciones ilícitas de un organismo público o que se haya visto adversamente afectado o perjudicado por la actuación de un organismo público está legitimado para ejercitar la correspondiente acción judicial ([210]). En este sentido, se puede demandar al órgano jurisdiccional que declare ilícitas y anule la actuación, las constataciones y las conclusiones del organismo público que sean arbitrarias, caprichosas, un abuso de la facultad de apreciación o, de otro modo, no conformes a Derecho ([211]).

(116) Más concretamente, el título II de la Ley de privacidad de las comunicaciones electrónicas ([212]) establece un régimen legal de derechos de privacidad y, como tal, regula el acceso de las autoridades policiales al contenido de las comunicaciones telefónicas, orales o electrónicas almacenadas por las empresas externas de servicios ([213]). Esta norma tipifica el acceso ilícito (es decir, no autorizado judicialmente o permitido de otro modo) a estas comunicaciones y contempla el derecho de los particulares afectados a ejercitar acciones civiles ante los órganos jurisdiccionales federales estadounidenses para la concesión de una indemnización por daños y perjuicios y la imposición de sanciones pecuniarias punitivas, así como a solicitar medidas de reparación declarativas o equitativas contra los EE. UU. o contra los funcionarios públicos que hayan cometido tales ilícitos con dolo.

(117) Además, otras normas de rango legal, como la Ley de interceptación de comunicaciones ([214]), la Ley de abusos y fraudes informáticos (Computer Fraud and Abuse Act) ([215]), la Ley federal de acciones de responsabilidad civil (Federal Torts Claim Act) ([216]), la Ley del derecho a la privacidad financiera ([217]) y la Ley sobre la imparcialidad de las fichas de información crediticia ([218]), confieren a los particulares legitimación para ejercitar acciones judiciales contra autoridades o funcionarios públicos estadounidenses con respecto al tratamiento de sus datos personales.

([209]) Título 5, artículo 702, del Código de Estados Unidos.

([210]) Por lo general, solo las actuaciones definitivas de los organismos públicos, y no las actuaciones preliminares, de instrucción o intermedias, están sujetas a revisión judicial. Véase el título 5, artículo 704, del Código de Estados Unidos.

([211]) Título 5, artículo 706, apartado 2, letra A), del Código de Estados Unidos.

([212]) Título 18, artículos 2701 a 2712, del Código de Estados Unidos.

([213]) La Ley de privacidad de las comunicaciones electrónicas protege las comunicaciones que obran en poder de dos clases definidas de empresas de servicios de red, a saber, las empresas de: i) servicios de comunicaciones electrónicas, por ejemplo, telefonía o correo electrónico; y ii) servicios informáticos remotos, como los servicios de almacenamiento informático o de procesamiento.

([214]) Título 18, artículos 2510 y ss., del Código de Estados Unidos. Con arreglo a la Ley de interceptación de comunicaciones (título 18, artículo 2520, del Código de Estados Unidos), los particulares cuyas comunicaciones por cable, orales o electrónicas sean interceptadas, reveladas o utilizadas intencionadamente pueden ejercitar la acción civil por vulneración de dicha Ley, incluso contra funcionarios públicos concretos o los EE. UU. en determinadas circunstancias. Por lo que respecta a la recogida de información no sustantiva (por ejemplo, dirección IP, dirección de correo electrónico destinataria o remitente), véase también el capítulo sobre los dispositivos de registro de comunicaciones salientes y entrantes del título 18, artículos 3121 a 3127 del Código de Estados Unidos; en cuanto a las acciones civiles, el artículo 2707).

([215]) Título 18, artículo 1030, del Código de Estados Unidos. Con arreglo a la Ley de abusos y fraudes informáticos, los particulares pueden ejercitar una acción judicial contra otros particulares por el acceso intencional no autorizado (o que haya excedido el acceso autorizado) para obtener información de una entidad financiera, un sistema informático de la Administración estadounidense u otro ordenador específico, incluso contra funcionarios públicos concretos en determinadas circunstancias.

([216]) Título 28, artículos 2671 y ss., del Código de Estados Unidos. En virtud de la Ley federal de acciones de responsabilidad civil, los particulares pueden ejercitar una acción judicial, en determinadas circunstancias, contra los EE. UU. por actos u omisiones negligentes o ilícitos de cualquier empleado público en el desempeño de su cargo o empleo.

([217]) Título 12, artículos 3401 y ss., del Código de Estados Unidos. En virtud de la Ley del derecho a la privacidad financiera, los particulares pueden ejercitar una acción judicial, en determinadas circunstancias, contra los EE. UU. por obtener o comunicar documentos económicos y financieros protegidos vulnerando lo dispuesto en dicha Ley. El acceso de los poderes públicos a los documentos económicos y financieros protegidos está prohibido con carácter general; no está prohibido si los poderes públicos acompañan la solicitud de un requerimiento o una orden de registro lícitos o, con determinadas limitaciones, si presentan una solicitud formal por escrito y se le da traslado de dicha solicitud al particular en cuestión.

([218]) Título 15, artículo 1681 a 1681 *quinvicies*, del Código de Estados Unidos. En virtud de la Ley sobre la imparcialidad de las fichas de información crediticia, los particulares pueden ejercitar una acción judicial contra todo particular que incumpla los requisitos (en particular la necesidad de autorización suficiente) aplicables a la recogida, la difusión y el uso de las fichas de información crediticia de consumidores o, en determinadas circunstancias, contra un organismo público.

(118) Asimismo, con arreglo a la Ley de libertad de información ([219]) (título 5, artículo 552, del Código de Estados Unidos), todo particular tiene derecho a obtener acceso a los documentos de los organismos federales, especialmente si contienen datos personales del particular en cuestión. Una vez agotada la vía administrativa, los particulares están legitimados para exigir judicialmente el derecho de acceso, salvo que los documentos estén protegidos frente a su publicación por una exención o dispensa policial especial ([220]). En este caso, el órgano jurisdiccional analiza si es de aplicación alguna exención o si la autoridad pública en cuestión ha hecho valer una exención lícita.

3.2. **Acceso y uso por parte de los poderes públicos estadounidenses con fines de seguridad nacional**

(119) El Derecho estadounidense contempla una serie de limitaciones y garantías con respecto a la consulta y la utilización de datos personales con fines de seguridad nacional, y establece mecanismos de supervisión y vías de impugnación que se ajustan a los requisitos mencionados en el considerando 89 de la presente Decisión. Las condiciones en las que se puede tener acceso y las garantías aplicables al ejercicio de estas competencias se precisan con detalle en las secciones siguientes.

3.2.1. ***Base jurídica, limitaciones y garantías***

3.2.1.1. *Marco jurídico aplicable*

(120) Los datos personales transferidos desde la UE a entidades participantes pueden ser recopilados por las autoridades estadounidenses con fines de seguridad nacional basándose en diferentes instrumentos normativos, con sujeción a condiciones y garantías específicas.

(121) cuando una entidad localizada en los EE. UU. reciben datos personales, los servicios de inteligencia estadounidenses pueden solicitar acceso a esos datos con fines de seguridad nacional únicamente cuando así se autorice por ley, específicamente en virtud de la Ley de vigilancia de inteligencia exterior (Foreign Intelligence Surveillance Act) o de las disposiciones legales que autoricen el acceso mediante requerimientos de seguridad nacional ([221]). La Ley de Vigilancia de inteligencia exterior incluye varias disposiciones de legitimación para recoger (y posteriormente tratar) los datos personales de los interesados de la UE que se haya transferido en el Marco de Privacidad de Datos UE-EE. UU. (artículo 105 ([222]), artículo 302 ([223]), artículo 402 ([224]), artículo 501 ([225]) y artículo 702 ([226]) de la Ley de vigilancia de inteligencia exterior), como se describe con más detalle en los considerandos 142 a 152.

([219]) Título 5, artículo 552, del Código de Estados Unidos.

([220]) No obstante, los supuestos de dispensa están tasados. Por ejemplo, según el título 5, artículo 552, letra b), punto 7, del Código de Estados Unidos, los derechos que otorga Ley de libertad de información no se pueden ejercer respecto de los documentos o información recogidos con fines policiales, pero únicamente en la medida en que la revelación de dichos documentos o información policiales a) pueda, razonablemente, interferir en la actividad policial; b) tenga el efecto de privar a una persona de su derecho a un proceso equitativo o a la resolución imparcial del proceso; c) pueda, razonablemente, constituir una injerencia injustificada en la vida privada; d) pueda, razonablemente, revelar la identidad de una fuente confidencial, en particular un organismo o autoridad estatal, local o extranjera o una entidad privada que haya proporcionado información de forma confidencial y, en el caso de un documento o información recogida por las autoridades policiales en el curso de una investigación penal o por un organismo que efectúe una investigación lícita de inteligencia relacionada con la seguridad nacional, la información proporcionada por una fuente confidencial; e) revele técnicas y procedimientos de las investigaciones policiales o de los procesos penales o revele directrices para las investigaciones policiales y procesos penales, cuando tal revelación pueda, razonablemente, acarrear el riesgo de fraude de ley; o f) pueda, razonablemente, poner en peligro la vida o la integridad física de alguna persona. Asimismo, cuando se presente una solicitud de acceso a documentos cuya revelación pueda, razonablemente, interferir en la actividad policial y a) la investigación o el proceso se refiera a un posible delito y b) haya razones para creer que i) la persona objeto de la investigación o el proceso no tiene conocimiento del mismo y que ii) la comunicación de la existencia de los documentos pueda, razonablemente, interferir en la actividad policial, el organismo puede, solo durante el tiempo en que concurra esta circunstancia, tratar los documentos como si no estuviesen sujetos a los requisitos de dicho artículo (título 5, artículo 552, letra c), punto 1, del Código de Estados Unidos).

([221]) Véase el título 12, artículo 3414, el título 15, artículos 1681 *duovicies* a 1681 *tervicies* y el título 18, artículo 2709, del Código de Estados Unidos. Véase el considerando 153.

([222]) Título 50, artículo 1804, del Código de Estados Unidos, que se refiere a la vigilancia electrónica individualizada tradicional.

([223]) Título 50, artículo 1822, del Código de Estados Unidos, que se refiere a los registros físicos con fines de inteligencia exterior.

([224]) Título 50, artículo 1842 y artículo 1841, apartado 2, del Código de Estados Unidos, y artículo 3127 del título 18, que se refieren a la instalación de dispositivos de registro de comunicaciones salientes y entrantes.

([225]) Título 50, artículo 1861, del Código de Estados Unidos, por el que se faculta al FBI para solicitar una resolución por la que se intime a un transportista común o al responsable de un establecimiento de alojamiento, una instalación de almacenamiento físico o un establecimiento de alquiler de vehículos a entregar los documentos que obren en su poder para una investigación destinada a recabar información de inteligencia exterior o una investigación relativa al terrorismo internacional.

([226]) Título 50, artículo 1881 *bis*, del Código de Estados Unidos, por el que se faculta a la Comunidad de Inteligencia estadounidense para solicitar acceso a información, incluido el contenido de las comunicaciones por internet, de sociedades estadounidenses, en relación con determinadas personas físicas no estadounidenses fuera de los EE. UU. con la ayuda, exigida legalmente, de empresas de servicios de comunicación electrónica.

(122) Los servicios de inteligencia estadounidenses también están facultados para recoger datos personales fuera de los EE. UU., incluidos datos personales en tránsito entre la UE y los EE. UU. La recogida de información fuera de los EE. UU. se basa en el Decreto Presidencial n.º 12333 ([227]), aprobado por el presidente de los EE. UU. ([228]).

(123) La recogida de inteligencia de señales es la forma de recogida de inteligencia más pertinente para la presente decisión de adecuación, ya que se refiere a la recogida de comunicaciones electrónicas y datos de sistemas de información. Esta recogida pueden llevarla a cabo los servicios de inteligencia estadounidenses tanto dentro de los EE. UU. (en virtud de la Ley de vigilancia de inteligencia exterior) como cuando los datos se encuentran en tránsito hacia los EE. UU. (en virtud del Decreto Presidencial n.º 12333).

(124) El 7 de octubre de 2022, el presidente de los EE. UU. aprobó el Decreto Presidencial n.º 14086, titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos», que establece limitaciones y garantías para todas las actividades de inteligencia de señales estadounidenses. Este Decreto Presidencial sustituye, en gran medida, a la Directiva Presidencial n.º 28 ([229]), refuerza las condiciones, limitaciones y garantías que se aplican a todas las actividades de inteligencia de señales (en virtud de la Ley de vigilancia de inteligencia exterior y del Decreto Presidencial n.º 12333) , independientemente del lugar en el que tengan lugar ([230]), y establece un nueva vía de reclamación con la que los particulares pueden exigir su cumplimiento ([231]) (véanse con más detalle los considerandos 176 a 194). Incorpora al Derecho estadounidense el resultado de las negociaciones que tuvieron lugar entre la UE y los EE. UU. tras la invalidación de la decisión de adecuación de la Comisión relativa al Escudo de la privacidad por parte del TJUE (véase el considerando 6). Por lo tanto, constituye un elemento especialmente importante del marco jurídico evaluado en la presente Decisión.

(125) Los límites y garantías introducidos por el Decreto Presidencial n.º 14086 complementan a los establecidos en el artículo 702 de la Ley de Vigilancia de Inteligencia Exterior y el Decreto Presidencial n.º 12333. Las obligaciones ante descritas (secciones 3.2.1.2 y 3.2.1.3) deben cumplirlas los servicios de inteligencia cuando realicen actividades de inteligencia de señales con arreglo al artículo 702 de la Ley de Vigilancia de Inteligencia Exterior y al Decreto Presidencial n.º 12333, por ejemplo, cuando seleccionen/especifique categorías de información de inteligencia exterior que deba adquirirse con arreglo al artículo 702 de la Ley de Vigilancia de Inteligencia Exterior, cuando recojan inteligencia exterior o contrainteligencia con arreglo al Decreto Presidencial n.º 12333 y cuando tomen decisiones de selección de objetivos individuales con arreglo al artículo 702 de la Ley de Vigilancia de Inteligencia Exterior y al Decreto Presidencial n.º 12333.

(126) Las obligaciones que impone dicho Decreto Presidencial, aprobado por el presidente, son vinculantes para toda la Comunidad de Inteligencia. Deben ser cumplidos a través de directrices y procedimientos de los organismos que las transpongan en instrucciones concretas para las operaciones cotidianas. A este respecto, el Decreto Presidencial n.º 14086 proporciona a los servicios de inteligencia estadounidenses un máximo de un año para actualizar sus directrices y procedimientos existentes (es decir, a más tardar el 7 de octubre de 2023) con el fin de adaptarlos a las obligaciones que impone el Decreto Presidencial. Estas directrices y procedimientos actualizados deben elaborarse en consulta con el secretario de Justicia, el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional (Office of the Director of National Intelligence) y la Junta de Supervisión de la Privacidad y las Libertades Civiles (Privacy and Civil Liberties Oversight Board), organismo de supervisión independiente facultado para examinar las directrices del poder ejecutivo y su aplicación, con vistas a proteger la privacidad y las libertades civiles (véase el considerando 110 en lo que respecta a la función y el estatuto de la Junta de Supervisión de la Privacidad y las Libertades Civiles), y deben publicarse ([232]). Además, una vez que se hayan puesto en práctica las directrices y los procedimientos actualizados, la Junta de Supervisión de la Privacidad y las

([227]) Decreto Presidencial n.º 12333: Actividades de inteligencia de los Estados Unidos (EO 12333: United States Intelligence Activities), Registro Federal, vol. 40, n.º 235 (de 8 de diciembre de 1981, en su versión modificada el 30 de julio de 2008). El Decreto Presidencial n.º 12333 define de manera más general los objetivos, las directrices, las obligaciones y las responsabilidades que rigen las actividades de inteligencia de los EE. UU. (incluida la función de los diversos componentes de la Comunidad de Inteligencia) y establece los parámetros generales para la realización de actividades de inteligencia.

([228]) De conformidad con el artículo II de la Constitución de los Estados Unidos, la responsabilidad de garantizar la seguridad nacional, incluida, en particular, la recopilación de inteligencia exterior, es competencia del presidente como comandante en jefe de las fuerzas armadas.

([229]) El Decreto Presidencial n.º 14086 sustituye a la Directiva Presidencial n.º 28 (Presidential Policy Directive 28), con la excepción de su artículo 3 y un anexo (que exige a los servicios de inteligencia que revisen anualmente sus prioridades y obligaciones en materia de inteligencia de señales, teniendo en cuenta en qué medida las actividades de inteligencia de señales coadyuvan a los intereses nacionales de los EE. UU., así como el riesgo que plantean dichas actividades) y el artículo 6 (disposiciones generales); véase la Circular de Seguridad Nacional sobre la derogación parcial de la Directiva Presidencial n.º 28, disponible en inglés en https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Véase el artículo 5, letra f), del Decreto Presidencial n.º 14086, que explica que tiene el mismo ámbito de aplicación que la Directiva Presidencial n.º 28, que, según su nota a pie de página n.º 3, se aplicaba a las actividades de inteligencia de señales realizadas con el fin de recoger comunicaciones o información sobre comunicaciones, excepto las actividades de inteligencia de señales realizadas para probar o desarrollar capacidades de inteligencia de señales.

([231]) Véase a este respecto, por ejemplo, el artículo 5, letra h), del Decreto Presidencial n.º 14086, que aclara que las garantías del Decreto Presidencial crean derechos y pueden ser exigidas por los particulares a través de la vía procesal establecida al efecto.

([232]) Véase el artículo 2, letra c), inciso iv), subletra C), del Decreto Presidencial n.º 14086.

Libertades Civiles llevará a cabo un nuevo examen para garantizar que respetan lo dispuesto en el Decreto Presidencial. En un plazo de 180 días a partir de la finalización de dicho examen por parte de la Junta de Supervisión de la Privacidad y las Libertades Civiles, cada servicio de inteligencia debe estudiar cuidadosamente y aplicar o atender de otro modo todas las recomendaciones de la Junta de Supervisión de la Privacidad y las Libertades Civiles. El 3 de julio de 2023, el Ejecutivo estadounidense publicó esas directrices y procedimientos actualizados ([233]).

3.2.1.2. *Limitaciones y garantías respecto de la recogida de datos personales con fines de seguridad nacional*

(127) El Decreto Presidencial n.º 14086 establece una serie de requisitos transversales que se aplican a todas las actividades de inteligencia de señales (recogida, utilización, difusión, etc. de datos personales).

(128) En primer lugar, estas actividades deben basarse en una ley o contar con autorización presidencial y llevarse a cabo de conformidad con la normativa estadounidense, especialmente la Constitución ([234]).

(129) En segundo lugar, deben establecerse garantías adecuadas con las que se asegure que la privacidad y las libertades civiles se tengan en cuenta en la planificación de tales actividades ([235]).

(130) En particular, las actividades de inteligencia de señales solo pueden llevarse a cabo tras determinar, en una valoración razonable de todos los factores pertinentes, que las actividades son necesarias para avanzar en la prioridad de inteligencia validada (en lo que respecta al concepto de «prioridad de inteligencia validada», véase el considerando 135) ([236]).

(131) Además, tales actividades solo pueden llevarse a cabo en una medida y una manera proporcionadas a la prioridad de inteligencia validada para la que hayan sido autorizadas ([237]). En otras palabras, debe lograrse un equilibrio adecuado entre la importancia de la prioridad de inteligencia perseguida y la repercusión en la privacidad y las libertades civiles de los particulares afectados, independientemente de su nacionalidad o de su lugar de residencia ([238]).

(132) Por último, para garantizar el cumplimiento de estos requisitos generales, que reflejan los principios de legalidad, necesidad y proporcionalidad, las actividades de inteligencia de señales están sujetas a supervisión (en la sección 3.2.2 se explica con mayor detenimiento) ([239]).

(133) Estos requisitos generales están más desarrollados con respecto a la recogida de inteligencia de señales: una serie de condiciones y limitaciones que garantizan que la injerencia en los derechos de los particulares se limite a lo que sea necesario y proporcionado para avanzar en un objetivo legítimo.

(134) En primer lugar, el Decreto Presidencial limita de dos maneras los motivos por los que pueden recogerse datos como parte de las actividades de inteligencia de señales. Por una parte, el Decreto Presidencial fija los objetivos legítimos que pueden perseguirse con la recogida de inteligencia de señales, por ejemplo: comprender o valorar las capacidades, intenciones o actividades de organizaciones extranjeras, incluidas las organizaciones terroristas internacionales, que suponen una amenaza presente o potencial para la seguridad nacional de los EE. UU.; proteger frente a las capacidades y actividades militares extranjeras; comprender o valorar las amenazas transnacionales que afectan a la seguridad mundial, como el cambio climático y otros cambios ecológicos, los riesgos para la salud pública y las amenazas humanitarias ([240]). Por otra parte, el Decreto Presidencial enumera determinados objetivos

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086.

([234]) Artículo 2, letra a), inciso i), del Decreto Presidencial n.º 14086.

([235]) Artículo 2, letra a), inciso ii), del Decreto Presidencial n.º 14086.

([236]) Artículo 2, letra a), inciso ii), subletra A), del Decreto Presidencial n.º 14086. No siempre supone que la inteligencia de señales sea el único medio para avanzar en aspectos de la prioridad de inteligencia validada. Por ejemplo, la recogida de inteligencia de señales puede utilizarse para contar con vías alternativas de validación (por ejemplo, para corroborar la información recibida de otras fuentes de inteligencia) o para tener un acceso fiable a la misma información [artículo 2, letra c), inciso i), subletra A), del Decreto Presidencial n.º 14086].

([237]) Artículo 2, letra a), inciso ii), subletra B), del Decreto Presidencial n.º 14086.

([238]) Artículo 2, letra a), inciso ii), subletra B), del Decreto Presidencial n.º 14086.

([239]) Artículo 2, letra a), inciso iii), en relación con el artículo 2, letra d), del Decreto Presidencial n.º 14086.

([240]) Artículo 2, letra b), inciso i), del Decreto Presidencial n.º 14086. Dado el carácter restringido de objetivos legítimos establecidos en el Decreto Presidencial, que no puede prever todas las posibles amenazas, el Decreto Presidencial contempla la posibilidad de que el presidente actualice esta lista si surgen nuevos imperativos de seguridad nacional, como nuevas amenazas a la seguridad nacional. En principio, estas actualizaciones deben publicarse, a menos que el presidente determine que hacerlo supondría un riesgo para la seguridad nacional de los EE. UU. [artículo 2, letra b), inciso i), subletra B), del Decreto Presidencial n.º 14086].

que nunca deben perseguirse con las actividades de inteligencia de señales, por ejemplo: hacer frente a las críticas, las opiniones disidentes o la libre expresión de ideas u opiniones políticas por parte de particulares o de la prensa; perjudicar a las personas por razón de su etnia, raza, sexo, identidad de género, orientación sexual o religión; u ofrecer una ventaja competitiva a las empresas estadounidenses ([241]).

(135) Además, los objetivos legítimos fijados en el Decreto Presidencial n.º 14086 no pueden, por sí solos, ser invocados por los servicios de inteligencia para justificar la recogida de inteligencia de señales, sino que deben fundamentarse, a efectos operativos, también en prioridades más concretas para las que pueda recogerse inteligencia de señales. En otras palabras, la recogida efectiva solo puede tener lugar para avanzar en una prioridad más específica. Estas prioridades se establecen mediante un proceso específico destinado a garantizar el cumplimiento de los requisitos legales aplicables, como los relativos a la privacidad y las libertades civiles. Más concretamente, las prioridades de inteligencia las elabora primero el director de Inteligencia Nacional (a través del denominado Marco de Prioridades Nacionales de Inteligencia) y se envían al presidente para su aprobación ([242]). Antes de proponer prioridades de inteligencia al presidente, el director debe, de conformidad con el Decreto Presidencial n.º 14086, recabar una evaluación del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional por cada prioridad en cuanto a si: 1) avanza en uno o varios de los objetivos legítimos enumerados en el Decreto Presidencial; 2) no se prevé ni ha sido diseñada para que dé lugar a la recogida de inteligencia de señales para uno de los objetivos prohibidos enumerados en el Decreto Presidencial; y 3) se estableció tras una adecuada consideración de la privacidad y las libertades civiles de todas las personas, independientemente de su nacionalidad o de su lugar de residencia ([243]). En caso de que el director no esté de acuerdo con la evaluación del responsable de la protección de las libertades civiles, ambos puntos de vista deben participarse al presidente ([244]).

(136) Por lo tanto, este proceso garantiza, en particular, que se tengan en cuenta la privacidad desde la fase inicial en la que se desarrollan las prioridades de inteligencia.

(137) En segundo lugar, una vez establecida la prioridad en materia de inteligencia, la decisión sobre si la inteligencia de señales puede recogerse y en qué medida para avanzar en dicha prioridad está sujeta a una serie de requisitos. Estos requisitos ponen en práctica los principios generales de necesidad y proporcionalidad establecidos en el artículo 2, letra a), del Decreto Presidencial.

(138) En particular, la inteligencia de señales solo puede recogerse tras determinar que, con arreglo a una valoración razonable de todos los factores pertinentes, la recogida es necesaria para avanzar en una prioridad específica de inteligencia ([245]). A la hora de determinar si es necesaria una actividad específica de recogida de inteligencia de señales para avanzar en una prioridad de inteligencia validada, los servicios de inteligencia estadounidenses deben tener en cuenta la disponibilidad, viabilidad e idoneidad de otras fuentes y métodos menos intrusivos, en particular los procedentes de fuentes diplomáticas y públicas ([246]). Cuando estén disponibles, debe darse prioridad a tales fuentes y métodos alternativos menos intrusivos ([247]).

(139) Cuando, al aplicar estos criterios, se considere necesaria la recogida de inteligencia de señales, debe ser lo más personalizada posible y no debe afectar de manera desproporcionada a la privacidad y las libertades civiles ([248]). Para garantizar que la privacidad y las libertades civiles no se vean afectadas de manera desproporcionada, es decir, para lograr un equilibrio adecuado entre las necesidades de seguridad nacional y la protección de la privacidad y las libertades civiles, deben tenerse debidamente en cuenta todos los factores pertinentes, como: la naturaleza del objetivo perseguido; el carácter intrusivo de la actividad de recogida, incluida su duración; la contribución probable de la recogida al objetivo perseguido; las consecuencias razonablemente previsibles para los particulares; y la naturaleza y el carácter delicado de los datos que deben recogerse ([249]).

([241]) Artículo 2, letra b), inciso ii), del Decreto Presidencial n.º 14086.

([242]) Artículo 102 *bis* de la Ley de seguridad nacional y artículo 2, letra b), inciso iii), del Decreto Presidencial n.º 14086.

([243]) En supuestos excepcionales (en particular, cuando dicho proceso no pueda llevarse a cabo debido a la necesidad de atender un requisito en materia de inteligencia nuevo o en desarrollo), dichas prioridades pueden ser establecidas directamente por el presidente o el jefe de un servicio de inteligencia, que, en principio, deben aplicar los mismos criterios que los descritos en el artículo 2, letra b), inciso iii), subletra A), puntos 1 a 3; véase el artículo 4, letra n), del Decreto Presidencial n.º 14086.

([244]) Artículo 2, letra b), inciso iii), subletra C), del Decreto Presidencial n.º 14086.

([245]) Artículo 2, letra b) y letra c), inciso i), subletra A), del Decreto Presidencial n.º 14086.

([246]) Artículo 2, letra c), inciso i), subletra A), del Decreto Presidencial n.º 14086.

([247]) Artículo 2, letra c), inciso i), subletra A), del Decreto Presidencial n.º 14086.

([248]) Artículo 2, letra c), inciso i), subletra B), del Decreto Presidencial n.º 14086.

([249]) Artículo 2, letra c), inciso i), subletra B), del Decreto Presidencial n.º 14086.

(140) Por lo que se refiere al tipo de recogida de inteligencia de señales, la recogida de datos en los EE. UU., que es la más pertinente para la presente decisión de adecuación, ya que se refiere a datos que se han transferido a entidades estadounidenses, siempre debe ser selectiva, como se explica pormenorizadamente en los considerandos 142 a 153.

(141) La recogida masiva ([250]) solo puede tener lugar fuera de los EE. UU., según el Decreto Presidencial n.º 12333. También en este caso, según el Decreto Presidencial n.º 14086, debe darse prioridad a la recogida selectiva ([251]). Por el contrario, la recogida masiva solo se permite cuando la información necesaria para avanzar en la prioridad de inteligencia validada no pueda obtenerse razonablemente mediante una recogida selectiva ([252]). Si es necesario llevar a cabo una recogida masiva de datos fuera de los EE. UU., se aplican las garantías específicas del Decreto Presidencial n.º 14086 ([253]). En primer lugar, deben aplicarse métodos y medidas técnicas para limitar los datos que se recogen únicamente a lo necesario para avanzar en una prioridad de inteligencia validada, minimizando al mismo tiempo la recogida de información no pertinente ([254]). En segundo lugar, el Decreto Presidencial limita el uso de la información recogida de forma masiva (incluidas las consultas) a seis objetivos específicos: la protección contra el terrorismo, la toma de rehenes y la privación de libertad de particulares por personas, organizaciones o administraciones públicas extranjeras o en nombre de estas; la protección contra los asesinatos, sabotajes y espionajes extranjeros; la protección contra las amenazas derivadas del desarrollo, la posesión o la proliferación de armas de destrucción masiva o tecnologías y amenazas relacionadas; etc. ([255]). En último lugar, la consulta de inteligencia de señales obtenidas de forma masiva solo puede realizarse cuando sea necesario para avanzar en una prioridad de inteligencia validada, para lograr alguno de esos seis objetivos y de conformidad con directrices y procedimientos que tengan debidamente en cuenta el efecto de las consultas sobre la privacidad y las libertades civiles de los particulares, independientemente de su nacionalidad o de su lugar de residencia ([256]).

(142) Además de las obligaciones que impone el Decreto Presidencial n.º 14086, la recogida de datos de inteligencia de señales que se han transferido a una entidad estadounidense está sujeta a limitaciones y garantías específicas reguladas por el artículo 702 de la Ley de vigilancia de inteligencia exterior ([257]). El artículo 702 de la Ley de vigilancia de inteligencia exterior autoriza la recogida de información de inteligencia exterior respecto de personas no estadounidenses que se considere que es razonable que se encuentren fuera de los EE. UU., con la ayuda obligada de las empresas de servicios de comunicación electrónica estadounidenses ([258]). Con el fin de recoger información de

([250]) Es decir, la recogida de grandes cantidades de inteligencia de señales que, debido a consideraciones técnicas u operativas, se adquieren sin emplear factores de discriminación (por ejemplo, sin utilizar criterios de selección o identificadores específicos); véase el artículo 4, letra b), del Decreto Presidencial n.º 14086. De conformidad con el Decreto Presidencial n.º 14086 y como se explica con más detalle en el considerando 141, la recogida masiva contemplada en el Decreto Presidencial n.º 12333 solo se realiza si es necesario para avanzar en prioridades de inteligencia validadas específicas y está sujeta a una serie de limitaciones y garantías destinadas a asegurar que no se acceda a los datos de forma indiscriminada. Por lo tanto, la recogida masiva debe contrastarse con la recogida que tiene lugar de forma generalizada e indiscriminada («vigilancia masiva») sin limitaciones ni garantías.

([251]) Artículo 2, letra c), inciso ii), subletra A), del Decreto Presidencial n.º 14086.

([252]) Artículo 2, letra c), inciso ii), subletra A), del Decreto Presidencial n.º 14086.

([253]) Las reglas específicas sobre la recogida masiva de datos del Decreto Presidencial n.º 14086 también se aplican a la actividad de recogida selectiva de inteligencia de señales que utilice datos adquiridos sin emplear factores de discriminación (por ejemplo, criterios de selección o identificadores específicos), es decir, de forma masiva (que solo está permitida fuera de territorio estadounidense). Este no es el caso cuando tales datos no solo se usan para contribuir a la fase técnica inicial de la actividad de recogida selectiva de inteligencia de señales, retenida solo por el período corto de tiempo necesario para completar esa fase y luego suprimida inmediatamente [artículo 2, letra c), inciso ii), subletra D), del Decreto Presidencial n.º 14086]. En este supuesto, la única finalidad de la recogida inicial sin factores de discriminación es posibilitar la recogida selectiva de información aplicando un criterio de selección o identificador específicos. En tal caso, solo se introducen en las bases de datos de la Administración los datos que arroja la aplicación de un determinado factor de discriminación, mientras que los datos restantes se destruyen. Por lo tanto, esta recogida selectiva sigue rigiéndose por las reglas generales aplicables a la recogida de inteligencia de señales, en particular el artículo 2, letra a), y el artículo 2, letra c), inciso i), del Decreto Presidencial n.º 14086.

([254]) Artículo 2, letra c), inciso ii), subletra A), del Decreto Presidencial n.º 14086.

([255]) Artículo 2, letra c), inciso ii), subletra B), del Decreto Presidencial n.º 14086. Si surgen nuevos imperativos de seguridad nacional, como nuevas amenazas a la seguridad nacional, el presidente puede actualizar esta lista. En principio, estas actualizaciones deben publicarse, a menos que el presidente determine que hacerlo supondría un riesgo para la seguridad nacional de los EE. UU. [artículo 2, letra c), inciso ii), subletra C), del Decreto Presidencial n.º 14086]. Por lo que se refiere a las consultas sobre datos recogidos de forma masiva, véase el artículo 2, letra c), inciso iii), subletra D), del Decreto Presidencial n.º 14086.

([256]) Artículo 2, letra a), inciso ii), subletra A), en relación con el artículo 2, letra c), inciso iii), subletra D), del Decreto Presidencial n.º 14086. Véase también el anexo VII.

([257]) Título 50, artículo 1881, del Código de Estados Unidos.

([258]) Título 50, artículo 1881 bis, letra a), del Código de Estados Unidos. En particular y como señala la Junta de Supervisión de la Privacidad y las Libertades Civiles, la vigilancia que contempla el artículo 702 consiste íntegramente en dirigirse a personas específicas no estadounidenses sobre las que se ha realizado una determinación individualizada [Junta de Supervisión de la Privacidad y las Libertades Civiles, Informe sobre el programa de vigilancia a efectos del artículo de la Ley de vigilancia de inteligencia exterior (Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act; en lo sucesivo, «informe sobre el artículo 702»), 2 de julio de 2014, p. 111]. Véase el informe del responsable de la protección de las libertades civiles de la Agencia Nacional de Seguridad (National Security Agency) titulado «Aplicación del artículo 702 de la Ley de vigilancia de inteligencia exterior por la NSA» (NSA's Implementation of Foreign Intelligence Surveillance Act Section 702), 16 de abril de 2014. El término «empresa de servicios de comunicación electrónica» se define en el título 50, artículo 1881 *bis*, apartado 4, del Código de Estados Unidos.

inteligencia exterior de conformidad con el artículo 702 de la Ley de vigilancia de inteligencia exterior, el secretario de Justicia y el director de Inteligencia Nacional presentan certificaciones anuales al Tribunal de Vigilancia de Inteligencia Exterior (Foreign Intelligence Surveillance Court) que especifican las categorías de información de inteligencia exterior que deben adquirirse ([259]). Las certificaciones deben ir acompañadas de procedimientos de selección de objetivos, minimización y consulta, que también aprueba el Tribunal y que son jurídicamente vinculantes para los servicios de inteligencia estadounidenses.

(143) El Tribunal de Vigilancia de Inteligencia Exterior es un órgano cuasijudicial ([260]) independiente creado por ley federal cuyas resoluciones pueden recurrirse ante el Tribunal de Apelación de Inteligencia Exterior (Foreign Intelligence Court of Review) ([261]) y, en última instancia, ante la Corte Suprema de los Estados Unidos ([262]). El Tribunal de Vigilancia de Inteligencia Exterior (y el Tribunal de Apelación de Inteligencia Exterior) cuenta con el apoyo de un grupo permanente de cinco abogados y cinco técnicos en materia de seguridad nacional y libertades civiles ([263]). El Tribunal designa de entre este grupo a un *amicus curiae* para que asista en el examen de cualquier solicitud de resolución o recurso que, a juicio del Tribunal, pida una interpretación nueva o significativa de la normativa aplicable, salvo que el Tribunal considere que no procede tal designación ([264]). Así se garantiza, en particular, que la apreciación del Tribunal tenga debidamente en cuenta todas las consideraciones relativas a la privacidad. El Tribunal también puede designar como amicus curiae, especialmente 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 ([265]).

(144) El Tribunal de Vigilancia de Inteligencia Exterior revisa las certificaciones y los procedimientos conexos (en particular, los procedimientos de selección de objetivos y minimización) para comprobar si se cumplen los requisitos que fija la Ley de vigilancia de inteligencia exterior. Si considera que no se cumplen los requisitos, puede no homologar total o parcialmente la certificación y solicitar la modificación de los procedimientos ([266]). A este respecto, el Tribunal de Vigilancia de Inteligencia Exterior ha confirmado en repetidas ocasiones que su revisión de los procedimientos de selección de objetivos y minimización a efectos del artículo 702 no se limita a los procedimientos escritos, sino que también incluye la forma en que la Administración pone en práctica tales procedimientos ([267]).

(145) La selección de objetivos la realiza la Agencia Nacional de Seguridad (que es el servicio de inteligencia responsable de seleccionar a los objetivos en virtud del artículo 702 de la Ley de vigilancia de inteligencia exterior) de conformidad con los procedimientos de selección aprobados por el Tribunal de Vigilancia de Inteligencia Exterior, que obligan a la Agencia Nacional de Seguridad a valorar, atendiendo a todas las circunstancias, si es probable que al dirigirse a la persona en cuestión se obtenga una categoría de información de inteligencia exterior especificada en la certificación ([268]). Esta valoración debe ser específica, tener base fáctica y estar informada por un juicio analítico, la

([259]) Título 50, artículo 1881 *bis*, letra g), del Código de Estados Unidos.

([260]) El Tribunal de Vigilancia de Inteligencia Exterior consta de once magistrados nombrados por el presidente de la Corte Suprema de los Estados Unidos de entre magistrados que integren las cortes federales distritales (*federal district courts*), que previamente han sido nombramos por el presidente de los Estados Unidos y confirmados por el Senado. Los magistrados, que tienen cargos vitalicios y solo pueden ser destituidos en casos debidamente justificados, ejercen su cargo en el Tribunal de Vigilancia de Inteligencia Exterior por períodos escalonados de siete años. La Ley de vigilancia de inteligencia exterior dispone que los magistrados deben proceder de un mínimo de siete distritos judiciales federales distintos. Véase el título 50, artículo 1803, letra a), del Código de Estados Unidos. Los magistrados están asistidos por letrados judiciales experimentados que integran la oficina judicial del Tribunal y elaboran análisis jurídicos de las solicitudes de recogida de datos. Véase la carta de Reggie B. Walton, presidente del Tribunal de Vigilancia de Inteligencia Exterior, a Patrick J. Leahy, presidente del Comité sobre el Poder Judicial del Senado de los EE. UU., de 29 de julio de 2013 (en lo sucesivo, «carta Walton»), p. 2, que se puede consultar en inglés en https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([261]) El Tribunal de Apelación de Inteligencia Exterior está integrado por tres magistrados nombrados por el presidente de la Corte Suprema de los EE. UU. de entre magistrados de las cortes federales distritales o de apelaciones y ejercen su cargo por períodos escalonados de siete años. Véase el título 50, artículo 1803, letra b), del Código de Estados Unidos.

([262]) Véase el título 50, artículo 1803, letra b), artículo 1861 *bis*, letra f), y artículo 1881 *bis*, letra h) y letra i), punto 4, del Código de Estados Unidos.

([263]) Título 50, artículo 1803, letra i), punto 1 y punto 3, subletra A), del Código de Estados Unidos.

([264]) Título 50, artículo 1803, letra i), punto 2, subletra A), del Código de Estados Unidos.

([265]) Título 50, artículo 1803, letra i), punto 2, subletra B), del Código de Estados Unidos.

([266]) Véase también el dictamen del Tribunal de Vigilancia de Inteligencia Exterior de 18 de octubre de 2018, disponible en inglés en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, confirmado por el Tribunal de Apelación de Inteligencia Exterior (Foreign Intelligence Court of Review) en su dictamen de 12 de julio de 2019, disponible en inglés en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Véase, por ejemplo, la resolución y el resumen del fallo del Tribunal de Vigilancia de Inteligencia Exterior, de 18 de noviembre de 2020, página 35 (cuya publicación se autorizó el 26 de abril de 2021), anexo D.

([268]) Título 50, artículo 1881 *bis*, letra a), del Código de Estados Unidos; procedimientos utilizados por la Agencia Nacional de Seguridad para seleccionar a particulares no estadounidenses que se considere que es razonable que se encuentren fuera de los EE. UU. para adquirir información de inteligencia exterior con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior, de 1978, en su versión modificada de marzo de 2018 («procedimientos de selección de objetivos de la Agencia Nacional de Seguridad»), disponible en inglés en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, pp. 1 a 4, explicado con más detalle en el informe de la Junta de Supervisión de la Privacidad y las Libertades Civiles, pp. 41 a 42.

formación especializada y la experiencia del analista, y la naturaleza de la información de inteligencia exterior que debe obtenerse ([269]). La selección de objetivos se lleva a cabo mediante la determinación de los denominados «selectores», que indican los medios de comunicación específicos, como la dirección de correo electrónico o el número de teléfono del destinatario, pero nunca palabras o nombres clave de particulares ([270]).

(146) En primer lugar, los analistas de la Agencia Nacional de Seguridad especifican 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 ([271]). Tal como se establece en los procedimientos de selección de objetivos de la Agencia Nacional de Seguridad, esta solo puede vigilar a un objetivo cuando ya sepa algo sobre el objetivo ([272]). Ello puede deberse a información procedente de diferentes fuentes, por ejemplo, la inteligencia humana. A través de estas otras fuentes, el analista también debe conocer un selector específico (es decir, una cuenta de comunicación) utilizado por el posible objetivo. Una vez que estas personas han sido seleccionadas y aprobadas como objetivos a través de un proceso complejo de examen dentro de la Agencia Nacional de Seguridad ([273]), se asignan (es decir, se desarrollan y aplican) una serie de selectores que determinan los medios de comunicación (por ejemplo, direcciones de correo electrónico) utilizados por dichas personas ([274]).

(147) La Agencia Nacional de Seguridad debe documentar la base fáctica de la selección del objetivo ([275]) y, a intervalos regulares después de la selección inicial, asegurar que siguen cumpliéndose esos presupuestos ([276]). Cuando dejen de cumplirse, debe cesar la actividad de recogida ([277]). Los funcionarios de los servicios de supervisión de inteligencia del Departamento de Justicia, que tienen la obligación de comunicar cualquier vulneración al Tribunal de Vigilancia de Inteligencia Exterior y al Congreso ([278]), revisan cada dos meses la selección por parte de la Agencia Nacional de Seguridad de cada objetivo y el expediente de cada evaluación y la justificación de los objetivos documentados para comprobar el cumplimiento de los procedimientos de selección de objetivos. La documentación escrita de la Agencia Nacional de Seguridad facilita la supervisión por parte del Tribunal de Vigilancia de Inteligencia Exterior de si determinadas personas han sido seleccionadas como objetivos correctamente con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior, de conformidad con sus competencias de supervisión, descritas en los considerandos 173 a 174 ([279]). Por último, el director de Inteligencia Nacional también está obligado a comunicar cada año el número total de objetivos seleccionados con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior en los informes públicos anuales de transparencia estadística. Las empresas que reciban instrucciones con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior pueden publicar datos agregados (en informes de transparencia) sobre las solicitudes que reciban ([280]).

([269]) Procedimientos de selección de objetivos de la Agencia Nacional de Seguridad, p. 4.

([270]) Informe sobre el artículo 702, Junta de Supervisión de la Privacidad y las Libertades Civiles, pp. 32, 33 y 45, más las referencias allí citadas. Véase también la «Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act» (Evaluación semestral del cumplimiento de los procedimientos y de las directrices aprobados de conformidad con el artículo 702 de la Ley de vigilancia de inteligencia exterior), presentada por el secretario de Justicia y el director de Inteligencia Nacional; período de referencia: 1 de diciembre de 2016 a 31 de mayo de 2017, p. 41 (octubre de 2018), disponible en inglés en https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) Informe sobre el artículo 702, Junta de Supervisión de la Privacidad y las Libertades Civiles, pp. 42 y 43.

([272]) Procedimientos de selección de objetivos de la Agencia Nacional de Seguridad, p. 2.

([273]) Informe sobre el artículo 702, Junta de Supervisión de la Privacidad y las Libertades Civiles, p. 46. Por ejemplo, la Agencia Nacional de Seguridad debe comprobar que existe una conexión entre el objetivo y el selector y especificar la información de inteligencia exterior que se prevé recabar; esta información debe ser revisada y aprobada por dos analistas superiores de la Agencia Nacional de Seguridad, y se hace un seguimiento de todo el proceso a efectos de las posteriores verificaciones del cumplimiento efectuadas por la Oficina del Director de Inteligencia Nacional y el Departamento de Justicia. Véase el informe del responsable de la protección de las libertades civiles de la Agencia Nacional de Seguridad titulado «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.

([274]) Título 50, artículo 1881 *bis*, letra h), del Código de Estados Unidos.

([275]) Procedimientos de selección de objetivos de la Agencia Nacional de Seguridad, p. 8. Véase también el informe sobre el artículo 702, Junta de Supervisión de la Privacidad y las Libertades Civiles, p. 46. La falta de justificación escrita constituye un incidente de cumplimiento en materia de documentación que debe comunicarse al Tribunal de Vigilancia de Inteligencia Exterior y al Congreso. Véase la «Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act» (Evaluación semestral del cumplimiento de los procedimientos y de las directrices aprobados de conformidad con el artículo 702 de la Ley de vigilancia de inteligencia exterior), presentada por el secretario de Justicia y el director de Inteligencia Nacional; período de referencia: 1 de diciembre de 2016 a 31 de mayo de 2017, p. 41 (octubre de 2018); y el informe sobre cumplimiento del Departamento de Justicia y la Oficina del Director de Inteligencia Nacional para el Tribunal de Vigilancia de Inteligencia Exterior, sobre el período comprendido entre diciembre de 2016 y mayo de 2017, p. A-6, disponible en inglés en https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Véase el escrito del Ejecutivo de los EE. UU. al Tribunal de Vigilancia de Inteligencia Exterior, titulado «Resumen de 2015 de exigencias destacadas del artículo 702» (2015 Summary of Notable Section 702 Requirements), pp. 2 y 3 (15 de julio de 2015), y la información proporcionada en el anexo VII.

([277]) Véase el escrito del Ejecutivo de los EE. UU. al Tribunal de Vigilancia de Inteligencia Exterior, titulado «Resumen de 2015 de exigencias destacadas del artículo 702», de 15 de julio de 2015, páginas 2 y 3, en el que se establece que si el Ejecutivo considera posteriormente que no se espera que seguir empleando el selector de un objetivo dé lugar a la adquisición de información de inteligencia exterior, debe desactivarse y el retraso en el cumplimiento de esta obligación puede constituir un incidente de cumplimiento que debe comunicarse. Véase también la información proporcionada en el anexo VII.

([278]) Informe sobre el artículo 702, Junta de Supervisión de la Privacidad y las Libertades Civiles, pp. 70 a 72; artículo 13, letra b), del Reglamento de procedimiento del Tribunal de Vigilancia de Inteligencia de los EE. UU. (Rules of Procedure of the United States Intelligence Surveillance Court), disponible inglés en https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Véase también el informe sobre cumplimiento del Departamento de Justicia y la Oficina del Director de Inteligencia Nacional para el Tribunal de Vigilancia de Inteligencia Exterior, sobre el período comprendido entre diciembre de 2016 y mayo de 2017, p. A-6.

([280]) Título 50, artículo 1874, del Código de Estados Unidos.

(148) Por lo que se refiere a las demás bases legales para recoger datos personales transferidos a entidades estadounidenses, se aplican diferentes limitaciones y garantías. En general, la recogida de datos masiva está expresamente prohibida en virtud del artículo 402 de la Ley de vigilancia de inteligencia exterior (dispositivos de registro de comunicaciones salientes y entrantes); debe hacerse con requerimientos de seguridad nacional y el uso de criterios de selección específicos es necesario ([281]).

(149) Para llevar a cabo la vigilancia electrónica individualizada tradicional (de conformidad con el artículo 105 de la Ley de vigilancia de inteligencia exterior), los servicios de inteligencia deben presentar una solicitud al Tribunal de Vigilancia de Inteligencia Exterior con una exposición de los hechos y circunstancias que refuerzan la hipótesis de que existe una causa probable para creer que una potencia extranjera o un agente de una potencia extranjera utiliza o está a punto de utilizar el bien en cuestión ([282]). El Tribunal de Vigilancia de Inteligencia Exterior analiza, entre otros aspectos, si los hechos expuestos acreditan que existen esa causa probable ([283]).

(150) Para llevar a cabo un registro de bienes inmuebles o muebles de los que se prevé que resultará una inspección, incautación, etc., de información, documentos o bienes (por ejemplo, un dispositivo informático) con arreglo al artículo 301 de la Ley de vigilancia de inteligencia exterior, es preciso solicitar una orden al Tribunal de Vigilancia de Inteligencia Exterior ([284]). En dicha solicitud se debe demostrar, entre otros aspectos: que existe una causa probable para considerar que el objetivo del registro sea una potencia extranjera o un agente de una potencia extranjera; que los bienes inmuebles o muebles objeto de registro contienen información de inteligencia exterior; y que una potencia extranjera o un agente de una potencia extranjera es propietaria, usuaria o poseedora de los inmuebles que se van a registrar, o estos están siendo transferidos desde o hacia la potencia extranjera en cuestión ([285]).

(151) Del mismo modo, para la instalación de dispositivos de registro de comunicaciones salientes y entrantes (de conformidad con el artículo 402 de la Ley de vigilancia de inteligencia exterior) es necesario solicitarlo al Tribunal de Vigilancia de Inteligencia Exterior (o a un juez de paz estadounidense) y usar un criterio de selección específico, es decir, un término que identifique específicamente a una persona, cuenta, etc. y que se utiliza para limitar, en la medida de lo razonablemente posible, la información solicitada ([286]). Esta facultad no se refiere al contenido de las comunicaciones, sino que se centra en la información relativa al cliente o usuario que utiliza el servicio (como su nombre, dirección, número de usuario, duración o naturaleza del servicio prestado y fuente o modalidad de pago).

(152) El artículo 501 de la Ley de vigilancia de inteligencia exterior ([287]), que permite la recogida de documentos comerciales de transportistas comunes (es decir, cualquier persona física o jurídica que se dedica al transporte de personas o bienes por tierra, ferrocarril, agua o aire con ánimo de lucro), establecimientos de alojamiento (por ejemplo, un hotel, un motel o un albergue), establecimientos de alquiler de vehículos o instalaciones de almacenamiento físico (es decir, que ofrece espacio o servicios relacionados con el almacenamiento de bienes y materiales) ([288]), también exige en estos casos que se presente una solicitud al Tribunal de Vigilancia de Inteligencia Exterior o a un juez de paz. Esta solicitud debe especificar los documentos solicitados y los hechos concretos y relacionados que llevan a creer que el particular al que se refieren los documentos es una potencia extranjera o un agente de una potencia extranjera ([289]).

(153) Por último, los requerimientos de seguridad nacional están autorizados por diferentes leyes y permiten a los organismos de investigación obtener cierta información (sin incluir el contenido de las comunicaciones) de determinadas entidades (por ejemplo, entidades financieras, agencias de información crediticia y empresas de servicios de comunicación electrónica) que obre en fichas de información crediticia, documentos económicos y financieros y registros de transacciones electrónicas y de usuarios digitales ([290]). La ley sobre los requerimientos de seguridad nacional que autoriza el acceso a las comunicaciones electrónicas solo contempla que aquellos puedan ser utilizados por el FBI y exige que en las solicitudes se utilice un término que identifique específicamente a una persona, entidad, número de teléfono o cuenta y se certifique que la información es pertinente para una investigación de seguridad nacional autorizada con el propósito de proteger contra el terrorismo internacional o las actividades clandestinas de inteligencia ([291]). Los destinatarios de requerimientos de seguridad nacional pueden impugnarlos judicialmente ([292]).

([281]) Título 50, artículo 1842, letra c), punto 3, del Código de Estados Unidos y, en lo relativo a los requerimientos de seguridad nacional, el título 12, artículo 3414, letra a), punto 2, el título 15, artículo 1681 *duovicies* y artículo 1681 *tervicies*, letra a), y el título 18, artículo 2709, letra a), del Código de Estados Unidos.

([282]) Por «agente de una potencia extranjera» puede entenderse personas no estadounidenses que realicen actividades de terrorismo internacional o proliferación internacional de armas de destrucción masiva (incluidos los actos preparatorios) [título 50, artículo 1801, letra b), punto 1, del Código de Estados Unidos].

([283]) Título 50, artículo 1804, del Código de Estados Unidos. Véase también el artículo 1841, apartado 4, con respecto a la elección de los criterios de selección.

([284]) Título 50, artículo 1821, apartado 5, del Código de Estados Unidos.

([285]) Título 50, artículo 1823, letra a), del Código de Estados Unidos.

([286]) Título 50, artículo 1842 y artículo 1841, apartado 2, del Código de Estados Unidos, y artículo 3127 del título 18.

([287]) Título 50, artículo 1862, del Código de Estados Unidos.

([288]) Título 50, artículos 1861 a 1862, del Código de Estados Unidos.

([289]) Título 50, artículo 1862, letra b), del Código de Estados Unidos.

([290]) Véase el título 12, artículo 3414, el título 15, artículos 1681 *duovicies* a 1681 *tervicies* y el título 18, artículo 2709, del Código de Estados Unidos.

([291]) Título 18, artículo 2709, letra b), del Código de Estados Unidos.

([292]) Por ejemplo, título 18, artículo 2709, letra d), del Código de Estados Unidos.

3.2.1.3. *Utilización ulterior de la información recogida*

(154) El tratamiento de los datos personales recogidos por los servicios de inteligencia estadounidenses a través de la inteligencia de señales está sujeto a una serie de garantías.

(155) En primer lugar, cada servicio de inteligencia debe garantizar una seguridad adecuada de los datos e impedir el acceso de personas no autorizadas a los datos personales recogidos a través de la inteligencia de señales. A este respecto, una serie de instrumentos, como leyes, directrices y normas varias, especifican en mayor medida los requisitos mínimos de seguridad de la información que deben implantarse (autenticación multifactorial, cifrado, etc.) ([293]). Solo debe poder acceder a los datos recogidos el personal autorizado y formado que necesite conocer la información para desempeñar sus funciones ([294]). En términos más generales, los servicios de inteligencia deben formar adecuadamente a sus empleados, en particular acerca de los procedimientos para denunciar y resolver las vulneraciones de la normativa aplicable (especialmente el Decreto Presidencial n.º 14086) ([295]).

(156) En segundo lugar, los servicios de inteligencia deben cumplir las normas de la Comunidad de Inteligencia en materia de exactitud y objetividad, en particular en lo que se refiere a garantizar la calidad y fiabilidad de los datos, a considerar fuentes alternativas de información y la objetividad en la realización de análisis ([296]).

(157) En tercer lugar y por lo que se refiere a la conservación de los datos, el Decreto Presidencial n.º 14086 aclara que los datos personales de particulares no estadounidenses están sujetos a los mismos períodos de conservación que los que se aplican a los datos de los particulares estadounidenses ([297]). Los servicios de inteligencia deben definir períodos de conversación específicos y/o los factores que deben valorarse para determinar la duración de los períodos de conservación aplicables (por ejemplo, si la información constituye prueba de un delito, si constituye información de inteligencia exterior, si la información es necesaria para proteger la seguridad de las personas o de entidades, especialmente la de las víctimas y los objetivos del terrorismo internacional), que se establecen en distintos instrumentos normativos ([298]).

(158) En cuarto lugar, se aplican reglas específicas en lo que respecta a la difusión de datos personales recogidos a través de la inteligencia de señales. Como disposición general, los datos personales de particulares no estadounidenses solo pueden difundirse si son del mismo tipo que la información que puede difundirse sobre particulares estadounidenses, por ejemplo, la información para proteger la seguridad de una persona u entidad (como objetivos, víctimas o rehenes de organizaciones terroristas internacionales) ([299]). Además, los datos personales no pueden difundirse únicamente por razón de la nacionalidad o del país de residencia del particular o con el fin de eludir las obligaciones que impone el Decreto Presidencial n.º 14086 ([300]). La difusión dentro del Ejecutivo estadounidense solo puede tener lugar si la persona autorizada y formada considera que existen motivos razonables para creer que

([293]) Artículo 2, letra c), inciso iii), subletra B), punto 1, del Decreto Presidencial n.º 14086. Véase también: el título VIII de la Ley de seguridad nacional (en el que se explican los requisitos para poder acceder a información clasificada); el artículo 1.5 del Decreto Presidencial n.º 12333 (por el que se exige a los jefes de los servicios de la Comunidad de Inteligencia que cumplan las directrices en materia de seguridad e intercambio de información y las obligaciones sobre la privacidad de la información y las legales de otro tipo); la Directiva de Seguridad Nacional n.º 42, titulada «National Policy for the Security of National Security Telecommunications and Information Systems» (Directrices nacionales para la seguridad de los sistemas de seguridad nacional de las telecomunicaciones y la información) (por la que se ordena al Comité de Sistemas de Seguridad Nacional que proporcione instrucciones sobre la seguridad de los sistemas de seguridad nacional a los Departamentos y organismos); y la Circular de Seguridad Nacional n.º 8, titulada «Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems» (Mejora de la ciberseguridad de la seguridad nacional, el Departamento de Defensa y los sistemas de la Comunidad de Inteligencia) (por la que se establecen plazos e instrucciones para la implantación de los requisitos de ciberseguridad a los sistemas de seguridad nacional, incluida la autenticación multifactorial, el cifrado, las tecnologías en la nube y los servicios de detección de los nodos finales).

([294]) Artículo 2, letra c), inciso iii), subletra B), punto 2, del Decreto Presidencial n.º 14086. Además, solo se puede acceder a los datos personales respecto de los que no haya habido un pronunciamiento firme sobre su conservación para informar o realizar dicho pronunciamiento o en el ejercicio de funciones administrativas, de ensayo, de desarrollo, de seguridad o de supervisión autorizadas [artículo 2, letra c), inciso iii), subletra B), punto 3, del Decreto Presidencial n.º 14086].

([295]) Artículo 2, letra d), inciso ii), del Decreto Presidencial n.º 14086.

([296]) Artículo 2, letra c), inciso iii), subletra C), del Decreto Presidencial n.º 14086.

([297]) Artículo 2, letra c), inciso iii), subletra A), punto 2, subsubletras a) a c), del Decreto Presidencial n.º 14086. De manera más general, cada servicio debe establecer directrices y procedimientos destinados a minimizar la difusión y conservación de los datos personales recogidos a través de la inteligencia de señales [artículo 2, letra c), inciso iii), subletra A), del Decreto Presidencial n.º 14086].

([298]) Véanse, por ejemplo: el artículo 309 de la Ley de autorización de actividades de inteligencia para el ejercicio de 2015 (Intelligence Authorization Act For Fiscal Year 2015); los procedimientos de minimización aprobados por cada servicio de inteligencia en virtud del artículo 702 de la Ley de Vigilancia de Inteligencia Exterior y autorizados por el Tribunal de Vigilancia de Inteligencia Exterior; y los procedimientos aprobados por el secretario de Justicia conforme a la Ley de archivos federales [por los que se exige a los organismos federales estadounidenses, especialmente los organismos de seguridad nacional, que fijen períodos de conversación de sus documentos, que deben ser aprobados por Administración Nacional de Archivos y Registros (National Archives and Record Administration)].

([299]) Artículo 2, letra c), inciso iii), subletra A), punto 1, subsubletra a), y punto 5, subsubletra d), del Decreto Presidencial n.º 14086, en conjunción con la parte 2, artículo 3, del Decreto Presidencial n.º 12333.

([300]) Artículo 2, letra c), inciso iii), subletra A), punto 1, subsubletras b) y e), del Decreto Presidencial n.º 14086.

el destinatario tiene la necesidad de conocer la información ([301]) y la protegerá adecuadamente ([302]). Para determinar si los datos personales pueden difundirse a destinatarios ajenos al Ejecutivo estadounidense (especialmente organismos públicos extranjeros u organizaciones internacionales), deben tenerse en cuenta la finalidad de la difusión, la naturaleza y la cantidad de los datos objeto de difusión y los posibles perjuicios para los particulares afectados ([303]).

(159) Por último, también para facilitar la supervisión del cumplimiento de los requisitos legales aplicables, así como de la reparación efectiva, cada servicio de inteligencia debe, en virtud del Decreto Presidencial n.º 14086, conservar la documentación adecuada sobre la recogida de inteligencia de señales. Esta obligación abarca elementos como la base fáctica de la evaluación de que es necesaria una actividad específica de recogida para avanzar en la prioridad de inteligencia validada ([304]).

(160) Además de las garantías antes mencionadas del Decreto Presidencial n.º 14086 para el uso de la información recogida mediante inteligencia de señales, todos los servicios de inteligencia estadounidenses están sometidos a las obligaciones más generales de limitación de la finalidad, minimización de los datos, exactitud, seguridad, conservación y difusión, que se derivan especialmente de la Circular n.º A-130 de la Oficina de Gestión y Presupuesto, la Ley de Administración digital, la Ley de archivos federales (véanse los considerandos 101 a 106) y de las orientaciones del Comité de Sistemas Nacionales de Seguridad (Committee on National Security Systems) ([305]).

3.2.2. ***Supervisión***

(161) Las actividades de los servicios de inteligencia estadounidenses están sujetas a la supervisión de diferentes organismos.

(162) En primer lugar, el Decreto Presidencial n.º 14086 exige que cada servicio de inteligencia cuente con funcionarios de alto nivel responsables de las cuestiones jurídicas, de supervisión y de cumplimiento para garantizar el cumplimiento de la normativa estadounidense aplicable ([306]). En particular, deben llevar a cabo una supervisión periódica de las actividades de inteligencia de señales y velar por que se subsane cualquier incumplimiento. Los servicios de inteligencia deben proporcionar a dichos funcionarios acceso a toda la información pertinente para llevar a cabo sus funciones de supervisión y no pueden tomar ninguna medida para impedir su labor de supervisión ni influir indebidamente en esta ([307]). Además, cualquier incidente significativo de incumplimiento ([308]) detectado por un funcionario de supervisión o por cualquier otro empleado debe comunicarse sin demora al jefe del servicio de inteligencia y al director de Inteligencia Nacional, que deben velar por que se tomen todas las medidas necesarias para reparar la situación y evitar que se repita el incidente significativo de incumplimiento ([309]).

(163) Esta función de supervisión la desempeñan funcionarios con un cargo específico en materia de verificación del cumplimiento, así como los responsables de la protección de la privacidad y de las libertades civiles y los inspectores generales ([310]).

([301]) Las Directrices del secretario de Justicia sobre las operaciones nacionales del FBI disponen, por ejemplo, que el FBI puede difundir información que obre en su poder si el destinatario tiene la necesidad de conocerla para poder desempeñar sus funciones o para proteger a la ciudadanía.

([302]) Artículo 2, letra c), inciso iii), subletra A), punto 1, subsubletra c), del Decreto Presidencial n.º 14086. Los servicios de inteligencia pueden, por ejemplo, difundir la información que obre en su poder en circunstancias pertinentes para una investigación penal o en relación con un delito, en particular: comunicando las amenazas de muerte, de lesiones físicas graves o de secuestro, comunicando la información sobre las respuestas a amenazas, incidentes o intrusiones informáticos y notificando a las víctimas o alertando a las potenciales víctimas de delitos.

([303]) Artículo 2, letra c), inciso iii), subletra A), punto 1, subsubletra d), del Decreto Presidencial n.º 14086.

([304]) Artículo 2, letra c), inciso iii), subletra E), del Decreto Presidencial n.º 14086.

([305]) Véase la Directriz n.º 22 del Comité de Sistemas Nacionales de Seguridad, sobre las directrices de gestión del riesgo en materia de ciberseguridad, y la Instrucción n.º 1253 del Comité de Sistemas Nacionales de Seguridad, que da consejos pormenorizados sobre las medidas de seguridad que deberían aplicarse a los sistemas de seguridad nacional.

([306]) Artículo 2, letra d), inciso i), subletras A) a B), del Decreto Presidencial n.º 14086.

([307]) Artículo 2, letra d), inciso i), subletras B) a C), del Decreto Presidencial n.º 14086.

([308]) Es decir, un incumplimiento sistemático o intencionado de la normativa estadounidense aplicable que puede socavar la reputación o la integridad de una agencia de la Comunidad de Inteligencia o cuestionar de otro modo la corrección de una actividad de los servicios de inteligencia, en particular atendiendo a la posible repercusión significativa en los intereses en materia de privacidad y libertades civiles del particular o particulares afectados; véase el artículo 5, letra l), del Decreto Presidencial n.º 14086.

([309]) Artículo 2, letra d), inciso iii), del Decreto Presidencial n.º 14086.

([310]) Artículo 2, letra d), inciso i), subletra B), del Decreto Presidencial n.º 14086.

(164) Al igual que en el caso de las autoridades policiales, en todos los servicios de inteligencia existen responsables de la protección de la privacidad y de las libertades civiles ([311]). Las facultades de estos funcionarios suelen incluir la supervisión de los procedimientos para garantizar que el correspondiente departamento o servicio tenga debidamente en cuenta las cuestiones relacionadas con la privacidad y las libertades civiles y haya implantado procedimientos adecuados para atender las reclamaciones de los particulares que consideren que se han vulnerado su privacidad o sus libertades civiles (y, en ocasiones, como en el caso de la Oficina del Director de Inteligencia Nacional, pueden estar facultados para investigar las reclamaciones ([312])). Los directores de los servicios de inteligencia deben velar por que los responsables de la protección de la privacidad y de las libertades civiles dispongan de los recursos necesarios para cumplir su misión, tengan acceso a todo el material y el personal necesarios para desempeñar sus funciones y sean informados y consultados sobre los cambios propuestos en este ámbito ([313]). Los responsables de la protección de la privacidad y de las libertades civiles presentan informes periódicos al Congreso y a la Junta de Supervisión de la Privacidad y las Libertades Civiles, entre otros aspectos, acerca del número y la naturaleza de las reclamaciones recibidas por el Departamento u organismo, así como un resumen del curso dado a las mismas, los controles e investigaciones llevados a cabo y las repercusiones de las actuaciones emprendidas por el funcionario ([314]).

(165) En segundo lugar, cada servicio de inteligencia dispone de un inspector general independiente, que se encarga, entre otras cosas, de supervisar las actividades de inteligencia exterior. En el caso de la Oficina del Director de Inteligencia Nacional, existe la Oficina del Inspector General de la Comunidad de Inteligencia (Office of the Inspector General of the Intelligence Community), que tiene amplias competencias sobre el conjunto de la Comunidad de Inteligencia y está facultada para investigar las reclamaciones o denuncias relativas a posibles conductas ilícitas o abusos de autoridad, en relación con los programas y actividades de la Oficina del Director de Inteligencia Nacional o de la Comunidad de Inteligencia ([315]). Al igual que en el caso de las autoridades policiales (véase el considerando 109), estos inspectores generales gozan de independencia por mandato legal ([316]) y se encargan de llevar a cabo auditorías e investigaciones sobre los programas y las actividades llevadas a cabo por el servicio correspondiente con fines de inteligencia nacional, en particular en relación con el uso abusivo o la vulneración de la normativa aplicable ([317]).

([311]) Véase el título 42, artículo 2000ee-1, del Código de Estados Unidos. Entre ellos figuran, por ejemplo, el Departamento de Estado, el Departamento de Justicia, el Departamento de Seguridad Nacional, el Departamento de Defensa, la Agencia Nacional de Seguridad, la Agencia Central de Inteligencia (por sus siglas en inglés, «CIA») y la Oficina del Director de Inteligencia Nacional.

([312]) Véase el artículo 3, letra c), del Decreto Presidencial n.º 14086.

([313]) Título 42, artículo 2000ee-1, letra d), del Código de Estados Unidos.

([314]) Véase el título 42, artículo 2000ee-1, letra f), puntos 1 y 2, del Código de Estados Unidos. Por ejemplo, el informe del funcionario responsable de la privacidad y las libertades civiles de la Agencia Nacional de Seguridad sobre el período comprendido entre enero de 2021 y junio de 2021 muestra que se llevaron a cabo 591 análisis de los efectos en las libertades civiles y la privacidad en diversos contextos, por ejemplo, en relación con las actividades de recogida, los acuerdos y decisiones de intercambio de información, las resoluciones de conservación de datos, etc., teniendo en cuenta diferentes factores, como la cantidad y el tipo de información asociada a la actividad, los particulares afectados, la finalidad y el uso previsto de los datos, las garantías existentes para mitigar los posibles riesgos para la privacidad, etc. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Del mismo modo, los informes de la Oficina de Privacidad y Libertades Civiles de la CIA sobre el período comprendido entre enero y junio de 2019 proporcionan información sobre las actividades de supervisión de la Oficina, por ejemplo, la verificación del cumplimiento de las Directrices del secretario de Justicia aprobadas a efectos del Decreto Presidencial n.º 12333 con respecto a la conservación y difusión de la información, las instrucciones proporcionadas sobre la aplicación de la Directiva Presidencial n.º 28 y las obligaciones de detectar y resolver las violaciones de la seguridad de los datos, así como verificaciones del uso y el tratamiento de la información personal (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Este inspector general es nombrado por el presidente de los EE. UU, con el respaldo del Senado, y únicamente puede ser destituido por el presidente.

([316]) Los inspectores generales 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 puede prohibir al inspector general que inicie, lleve a cabo o finalice la auditoría o investigación cuando se considere necesario en aras de intereses de seguridad nacional importantes. No obstante, el Congreso debe ser informado del ejercicio de esta facultad y puede exigir responsabilidades a este respecto al director correspondiente. Véanse, por ejemplo, la Ley sobre los inspectores generales, de 1978, artículo 8 (respecto del Departamento de Defensa), artículo 8 *sexies* (respecto del Departamento de Justicia) y artículo 8 *octies*, letra d), punto 2, subletras A) y B) (respecto de la Agencia Nacional de Seguridad); el título 50, artículo 403 *octodecies*, letra b), del Código de Estados Unidos (respecto de la CIA); y la Ley de autorización de actividades de inteligencia para el ejercicio de 2010, artículo 405, letra f) (respecto de la Comunidad de Inteligencia).

([317]) Ley sobre los inspectores generales, de 1978, en su versión modificada (Ley pública n.º 117-108, de 8 de abril de 2022). Por ejemplo, como se explica en los informes semestrales al Congreso referidos al período comprendido entre el 1 de abril de 2021 y el 31 de marzo de 2022, el inspector general de la Agencia Nacional de Seguridad llevó a cabo evaluaciones del tratamiento de la información de particulares estadounidenses recogidas con arreglo a el Decreto Presidencial n.º 12333, el proceso de expurgo de los datos de inteligencia de señales, la herramienta de selección automatizada de objetivos utilizada por la Agencia Nacional de Seguridad y el cumplimiento de las reglas en materia de documentación y consulta con respecto a la recogida de datos con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior y formuló varias recomendaciones en este sentido (disponible en inglés en https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, pp. 5 a 8, y https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, pp. 10 a 13). Véanse también las auditorías e investigaciones recientes llevadas a cabo por el inspector general de la Comunidad de Inteligencia sobre seguridad de la información y comunicación no autorizada de información clasificada de seguridad nacional (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, pp. 8 y 11, yhttps://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, pp. 19 a 20).

Pueden consultar todos los registros, informes, auditorías, expedientes, documentos, escritos, recomendaciones u otro material pertinente, previo requerimiento si es preciso, y pueden tomar declaración ([318]). Los inspectores generales remiten los posibles casos de delito a las autoridades competentes para su enjuiciamiento y formulan recomendaciones de medidas correctoras a los jefes de los servicios en cuestión ([319]). Aunque sus recomendaciones no son vinculantes, sus informes, especialmente los relativos a las actuaciones a raíz de recomendaciones (o a su ausencia) ([320]), se publican y se transmiten asimismo al Congreso, que puede ejercer su función de supervisión a este respecto (véanse los considerandos 168 a 169) ([321]).

(166) En tercer lugar, la Junta de Supervisión de Inteligencia (Intelligence Oversight Board), integrada dentro de la Junta Asesora de Inteligencia del presidente de los EE. UU. (President's Intelligence Advisory Board), supervisa el cumplimiento de la Constitución y de las demás normas pertinentes por parte de los servicios de inteligencia estadounidenses ([322]). La Junta Asesora de Inteligencia del presidente de los EE. UU. es un órgano consultivo de la Oficina Ejecutiva del Presidente (Executive Office of the President) compuesto por 16 miembros nombrados por el presidente; los miembros no pueden formar parte del Gobierno. La Junta de Supervisión de Inteligencia está compuesta por un máximo de cinco miembros designados por el presidente de entre los miembros de la Junta Asesora de Inteligencia del presidente de los EE. UU. Según el Decreto Presidencial n.º 12333 ([323]), los jefes de todos los servicios de inteligencia están obligados a informar a la Junta de Supervisión de Inteligencia de cualquier actividad de inteligencia respecto de la cual haya motivos para creer que puede ser ilícita o contraria a un decreto presidencial o a una directiva presidencial. Para garantizar que la Junta de Supervisión de Inteligencia tenga acceso a la información necesaria para el desempeño de sus funciones, el Decreto Presidencial n.º 13462 obliga al director de Inteligencia Nacional y a los jefes de los servicios de inteligencia a que proporcionen toda la información y ayuda que la Junta de Supervisión de Inteligencia determine que son necesarias para desempeñar sus funciones, en la medida en que lo permita la normativa aplicable ([324]). A su vez, la Junta de Supervisión de Inteligencia está obligada a informar al presidente de los EE. UU. sobre las actividades de inteligencia que considere que pueden constituir una vulneración del Derecho estadounidense (especialmente los decretos presidenciales) y no están siendo tratadas adecuadamente por el secretario de Justicia, el director de Inteligencia Nacional o el director del servicio de inteligencia correspondiente ([325]). Además, la Junta de Supervisión de Inteligencia está obligada a denunciar al secretario de Justicia los supuestos de posible comisión de delitos.

(167) En cuarto lugar, los servicios de inteligencia están sometidos a la supervisión de la Junta de Supervisión de la Privacidad y las Libertades Civiles. De conformidad con la ley que la crea, la Junta de Supervisión de la Privacidad y las Libertades Civiles tiene encomendadas responsabilidades en el ámbito de las políticas de lucha contra el terrorismo y su ejecución, con el fin de proteger la privacidad y las libertades civiles. Para supervisar la actividad de los servicios de inteligencia, puede acceder a todos los registros, informes, auditorías, expedientes, documentos, escritos y recomendaciones, incluida información clasificada, así como realizar interrogatorios y tomar declaración ([326]). También recibe informes de los responsables de la protección de las libertades civiles y la privacidad de diversos Departamentos y organismos federales ([327]), puede formular recomendaciones a los organismos públicos y a los servicios de inteligencia, e informa periódicamente a los comités del Congreso y al presidente de los EE. UU. ([328]). Los informes de la Junta, incluidos los dirigidos al Congreso, deben publicarse en la mayor medida posible ([329]). La Junta de Supervisión de la Privacidad y las Libertades Civiles ha publicado varios informes de supervisión y seguimiento, incluido un análisis de los programas ejecutados con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior, de la protección de la privacidad en este contexto y de la aplicación de la Directiva Presidencial n.º 28 y el Decreto Presidencial n.º 12333 ([330]). A la Junta de Supervisión de la Privacidad y

([318]) Véase la Ley sobre los inspectores generales, de 1978, artículo 6.
([319]) Véase la nota anterior, artículos 4, 5 y 6.
([320]) Por lo que se refiere al seguimiento que se da a los informes y recomendaciones de los inspectores generales, véase, por ejemplo, la respuesta a un informe del inspector general del Departamento de Justicia en el que se constató que el FBI no fue suficientemente transparente con el Tribunal de Vigilancia de Inteligencia Exterior respecto de las solicitudes presentadas entre 2014 y 2019, lo que dio lugar a reformas para mejorar el cumplimiento, la supervisión y la rendición de cuentas en el FBI (por ejemplo, el director del FBI ordenó más de cuarenta medidas correctoras, incluidas doce específicas del procedimiento de la Ley de vigilancia de inteligencia exterior relativo a la documentación, la supervisión, la conservación de expedientes, la formación y las auditorías) (disponible en inglés en https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance y https://oig.justice.gov/reports/2019/o20012.pdf). Véase también, por ejemplo, la auditoría que el inspector general del Departamento de Justicia hizo de la Oficina del Consejero General del FBI sobre las funciones y responsabilidades de este en la supervisión del cumplimiento de las normas, directrices y procedimientos aplicables a las actividades de seguridad nacional del FBI, así como el apéndice 2, que incluye una carta del FBI en la que se aceptan todas las recomendaciones. A este respecto, en el apéndice 3 se ofrece una visión general de las medidas de seguimiento y la información que el inspector general solicitó al FBI para poder dar por cumplidas sus recomendaciones (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).
([321]) Véase la Ley sobre los inspectores generales, de 1978, artículo 4, apartado 5, y artículo 5.
([322]) Véase el Decreto Presidencial n.º 13462.
([323]) Parte 1, artículo 6, letra c), del Decreto Presidencial n.º 12333.
([324]) Artículo 8, letra a), del Decreto Presidencial n.º 13462.
([325]) Artículo 6, letra b), del Decreto Presidencial n.º 13462.
([326]) Título 42, artículo 2000ee, letra g), del Código de Estados Unidos.
([327]) Véase el título 42, artículo 2000ee-1, letra f), punto 1, subletra A), inciso iii), del Código de Estados Unidos. Entre ellos figuran, como mínimo, el Departamento de Justicia, el Departamento de Defensa, el Departamento de Seguridad Nacional, el director de Inteligencia Nacional y la CIA, así como cualquier otro Departamento, organismo o servicio del poder ejecutivo que la Junta de Supervisión de la Privacidad y las Libertades Civiles considere pertinente.
([328]) Título 42, artículo 2000ee, letra e), del Código de Estados Unidos.
([329]) Título 42, artículo 2000ee, letra f), del Código de Estados Unidos.
([330]) Disponible en inglés en https://www.pclob.gov/Oversight.

las Libertades Civiles también se le atribuyeron funciones de supervisión específicas en lo que respecta a la aplicación del Decreto Presidencial n.º 14086, en particular mediante la revisión de la coherencia de los procedimientos de los servicios con el Decreto Presidencial (véase el considerando 126) y la evaluación de la eficacia de la vía de impugnación (véase el considerando 194).

(168) En quinto lugar, aparte de los mecanismos de supervisión dentro del poder ejecutivo, hay comités específicos del Congreso de los EE. UU. (en particular, los Comités sobre el Poder Judicial y sobre Inteligencia de la Cámara y del Senado) que tienen competencias de supervisión sobre todas las actividades de inteligencia exterior del país, incluidas las relacionadas con la inteligencia de señales. Los miembros de dichos Comités tienen acceso a información clasificada, así como a los métodos y programas de inteligencia ([331]). Los Comités llevan a cabo su labor de supervisión de diferentes maneras, en particular a través de audiencias, investigaciones, revisiones e informes ([332]).

(169) Los comités del Congreso reciben informes periódicos sobre las actividades de inteligencia, en particular del secretario de Justicia, el director de Inteligencia Nacional, los servicios de inteligencia y otros organismos de supervisión (por ejemplo, los inspectores generales) (véanse los considerandos 164 a 165). En particular, en virtud de la Ley de seguridad nacional, el presidente de los EE UU. garantiza que los comités sobre inteligencia del Congreso reciban constantemente información completa y actualizada sobre las actividades de inteligencia de los EE. UU., incluida toda actividad significativa prevista con arreglo a lo dispuesto en el subcapítulo correspondiente ([333]). Asimismo, la citada Ley dispone que el presidente vela por que se comunique cuanto antes a los comités sobre inteligencia del Congreso toda actividad de inteligencia ilícita, así como toda medida correctora que se haya tomado o se prevea tomar con respecto a dicha actividad ilícita ([334]).

(170) Además, hay leyes específicas que imponen obligaciones de información adicionales. En particular, la Ley de vigilancia de inteligencia exterior exige al secretario de Justicia que informe exhaustivamente a los Comités sobre el Poder Judicial y sobre Inteligencia de la Cámara y del Senado acerca de las actividades realizadas por el Ejecutivo en virtud de determinados artículos de la Ley de vigilancia de inteligencia exterior ([335]). Por otro lado, dispone que el Ejecutivo proporcione a los comités del Congreso copias de todas las resoluciones o dictámenes del Tribunal de Vigilancia de Inteligencia Exterior y del Tribunal de Apelación de Inteligencia Exterior que contengan interpretaciones significativas de las disposiciones de la Ley de vigilancia de inteligencia exterior. Por lo que respecta a la vigilancia contemplada en el artículo 702 de la Ley de vigilancia de inteligencia exterior, la supervisión parlamentaria se ejerce mediante el análisis de los informes que la legislación exige que se envíe a los Comités sobre el Poder Judicial y sobre Inteligencia, así como mediante la celebración de frecuentes reuniones informativas y audiencias. Entre los documentos presentados figuran el informe semestral del secretario de Justicia en el que se describe la aplicación del artículo 702 de la Ley de vigilancia de inteligencia exterior, acompañado de documentos justificativos, en particular, los informes sobre cumplimiento del Departamento de Justicia y de la Oficina del Director de Inteligencia Nacional y la lista de los incidentes de incumplimiento detectados ([336]), así como una evaluación semestral elaborada aparte por el secretario de Justicia y el director de Inteligencia Nacional para documentar el cumplimiento de los procedimientos de selección de objetivos y de minimización ([337]).

([331]) Título 50, artículo 3091, del Código de Estados Unidos.

([332]) Por ejemplo, los comités celebran reuniones por temas (véase, por ejemplo, la audiencia reciente del Comité sobre el Poder Judicial de la Cámara sobre las redadas digitales masivas, disponible en inglés en https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983, y la audiencia del Comité sobre Inteligencia de la Cámara sobre el uso de la inteligencia artificial por parte de la Comunidad de Inteligencia, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), así como audiencias periódicas de supervisión, por ejemplo, de la actividad del FBI o de la División de Seguridad Nacional del Departamento de Justicia (disponibles en inglés en https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation, https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 y https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899). Un ejemplo de investigación es la del Comité sobre Inteligencia del Senado acerca la injerencia rusa en las elecciones estadounidenses de 2016; disponible en inglés en https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures. En cuanto a informes, véase, por ejemplo, el resumen de las actividades (de supervisión) que figura en el informe del Comité sobre Inteligencia del Senado relativo al período comprendido entre el 4 de enero de 2019 y el 3 de enero de 2021, dirigido al Senado, disponible en inglés en https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Véase el título 50, artículo 3091, letra a), punto 1, del Código de Estados Unidos. Esta disposición expone los requisitos generales aplicables a la supervisión por parte del Congreso en el ámbito de la seguridad nacional.

([334]) Véase el título 50, artículo 3091, letra b), del Código de Estados Unidos.

([335]) Véase el título 50, artículos 1808, 1846, 1862, 1871 y 1881 *septies*, del Código de Estados Unidos.

([336]) Véase el título 50, artículo 1881 *septies*, del Código de Estados Unidos.

([337]) Véase el título 50, artículo 1881 *bis*, letra l), punto 1, del Código de Estados Unidos.

(171) Además, la Ley de vigilancia de inteligencia exterior exige que el Ejecutivo estadounidense comunique cada año al Congreso (y que publique) el número de órdenes de las contempladas en la Ley de vigilancia de inteligencia exterior que se solicitan y que se dictan, así como estimaciones del número de ciudadanos estadounidenses y no estadounidenses sometidos a vigilancia, entre otros aspectos ([338]). La citada Ley impone asimismo la obligación de comunicar el número de requerimientos de seguridad nacional emitidos tanto con respecto a ciudadanos estadounidenses como no estadounidenses (si bien también permite a los destinatarios de las órdenes y certificaciones contempladas en la Ley de vigilancia de inteligencia exterior y de requerimientos de seguridad nacional presentar informes de transparencia en determinadas circunstancias) ([339]).

(172) En términos más generales, la Comunidad de Inteligencia estadounidense trata de distintos modos dar transparencia a sus actividades de inteligencia (exterior). Por ejemplo, en 2015, la Oficina del Director de Inteligencia Nacional aprobó principios de transparencia de la inteligencia y un Plan de transparencia y encargó a cada servicio de inteligencia que nombrara a un responsable de la transparencia en materia de inteligencia para fomentar la transparencia y dirigir iniciativas de transparencia ([340]). Como parte de estas medidas, la Comunidad de Inteligencia ha desclasificado y sigue desclasificando directrices, procedimientos, informes de supervisión, informes de actividades realizadas con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior y el Decreto Presidencial n.º 12333, las resoluciones del Tribunal de Vigilancia de Inteligencia Exterior y otros documentos, en particular en el sitio web «IC on the Record», administrado por la Oficina del Director de Inteligencia Nacional ([341]).

(173) Por último, la recogida de datos personales con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior está sujeta a la revisión del Tribunal de Vigilancia de Inteligencia Exterior junto a la supervisión de los organismos de supervisión mencionados en los considerandos 162 a 168 ([342]). De conformidad con el artículo 13 del Reglamento de procedimiento del Tribunal de Vigilancia de Inteligencia Exterior, los responsables en materia de cumplimiento de los servicios de inteligencia estadounidenses están obligados a notificar cualquier vulneración de los procedimientos de selección de objetivos, minimización y consulta contemplados en el artículo 702 de la Ley de vigilancia de inteligencia exterior al Departamento de Justicia y a la Oficina del Director de Inteligencia Nacional, que, a su vez, las notifican al Tribunal de Vigilancia de Inteligencia Exterior. Además, el Departamento de Justicia y la Oficina del Director de Inteligencia Nacional presentan informes conjuntos semestrales de evaluación de la supervisión al Tribunal de Vigilancia de Inteligencia Exterior, en los que se indican las tendencias en materia de cumplimiento sobre la selección de objetivos, se describen pormenorizadamente las razones por las que se han producido determinados incidentes de cumplimiento y se señalan las medidas tomadas por los servicios de inteligencia para evitar que se repitan ([343]).

(174) En caso necesario (por ejemplo, si se detectan vulneraciones de los procedimientos de selección de objetivos), el Tribunal puede ordenar al servicio de inteligencia en cuestión que tome medidas correctoras ([344]). Estas medidas pueden ir desde medidas individuales a medidas estructurales, por ejemplo, desde la finalización de la adquisición de datos y la supresión de los datos obtenidos ilícitamente hasta un cambio en las prácticas de recogida de datos, incluidas nuevas directrices y formación para el personal ([345]). Por otra parte, en su revisión anual de las

([338]) Título 50, artículo 1873, letra b), del Código de Estados Unidos. Por otra parte, el artículo 402 dispone que el director de Inteligencia Nacional, en consulta con el secretario de Justicia, debe analizar la posibilidad de desclasificar las resoluciones, órdenes o dictámenes dictados por el Tribunal de Vigilancia de Inteligencia Exterior o el Tribunal de Apelación de Inteligencia Exterior [tal como se define en el artículo 601, letra e)] que contengan alguna interpretación significativa de cualquier disposición normativa, incluida las interpretaciones nuevas o significativas del término «criterio de selección específico», y, en función de dicho análisis, publicar en la medida de lo posible tales resoluciones, órdenes o dictámenes.

([339]) Título 50, artículo 1873, letra b), punto 7, y artículo 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) Véase el sitio web «IC in the Record», disponible en inglés en https://icontherecord.tumblr.com/.

([342]) El Tribunal de Vigilancia de Inteligencia Exterior llegó a la conclusión de que es evidente que los organismos competentes, así como la Oficina del Director de Inteligencia Nacional y la División de Seguridad Nacional del Departamento de Justicia, dedican recursos sustanciales a las responsabilidades de cumplimiento y supervisión que les impone el artículo 702. Por regla general, los supuestos de incumplimiento se detectan con prontitud y se toman medidas correctoras adecuadas para someter la información obtenida indebidamente o sujeta a obligación de destrucción a los procedimientos correspondientes. Resolución y resumen del fallo del Tribunal de Vigilancia de Inteligencia Exterior (expurgados) (2014), disponible en inglés en https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) Véase, por ejemplo, el informe del Departamento de Justicia y la Oficina del Director de Inteligencia Nacional para el Tribunal de Vigilancia de Inteligencia Exterior, sobre el cumplimiento del artículo 702 de la Ley de vigilancia de inteligencia exterior en el período comprendido entre junio de 2018 y noviembre de 2018, pp. 21 a 65.

([344]) Título 50, artículo 1803, letra h), del Código de Estados Unidos. Véase también el informe sobre el artículo 702, Junta de Supervisión de la Privacidad y las Libertades Civiles, p. 76. Además, véase la resolución y el resumen del fallo del Tribunal de Vigilancia de Inteligencia Exterior de 3 de octubre de 2011 como ejemplo de una resolución por incumplimiento en la que se ordenó al Ejecutivo subsanar las deficiencias detectadas en un plazo de treinta días. Disponible en inglés en https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Véase la carta Walton, sección 4, pp. 10 y 11. Véase también el dictamen del Tribunal de Vigilancia de Inteligencia Exterior de 18 de octubre de 2018, disponible en inglés en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, confirmado por el Tribunal de Apelación de Inteligencia Exterior (Foreign Intelligence Court of Review) en su dictamen de 12 de julio de 2019, disponible en inglés en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, en el que, entre otras cuestiones, el Tribunal de Vigilancia de Inteligencia Exterior ordenó a la Administración que cumpliera determinadas obligaciones de notificación, documentación e información con respecto al Tribunal de Vigilancia de Inteligencia Exterior.

([345]) Véase, por ejemplo, la resolución y el resumen del fallo del Tribunal de Vigilancia de Inteligencia Exterior de 6 de diciembre de 2019, página 76 (cuya publicación se autorizó el 4 de septiembre de 2020), en el que el Tribunal de Vigilancia de Inteligencia Exterior instó al Ejecutivo a presentar, antes del 28 de febrero de 2020, un informe escrito sobre las medidas que estaba tomando para mejorar los procesos de especificación y eliminación de los informes derivados de la información a que se refiere el artículo 702 de la Ley de vigilancia de inteligencia exterior que se retiran por motivos de cumplimiento, así como otras cuestiones. Véase también el anexo VII.

certificaciones contempladas en el artículo 702, el Tribunal de Vigilancia de Inteligencia Exterior analiza las incidencias de incumplimiento para determinar si las certificaciones presentadas cumplen los requisitos de la Ley de vigilancia de inteligencia exterior. Del mismo modo, si el Tribunal de Vigilancia de Inteligencia Exterior considera que las certificaciones del Ejecutivo no son suficientes, especialmente debido a incidentes particulares de cumplimiento, puede dictar una resolución por incumplimiento en la que exija al Ejecutivo que subsane la vulneración en un plazo de treinta días o que exija al Ejecutivo que cese la ejecución o no empiece a ejecutar la certificación contemplada del artículo 702. Por último, el Tribunal de Vigilancia de Inteligencia Exterior analiza las tendencias que observa en cuestiones de cumplimiento y puede exigir cambios en los procedimientos o una supervisión y notificación adicionales para corregir esas tendencias ([346]).

3.2.3. ***Reparación***

(175) Como se explica con más detalle en la presente sección, en los EE. UU. hay una serie de vías procesales que ofrecen a los interesados de la UE la posibilidad de solicitar a órganos cuasijudiciales independientes e imparciales que dicten medidas con carácter vinculante. Gracias a ellas, los particulares pueden acceder a sus datos personales, hacer que se revise la licitud del acceso a sus datos por los poderes públicos y, si se constata una vulneración, que se tomen medidas de reparación, en particular la rectificación o supresión de sus datos personales.

(176) En primer lugar, se establece una vía específica, en virtud del Decreto Presidencial n.º 14086, complementado por el Reglamento por el que se crea el Tribunal de Recurso en Materia de Protección de Datos, para tramitar y resolver las reclamaciones de particulares relativas a actividades de inteligencia de señales estadounidenses. Todo particular de la UE está legitimado para presentar una reclamación ante el órgano competente en relación con las posibles vulneraciones de la normativa estadounidense que regula las actividades de inteligencia de señales (por ejemplo, el Decreto Presidencial n.º 14086, el artículo 702 de la Ley de vigilancia de inteligencia exterior y el Decreto Presidencial n.º 12333) que afecten negativamente a sus intereses en materia de privacidad y libertades civiles ([347]). Pueden recurrir a esta vía los particulares procedentes de países o las organizaciones regionales de integración económica designados por el secretario de Justicia de los Estados Unidos como «Estados cualificados» ([348]). El 30 de junio de 2023, la UE y los tres países de la AELC que componen el EEE fueron designados por el secretario de Justicia como «Estados cualificados» con arreglo al artículo 3, letra f), del Decreto Presidencial n.º 14086 ([349]). Esta designación se entiende sin perjuicio del artículo 4, apartado 2, del Tratado de la Unión Europea.

(177) Los interesados de la UE que quieran presentar tal reclamación deben enviarla primero a la autoridad de control del Estado miembro de la UE competente en materia de supervisión del tratamiento de datos personales por parte de las autoridades públicas (APD) ([350]). De este modo, se garantiza una vía fácil de impugnación, ya que los particulares se pueden dirigir a una autoridad «cercana» con la que pueden comunicarse en su propia lengua. Una vez que se haya comprobado el cumplimiento los requisitos para presentar una reclamación a que se refiere el considerando 178, la APD competente canaliza la reclamación, a través de la Secretaría del Comité Europeo de Protección de Datos, al órgano correspondiente.

(178) Los requisitos de admisión a trámite de las reclamaciones no son exigentes, ya que los particulares no necesitan demostrar que sus datos hayan sido efectivamente objeto de actividades de inteligencia de señales estadounidenses ([351]). Al mismo tiempo, para que el órgano en cuestión tenga un mínimo con el que empezar a analizar la cuestión, debe proporcionarse determinada información básica, como por ejemplo: los datos personales que se cree que se han transferido a los EE. UU. y los medios por los que se cree que han sido transferidos; qué organismos públicos estadounidenses se cree que están implicados en la presunta vulneración (si se conocen); los indicios en que se fundamenta la alegación de que se ha producido una vulneración de la normativa estadounidense (aunque de nuevo no es necesario demostrar que los servicios de inteligencia estadounidenses recogieron los datos personales) y la naturaleza de la medida de reparación solicitada.

([346]) Véase el anexo VII.

([347]) Véase el artículo 4, letra k), inciso iv), del Decreto Presidencial n.º 14086, que establece que la reclamación ante el órgano competente debe ser presentada por el reclamante actuando en nombre propio (es decir, no como representante de un Gobierno, organización no gubernamental u organización intergubernamental). El concepto «adversamente afectado» no exige al reclamante que supere un determinado mínimo para poder acogerse a la vía procesal (véase el considerando 178 a este respecto). Más bien, aclara que el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y el Tribunal de Recurso en Materia de Protección de Datos tienen competencia para reparar las vulneraciones del Derecho estadounidense que rige las actividades de inteligencia de señales que afecten adversamente a las libertades civiles y la privacidad del reclamante. En sentido contrario, las vulneraciones de las obligaciones que impone el Derecho estadounidense que no están diseñadas para proteger a los particulares (por ejemplo, las obligaciones presupuestarias) no están amparadas por la competencia del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y del Tribunal de Recurso en Materia de Protección de Datos.

([348]) Artículo 3, letra f), del Decreto Presidencial n.º 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Artículo 4, letra d), inciso v), del Decreto Presidencial n.º 14086.

([351]) Véase el artículo 4, letra k), incisos i) a iv), del Decreto Presidencial n.º 14086.

(179) La investigación inicial de las reclamaciones presentadas por esta vía la lleva a cabo el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional, cuya función y competencias legales se han ampliado para abarcar las medidas específicas tomadas con arreglo al Decreto Presidencial n.º 14086 ([352]). Dentro de la Comunidad de Inteligencia, el responsable de la protección de las libertades civiles se encarga de, entre otras cuestiones: garantizar que la protección de las libertades civiles y la privacidad se integre adecuadamente en las directrices y procedimientos de la Oficina del Director de Inteligencia Nacional y los servicios de inteligencia; supervisar el cumplimiento por parte de la Oficina de las obligaciones aplicables en materia de libertades civiles y privacidad; y realizar evaluaciones de impacto en materia de privacidad ([353]). El responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional solo puede ser destituido por el director de Inteligencia Nacional en supuestos justificados, a saber, en caso de falta administrativa, delito contra la Administración pública, violación de la seguridad, incumplimiento de deberes o incapacidad ([354]).

(180) Al llevar a cabo su examen, el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional tiene acceso a la información para su evaluación y puede recabar la asistencia obligada de los responsables de la protección de la privacidad y de las libertades civiles en los diferentes servicios de inteligencia ([355]). Se prohíbe a los servicios de inteligencia impedir el examen del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional o influir indebidamente en este. Esta prohibición se extiende al director de Inteligencia Nacional, que no debe interferir en el examen ([356]). Al examinar la reclamaciones, el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional debe aplicar la normativa en vigor de manera imparcial, teniendo en cuenta tanto los intereses de seguridad nacional en las actividades de inteligencia de señales como la protección de la privacidad ([357]).

(181) En el marco de su examen, el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional determina si se ha producido una vulneración de la normativa estadounidense aplicable y, en tal caso, dicta medidas de reparación adecuadas ([358]), es decir, medidas que reparan plenamente la vulneración detectada, como poner fin a la obtención ilícita de datos, suprimir los datos recogidos ilícitamente, eliminar los resultados de consultas realizadas de forma inadecuada sobre datos recogidos lícitamente por otros medios, restringir el acceso a los datos recogidos lícitamente a personal debidamente formado o retirar informes de inteligencia que contengan datos obtenidos sin autorización suficiente o que hayan sido difundidos ilícitamente ([359]). Las resoluciones del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional respecto de reclamaciones individuales (incluidas las medidas de reparación) son vinculantes para los servicios de inteligencia en cuestión ([360]).

(182) El responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional debe conservar la documentación de su examen y elaborar una resolución clasificada que explique el fundamento de sus conclusiones fácticas, la determinación de si se ha producido una vulneración y la determinación de la reparación adecuada ([361]). Si el examen del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional pone de manifiesto una vulneración por parte de autoridades sujetas al control del Tribunal de Vigilancia de Inteligencia Exterior, el responsable de la protección de las libertades civiles también debe presentar un informe clasificado al fiscal general adjunto de Seguridad Nacional, que a su vez tiene la obligación de notificar la vulneración al Tribunal de Vigilancia de Inteligencia Exterior, que puede tomar nuevas medidas coercitivas (de conformidad con el procedimiento descrito en los considerandos 173 a 174) ([362]).

(183) Una vez concluido el examen, el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional informa al reclamante, a través de la autoridad nacional, de que en el examen no se apreció ninguna vulneración o de que el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional exigió una reparación adecuada ([363]). De este modo, se puede proteger la confidencialidad de las actividades realizadas para proteger la seguridad nacional, al tiempo que los particulares cuentan con una resolución que confirma que su reclamación ha sido debidamente investigada y resuelta. Además, esta resolución puede ser impugnada por el particular. A tal fin, se le informa de la posibilidad de recurrir al Tribunal de Recurso en Materia de Protección de Datos para que revise los pronunciamiento del responsable de la protección de las libertades civiles (véanse los considerandos 184 y siguientes) y de que, en caso de que se recurra ante el Tribunal, se seleccionará a un abogado especial para defender el interés del reclamante ([364]).

([352]) Artículo 3, letra c), inciso iv), del Decreto Presidencial n.º 14086. Véase también la Ley de seguridad nacional, de 1947 (título 50, artículo 403, apartado 3 *quinquies*, que comprende el artículo 103 *quinquies* de la Ley), relativa a la función del responsable de la protección de las libertades civiles en la Oficina del Director de Inteligencia Nacional.

([353]) Título 50, artículo 3029, letra b), del Código de Estados Unidos.

([354]) Artículo 3, letra c), inciso iv), del Decreto Presidencial n.º 14086.

([355]) Artículo 3, letra c), inciso iii), del Decreto Presidencial n.º 14086.

([356]) Artículo 3, letra c), inciso iv), del Decreto Presidencial n.º 14086.

([357]) Artículo 3, letra c), inciso i), subletra B), subincisos i) y iii), del Decreto Presidencial n.º 14086.

([358]) Artículo 3, letra c), inciso i), del Decreto Presidencial n.º 14086.

([359]) Artículo 4, letra a), del Decreto Presidencial n.º 14086.

([360]) Artículo 3, letras c) y d), del Decreto Presidencial n.º 14086.

([361]) Artículo 3, letra c), inciso i), subletras F) a G), del Decreto Presidencial n.º 14086.

([362]) Véase también el artículo 3, letra c), inciso i), subletra D), del Decreto Presidencial n.º 14086.

([363]) Artículo 3, letra c), inciso i), subletra E), punto 1, del Decreto Presidencial n.º 14086.

([364]) Artículo 3, letra c), inciso i), subletra E), puntos 2 a 3, del Decreto Presidencial n.º 14086.

(184) Todo reclamante, así como cada servicio de la Comunidad de Inteligencia, puede recurrir la resolución del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional ante el Tribunal de Recurso en Materia de Protección de Datos. Dicho recurso debe presentarse en un plazo de sesenta días a partir de la recepción de la notificación del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional de que ha concluido su examen e incluir cualquier información que el particular quiera comunicar al Tribunal de Recurso en Materia de Protección de Datos (por ejemplo, argumentación sobre cuestiones de Derecho o la aplicación del Derecho al caso ([365])). Los interesados de la UE pueden volver a presentar su solicitud a la APD competente (véase el considerando 177).

(185) El Tribunal de Recurso en Materia de Protección de Datos es un órgano cuasijudicial independiente establecido por el secretario de Justicia con arreglo a el Decreto Presidencial n.º 14086 ([366]). Está compuesto por al menos seis magistrados, nombrados por el secretario de Justicia tras consultarlo con la Junta de Supervisión de la Privacidad y las Libertades Civiles, el secretario de Comercio y el director de Inteligencia Nacional por mandatos renovables de cuatro años ([367]). El nombramiento de los magistrados por el secretario de Justicia se basa en los criterios utilizados por el poder ejecutivo al valorar a los candidatos a la judicatura federal, dando preponderancia a la experiencia judicial previa ([368]). Además, los magistrados deben ser profesionales del Derecho (es decir, miembros colegiados en activo y debidamente autorizados para ejercer la abogacía) y tener la experiencia adecuada en materia de privacidad y normativa de seguridad nacional. El secretario de Justicia debe procurar que al menos la mitad de los magistrados en cualquier momento tengan experiencia judicial previa, y todos los magistrados deben contar con las habilitaciones de seguridad necesarias para poder acceder a información clasificada de seguridad nacional ([369]).

(186) Solo las personas que reúnan las cualificaciones mencionadas en el considerando 185 y que no sean empleadas del poder ejecutivo en el momento de su nombramiento o en los dos años anteriores pueden ser nombradas para el Tribunal de Recurso en Materia de Protección de Datos. Del mismo modo, durante su mandato en el Tribunal de Recurso en Materia de Protección de Datos, los magistrados no pueden desempeñar ninguna función o empleo oficial en el Ejecutivo estadounidense (solo pueden ejercer de magistrados del Tribunal de Recurso en Materia de Protección de Datos) ([370]).

(187) La independencia de sus pronunciamientos se logra a través de una serie de garantías. En particular, el poder ejecutivo (el secretario de Justicia y los servicios de inteligencia) no puede injerirse o influir indebidamente en la actividad del Tribunal de Recurso en Materia de Protección de Datos ([371]). El propio Tribunal de Recurso en Materia de Protección de Datos está obligado a resolver imparcialmente los asuntos ([372]) y funciona con arreglo a su propio reglamento interno (aprobado por mayoría). Además, los magistrados del Tribunal de Recurso en Materia de Protección de Datos solo pueden ser destituidos por el secretario de Justicia y exclusivamente en supuestos justificados (falta administrativa, delito contra la Administración pública, violación de la seguridad, incumplimiento de deberes o incapacidad), tras haber tenido debidamente en cuenta el régimen aplicable a los magistrados federales, establecido en el Reglamento sobre los procedimientos relativos a la conducta y la incapacidad de jueces y magistrados (Rules for Judicial-Conduct and Judicial-Disability Proceedings) ([373]).

([365]) Artículo 201.6, letras a) a b), del Reglamento sobre el Tribunal de Recurso.

([366]) Artículo 3, letra d), inciso i), y Reglamento sobre el Tribunal de Recurso. La Corte Suprema de los EE. UU. ha reconocido la posibilidad de que el secretario de Justicia establezca órganos independientes con facultades decisorias, incluida la posibilidad de juzgar casos particulares; véase, en particular, los asuntos United States ex rel. Accardi c. Shaughnessy (volumen 347, página 260, del Repertorio Jurisprudencial de los EE. UU., de 1954) y United States v. Nixon (volumen 418, páginas 683 y 695, del Repertorio Jurisprudencial de los EE. UU., de 1974). El cumplimiento de las distintas obligaciones del Decreto Presidencial n.º 14086, como por ejemplo los criterios y procedimientos para el nombramiento y la destitución de los magistrados del Tribunal de Recurso en Materia de Protección de Datos, está sometido a la supervisión del inspector general del Departamento de Justicia (véase también el considerando 109 respecto de las competencias legales de los inspectores generales).

([367]) Artículo 3, letra d), inciso i), subletra A), del Decreto Presidencial n.º 14086 y artículo 201.3, letra a), del Reglamento sobre el Tribunal de Recurso.

([368]) Artículo 201.3, letra b), del Reglamento sobre el Tribunal de Recurso.

([369]) Artículo 3, letra d), inciso i), subletra B), del Decreto Presidencial n.º 14086.

([370]) Artículo 3, letra d), inciso i), subletra A), del Decreto Presidencial n.º 14086 y artículo 201.3, letras a) y c), del Reglamento sobre el Tribunal de Recurso. Las personas nombradas para el Tribunal de Recurso en Materia de Protección de Datos pueden participar en actividades extrajudiciales, en particular actividades empresariales, financieras, de recaudación de fondos sin ánimo de lucro y fiduciarias, así como la práctica del Derecho, siempre que dichas actividades no interfieran en el desempeño imparcial de sus funciones o en la eficacia o independencia del Tribunal de Recurso en Materia de Protección de Datos [artículo 201.7, letra c), del Reglamento sobre el Tribunal de Recurso].

([371]) Artículo 3, letra d), incisos iii) a iv), del Decreto Presidencial n.º 14086 y artículo 201.7, letra d), del Reglamento sobre el Tribunal de Recurso.

([372]) Artículo 3, letra d), inciso i), subletra D), del Decreto Presidencial n.º 14086 y artículo 201.9 del Reglamento sobre el Tribunal de Recurso.

([373]) Artículo 3, letra d), inciso iv), del Decreto Presidencial n.º 14086 y artículo 201.7, letra d), del Reglamento sobre el Tribunal de Recurso. Véase también el asunto Bumap c. United States (volumen 252, páginas 512 y 515, del Repertorio Jurisprudencial de los EE. UU., de 1920), en el que se confirmó el principio de larga data del Derecho estadounidense según el cual la competencia para destituir se deriva de la competencia nombrar; también lo confirmó el Servicio Jurídico (Office of Legal Counsel) del Departamento de Justicia en La separación constitucional de poderes entre el presidente y el Congreso [The Constitutional Separation of Powers Between the President and Congress; 20 Op. O.L.C. 124, 166 (1996)].

(188) Los recursos presentados al Tribunal de Recurso en Materia de Protección de Datos son examinados por salas de dos magistrados y un magistrado ponente que deben actuar de conformidad con el Código de conducta de los jueces y magistrados estadounidenses (Code of Conduct for U.S. Judges) ([374]). Cada sala está asistida por un abogado especial ([375]), que tiene acceso a toda la información relacionada con el asunto, incluida la información clasificada ([376]). La función del abogado especial es garantizar que los intereses del reclamante estén representados y que la sala esté bien informada sobre todas las cuestiones de hecho y de Derecho pertinentes ([377]). Para cumplir adecuadamente su función respecto del recurso del particular, el abogado especial puede solicitar información a este mediante preguntas escritas ([378]).

(189) El Tribunal de Recurso en Materia de Protección de Datos revisa las resoluciones del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional (tanto si se ha producido una vulneración de la normativa estadounidense aplicable como si la reparación ha sido adecuada) basándose, como mínimo, en el expediente de la investigación del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional, así como en cualquier información y documentos del reclamante, del abogado especial o del servicio de inteligencia ([379]). Las salas del Tribunal de Recurso en Materia de Protección de Datos tienen acceso a toda la información necesaria para resolver, que pueden obtener a través del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional (la sala puede, por ejemplo, solicitar al responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional que complemente el expediente con información adicional o conclusiones fácticas si fuera necesario para resolver) ([380]).

(190) El Tribunal de Recurso en Materia de Protección de Datos puede 1) resolver que no existen pruebas que indiquen que se han realizado actividades de inteligencia de señales que incluyan datos personales del reclamante, 2) determinar que la resolución del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional era jurídicamente correcta y estaba respaldada por pruebas sustanciales o, 3) si el Tribunal de Recurso en Materia de Protección de Datos no está de acuerdo con la resolución del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional (si se ha producido una vulneración de la normativa estadounidense aplicable o si las medidas reparatorias son adecuadas), dar su propio fallo ([381]).

([374]) Artículo 3, letra d), inciso i), subletra B), del Decreto Presidencial n.º 14086 y artículo 201.7, letras a) a c), del Reglamento sobre el Tribunal de Recurso. La Oficina de Privacidad y Libertades Civiles del Departamento de Justicia, que es la responsable de prestar auxilio administrativo al Tribunal de Recurso en Materia de Protección de Datos y a los abogados especiales (véase el artículo 201.5 del Reglamento sobre el Tribunal de Recurso), selecciona una sala de tres personas que van rotando, con el fin de garantizar que cada sala tenga al menos un magistrado con experiencia judicial previa (si ninguno de los magistrado de la sala tiene dicha experiencia, el magistrado ponente será el primero elegido por la Oficina de Privacidad y Libertades Civiles).

([375]) Artículo 201.4 del Reglamento sobre el Tribunal de Recurso. El secretario de Justicia nombra al menos dos abogados especiales, en consulta con el secretario de Comercio, el director de Inteligencia Nacional y la Junta de Supervisión de la Privacidad y las Libertades Civiles, para dos mandatos renovables. Los abogados especiales deben tener experiencia adecuada en el ámbito de la normativa en materia de privacidad y seguridad nacional, ser abogados experimentados, ser miembros colegiados en activo y estar debidamente autorizados para ejercer la abogacía. Además, en el momento de su nombramiento inicial, no deben haber sido empleados del poder ejecutivo durante los dos años anteriores. Por cada recurso, el magistrado ponente selecciona un abogado especial para asistir a la sala; véase el artículo 201.8, letra a), del Reglamento sobre el Tribunal de Recurso.

([376]) Artículo 201.8, letra c), y artículo 201.11 del Reglamento sobre el Tribunal de Recurso.

([377]) Artículo 3, letra d), inciso i), subletra C), del Decreto Presidencial n.º 14086 y artículo 201.8, letra e), del Reglamento sobre el Tribunal de Recurso. El abogado especial no actúa por cuenta de la parte reclamante ni tiene una relación abogado-cliente con esta.

([378]) Artículo 201.8, letras d) y e), del Reglamento sobre el Tribunal de Recurso. Estas cuestiones son examinadas en primer lugar por la Oficina de Privacidad y Libertades Civiles, en consulta con los servicios de inteligencia pertinentes, con el fin de especificar y excluir la información clasificada, privilegiada o protegida antes de transmitirla al reclamante. La información adicional recibida por el abogado especial en respuesta a estas preguntas se incluye en las observaciones del abogado especial al Tribunal de Recurso en Materia de Protección de Datos.

([379]) Artículo 3, letra d), inciso i), subletra D), del Decreto Presidencial n.º 14086.

([380]) Artículo 3, letra d), inciso iii), del Decreto Presidencial n.º 14086 y artículo 201.9, letra b), del Reglamento sobre el Tribunal de Recurso.

([381]) Artículo 3, letra d), inciso i), subletra E), del Decreto Presidencial n.º 14086 y artículo 201.9, letras c) a e), del Reglamento sobre el Tribunal de Recurso. Según la definición de medidas reparatorias adecuadas del artículo 4, letra a), del Decreto Presidencial n.º 14086, el Tribunal de Recurso en Materia de Protección de Datos debe tener en cuenta las formas en que las vulneraciones del tipo en cuestión han sido resueltas normalmente al decidir las medidas reparatorias en el asunto concreto, es decir, el Tribunal de Recurso en Materia de Protección de Datos debe considerar, entre otros factores, cómo se han resuelto otros asuntos de incumplimiento anteriormente para garantizar que la reparación sea efectiva y adecuada.

(191) En todos los casos, el Tribunal de Recurso en Materia de Protección de Datos toma su decisión por mayoría y la plasma por escrito. Si durante su análisis el Tribunal constata una vulneración de la normativa aplicable, al resolver dicta medidas reparatorias adecuadas, como poner fin a la obtención ilícita de datos, suprimir los datos recogidos ilícitamente, eliminar los resultados de consultas realizadas de forma inadecuada, restringir el acceso a los datos recogidos lícitamente a personal debidamente formado o retirar informes de inteligencia que contengan datos obtenidos sin autorización suficiente o que hayan sido difundidos ilícitamente ([382]). La resolución del Tribunal de Recurso en Materia de Protección de Datos es vinculante y firme con respecto a la reclamación ([383]). Además, si se pone de manifiesto una vulneración por parte de autoridades sujetas al control del Tribunal de Vigilancia de Inteligencia Exterior, el Tribunal de Recurso en Materia de Protección de Datos también debe presentar un informe clasificado al fiscal general adjunto de Seguridad Nacional, que a su vez tiene la obligación de notificar la vulneración al Tribunal de Vigilancia de Inteligencia Exterior, que puede tomar nuevas medidas coercitivas (de conformidad con el procedimiento descrito en los considerandos 173 a 174) ([384]).

(192) Las resoluciones de las salas del Tribunal de Recurso en Materia de Protección de Datos se transmiten al responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional ([385]). En los casos en que el recurso al Tribunal de Recurso en Materia de Protección de Datos procede del reclamante, se notifica a este, a través de la autoridad nacional correspondiente, que el Tribunal de Recurso en Materia de Protección de Datos, bien no detectó ninguna vulneración pertinente, bien resolvió dictando medidas reparatorias adecuadas ([386]). La Oficina de Privacidad y Libertades Civiles del Departamento de Justicia lleva un registro de toda la información examinada por el Tribunal de Recurso en Materia de Protección de Datos y de todas sus resoluciones, que se pone a disposición de las salas del Tribunal de Recurso en Materia de Protección de Datos como precedentes no vinculantes ([387]).

(193) El Departamento de Comercio también está obligado a llevar un registro de cada persona que haya presentado una reclamación ([388]). Para aumentar la transparencia, el Departamento de Comercio debe ponerse en contacto, al menos cada cinco años, con los servicios de inteligencia pertinentes para verificar si la información relativa a un recurso ante el Tribunal de Recurso en Materia de Protección de Datos ha sido desclasificada ([389]). Si este es el caso, se notifica al particular que dicha información puede consultarse con arreglo a la normativa aplicable (es decir, que puede solicitar acceso con arreglo a la Ley de libertad de información; véase el considerando 199).

(194) Por último, el correcto funcionamiento de esta vía de recurso está sujeto a una evaluación periódica e independiente. Más concretamente y de conformidad con el Decreto Presidencial n.º 14086, el funcionamiento de esta vía de recurso está sujeto a revisión anual por parte de la Junta de Supervisión de la Privacidad y las Libertades Civiles, un organismo independiente (véase el considerando 110) ([390]). Como parte de esta revisión, la Junta de Supervisión de la Privacidad y las Libertades Civiles evalúa, entre otros aspectos: si el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y el Tribunal de Recurso en Materia de Protección de Datos han tramitado las reclamaciones de manera oportuna; si han obtenido pleno acceso a la información necesaria; si las garantías sustantivas del Decreto Presidencial n.º 14086 se han tenido debidamente en cuenta en los recursos; y si la Comunidad de Inteligencia ha cumplido plenamente las resoluciones del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y el Tribunal de Recurso en Materia de Protección de Datos. La Junta de Supervisión de la Privacidad y las Libertades Civiles debe presentar un informe sobre el resultado de su revisión al presidente de los EE. UU, al secretario de Justicia, al director de Inteligencia Nacional, a los jefes de los servicios de inteligencia, al responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y a los comités sobre inteligencia del Congreso, que también se publicará en una versión no clasificada y, a su vez, contribuirá a la revisión periódica del funcionamiento de la presente Decisión que llevará a cabo la Comisión Europea. El secretario de Justicia, el director de Inteligencia Nacional, el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y los jefes de los servicios de inteligencia están obligados a cumplir o tratar de otro modo todas las recomendaciones incluidas en dichos informes. Además, la Junta de Supervisión de la Privacidad y las Libertades Civiles debe hacer una certificación pública anual de si los recursos se tramitan de conformidad con los requisitos del Decreto Presidencial n.º 14086.

([382]) Artículo 4, letra a), del Decreto Presidencial n.º 14086.

([383]) Artículo 3, letra d), inciso iii), del Decreto Presidencial n.º 14086 y artículo 201.9, letra g), del Reglamento sobre el Tribunal de Recurso. Dado que la resolución del Tribunal de Recurso en Materia de Protección de Datos es firme y vinculante, ningún otro organismo o institución administrativo ejecutivo (ni siquiera el presidente de los Estados Unidos) puede dejar sin efecto la resolución del Tribunal de Recurso en Materia de Protección de Datos. Este extremo fue confirmado en su jurisprudencia por la Corte Suprema, que aclaró que, al haber delegado el secretario de Justicia su competencia exclusiva dentro del Ejecutivo para tomar decisiones vinculantes respecto de organismos independientes, este renuncia a poder tomar todo tipo de decisiones sobre dicho organismo; véase el asunto United States ex rel. Accardi c. Shaughnessy, (volumen 347, página 260, del Repertorio Jurisprudencial de los EE. UU., de 1954).

([384]) Artículo 3, letra d), inciso i), subletra F), del Decreto Presidencial n.º 14086 y artículo 201.9, letra i), del Reglamento sobre el Tribunal de Recurso.

([385]) Artículo 201.9, letra h), del Reglamento sobre el Tribunal de Recurso.

([386]) Artículo 3, letra d), inciso i), subletra H), del Decreto Presidencial n.º 14086 y artículo 201.9, letra h), del Reglamento sobre el Tribunal de Recurso. En lo que se refiere al carácter de la notificación, véase el artículo 201.9, letra h), punto 3, del Reglamento sobre el Tribunal de Recurso.

([387]) Artículo 201.9, letra j), del Reglamento sobre el Tribunal de Recurso.

([388]) Artículo 3, letra d), inciso v), subletra A), del Decreto Presidencial n.º 14086.

([389]) Artículo 3, letra d), inciso v), del Decreto Presidencial n.º 14086.

([390]) Artículo 3, letra e), del Decreto Presidencial n.º 14086. Véase también (en inglés) https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Además de la vía procesal específica establecida en el Decreto Presidencial n.º 14086, los particulares (con independencia de su nacionalidad o lugar de residencia) también pueden recurrir a la vía judicial ordinaria estadounidense ([391]).

(196) En particular, la Ley de vigilancia de inteligencia exterior y una ley conexa legitiman a los particulares para: interponer una demanda de indemnización por daños y perjuicios contra los EE. UU. cuando se haya utilizado o comunicado información suya de manera intencionada e ilícita ([392]); interponer una demanda de indemnización por daños y perjuicios contra funcionarios públicos estadounidenses cuando actúen a título personal ([393]); e impugnar la legalidad de la vigilancia (y solicitar la supresión de la información) en el supuesto de que el Ejecutivo estadounidense pretenda utilizar o comunicar información obtenida o derivada de la vigilancia electrónica en contra del interesado en procesos judiciales o procedimientos administrativos emprendidos en dicho país ([394]). De manera más general, si el Ejecutivo tiene la intención de utilizar la información obtenida durante las operaciones de inteligencia contra un sospechoso en un asunto penal, la Constitución y ciertas leyes ([395]) imponen la obligación de comunicar determinada información de modo que el encausado pueda impugnar la licitud de la recogida y el uso de medios de pruebas por parte del Ejecutivo.

(197) Por otra parte, hay una serie de vías procesales específicas con las que impugnar la actuaciones de los funcionarios por el acceso ilícito a datos personales y la utilización de estos por parte del Ejecutivo, incluso con presuntos fines de seguridad nacional (a saber, la Ley de abusos y fraudes informáticos ([396]), la Ley de privacidad de las comunicaciones electrónicas ([397]) y la Ley del derecho la privacidad financiera ([398])). Todas estas acciones judiciales se refieren a datos, objetivos o tipos de acceso específicos (por ejemplo, el acceso remoto a un ordenador a través de internet) y pueden ejercitarse en determinadas circunstancias (tales como los actos u omisiones dolosos, los actos u omisiones que no se realizan como parte de un cargo o función oficial y la existencia de daños y perjuicios).

(198) Otra vía procesal más general se contempla en la Ley de lo contencioso-administrativo ([399]), según la cual todo particular que sufra un perjuicio por actuaciones ilícitas de un organismo público o que se haya visto adversamente afectado o perjudicado por la actuación de un organismo público está legitimado para ejercitar la correspondiente acción judicial ([400]). En este sentido, se puede demandar al órgano jurisdiccional que declare ilícitas y anule la actuación, las constataciones y las conclusiones del organismo público que sean arbitrarias, caprichosas, un abuso de la facultad de apreciación o, de otro modo, no conformes a Derecho ([401]). Por ejemplo, una corte federal de apelaciones resolvió, respecto de una acción de las contempladas en la Ley de lo contencioso-administrativo ejercitada en 2015, que la recogida masiva de metadatos telefónicos por parte del Ejecutivo estadounidense no estaba autorizada por el artículo 501 de la Ley de vigilancia de inteligencia exterior ([402]).

([391]) En este caso, será necesario contar con la legitimación activa correspondiente. Esta regla, que se aplica a cualquier particular con independencia de su nacionalidad, se deriva del principio de *case or controversy* del artículo III de la Constitución de los EE. UU. Según la Corte Suprema, este principio exige 1) que el particular haya sufrido un perjuicio concreto (es decir, una lesión de un interés jurídicamente protegido que sea concreta, determinada y presente o inminente), 2) que exista una relación causal entre el perjuicio y la conducta que se impugna judicialmente y 3) que sea probable, y no simplemente posible, que se repare el perjuicio si se dicta una resolución judicial favorable (véase el asunto Lujan c. Defenders of Wildlife, volumen 504, página 555, del Repertorio Jurisprudencial de los EE. UU., de 1992).

([392]) Título 18, artículo 2712, del Código de Estados Unidos.

([393]) Título 50, artículo 1810, del Código de Estados Unidos.

([394]) Título 50, artículo 1806, del Código de Estados Unidos.

([395]) Véanse, respectivamente, el asunto Brady c. Maryland (volumen 373, página 83, del Repertorio Jurisprudencial de los EE. UU., de 1963) y la Ley Jencks (Jencks Act) (título 18, artículo 3500, del Código de Estados Unidos).

([396]) Título 18, artículo 1030, del Código de Estados Unidos.

([397]) Título 18, artículos 2701 a 2712, del Código de Estados Unidos.

([398]) Título 12, artículo 3417, del Código de Estados Unidos.

([399]) Título 5, artículo 702, del Código de Estados Unidos.

([400]) Por lo general, solo las actuaciones definitivas de los organismos públicos, y no las actuaciones preliminares, de instrucción o intermedias, están sujetas a revisión judicial. Véase el título 5, artículo 704, del Código de Estados Unidos.

([401]) Título 5, artículo 706, apartado 2, letra A), del Código de Estados Unidos.

([402]) ACLU c. Clapper, volumen 785, tercera serie del Repertorio Jurisprudencial Federal, página 787 (Corte de Apelaciones del Segundo Distrito), 2015. La Ley de libertad de los Estados Unidos puso fin en 2015 al programa de recogida masiva de datos telefónicos impugnado en estos asuntos.

(199) Por último, además de las vías procesales mencionadas en los considerandos 176 a 198, todo particular tiene derecho a solicitar acceso a los documentos que obren en poder los organismos federales en el marco de la Ley de libertad de información, especialmente cuando contengan datos personales de ese particular ([403]). La concesión de este acceso también puede facilitar el ejercicio de las acciones judiciales correspondientes ante los órganos jurisdiccionales ordinarios, especialmente para demostrar que se goza de legitimación activa. Los organismos pueden no proporcionar información en supuestos excepcionales tasados, como el acceso a información clasificada de seguridad nacional y a información relativa a investigaciones policiales ([404]), pero los reclamantes que no estén satisfechos con la respuesta pueden impugnarla primero por la vía administrativa y, posteriormente, por la judicial (federal) ([405]).

(200) De lo anterior se desprende que, cuando las autoridades policiales y las autoridades de seguridad nacional estadounidenses acceden a datos personales que entran en el ámbito de aplicación de la presente Decisión, dicho acceso se rige por un marco jurídico que establece las condiciones en las que puede concederse el acceso y garantiza que el acceso y el uso ulterior de los datos se limiten a lo que sea necesario y proporcionado al objetivo perseguido de interés general. Estas garantías pueden hacerlas valer los particulares que gocen de legitimación.

4. **CONCLUSIÓN**

(201) La Comisión considera que los EE. UU. garantizan, a través de los principios en materia de privacidad publicados por el Departamento de Comercio de los EE. UU., un nivel de protección de los datos personales transferidos desde la UE a entidades estadounidenses certificadas en el Marco de Privacidad de Datos UE-EE. UU. que es equivalente en lo esencial al garantizado por el Reglamento (UE) 2016/679.

(202) Por otra parte, la Comisión considera que la aplicación efectiva de los principios en materia de privacidad queda garantizada por las obligaciones de transparencia y la administración del Marco de Privacidad de Datos UE-EE. UU. que realiza el Departamento de Comercio. Además, en su conjunto, los mecanismos de supervisión y las vías de impugnación contemplados en el Derecho estadounidense son suficientes para detectar y sancionar en la práctica las vulneraciones de la normativa de protección de datos y brindan al interesado medios jurídicos para solicitar el acceso a sus datos personales y, en su caso, su rectificación o supresión.

(203) Por último, sobre la base de la información disponible acerca del ordenamiento jurídico estadounidense, en particular la información que figura en los anexos VI y VII, la Comisión considera que toda injerencia por motivos de interés público, en particular a efectos penales y de seguridad nacional, por los poderes públicos estadounidenses en los derechos fundamentales de los particulares cuyos datos personales sean transferidos desde la UE a los EE. UU. en el Marco de Privacidad de Datos UE-EE. UU. se limitará a lo estrictamente necesario para lograr el objetivo legítimo perseguido, y que existen garantías jurídicas efectiva contra tales injerencias. Por lo tanto y teniendo en consideración las constataciones anteriores, debe concluirse que los EE. UU. garantizan un nivel de protección adecuado, en el sentido del artículo 45 del Reglamento (UE) 2016/679, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, de los datos personales transferidos desde la UE a las entidades participantes en el Marco de Privacidad de Datos UE-EE. UU.

(204) Dado que las limitaciones, garantías, vías de impugnación y órganos establecidos por el Decreto Presidencial n.º 14086 son elementos esenciales del marco jurídico estadounidense en el que se basa la evaluación de la Comisión, la adopción de la presente Decisión depende notoriamente de que los servicios de inteligencia estadounidenses aprueben directrices y procedimientos actualizados que pongan en práctica los preceptos del Decreto Presidencial n.º 14086, y de la designación de la UE como organización internacional cualificada a efectos de la vía de reparación; ambas decisiones han sido tomadas, respectivamente, el 3 de julio de 2023 (véase el considerando 126) y el 30 de junio de 2023 (véase el considerando 176).

([403]) Título 5, artículo 552, del Código de Estados Unidos. Existen leyes similares de los Estados federados.

([404]) De ser así, lo normal es que el particular solo reciba una respuesta tipo en la que el servicio correspondiente se niegue a confirmar o desmentir la existencia de ningún tipo de documentos. Véase ACLU c. CIA, volumen 710, tercera serie del Repertorio Jurisprudencial Federal, página 422 (Corte de Apelaciones del Distrito de Columbia), 2014. Los criterios y la duración de la clasificación se establecen en el Decreto Presidencial n.º 13526, que dispone, como norma general, que debe fijarse una fecha o hecho específico para la desclasificación en función de la duración del carácter delicado de la información para la seguridad nacional, momento en el que la información debe desclasificarse automáticamente (véase el artículo 1, apartado 5, del Decreto Presidencial n.º 13526).

([405]) El órgano jurisdiccional resuelve, como si fuese por primera vez, si los documentos se están reteniendo lícitamente y puede obligar al Ejecutivo a conceder acceso a estos [título 5, artículo 552, letra a), punto 4, subletra B), del Código de Estados Unidos].

5. EFECTOS DE LA PRESENTE DECISIÓN Y ACTUACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

(205) Los Estados miembros y sus organismos están obligados a tomar las medidas necesarias para dar cumplimiento a los actos de las instituciones de la UE, ya que estos disfrutan de presunción de legalidad y producen, por consiguiente, efectos jurídicos en tanto no hayan sido revocados, anulados en el marco de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad.

(206) Por lo tanto, toda decisión de adecuación de la Comisión adoptada en virtud del artículo 45, apartado 3, del Reglamento (UE) 2016/679 vincula a todos los organismos de los Estados miembros destinatarios, incluidas sus autoridades de control independientes. En particular, pueden producirse transferencias de responsables o encargados del tratamiento en la UE a entidades certificadas estadounidenses sin necesidad de autorización adicional.

(207) Cabe recordar que, de conformidad con el artículo 58, apartado 5, del Reglamento (UE) 2016/679 y como explicó el Tribunal de Justicia en la sentencia Schrems ([406]), cuando una autoridad nacional de protección de datos cuestiona, en especial a raíz de una reclamación, la compatibilidad de una decisión de adecuación de la Comisión con los derechos fundamentales del particular a la privacidad y la protección de los datos, el Derecho nacional debe prever las vías de acción para exponer las alegaciones correspondientes ante los tribunales nacionales, a los que podrá pedirse que planteen una cuestión prejudicial al TJUE ([407]).

6. SUPERVISIÓN Y REVISIÓN DE LA PRESENTE DECISIÓN

(208) De conformidad con la jurisprudencia del TJUE ([408]) y tal como se reconoce en el artículo 45, apartado 4, del Reglamento (UE) 2016/679, la Comisión debe supervisar de manera continuada los acontecimientos en el tercer país después de la adopción de la decisión de adecuación, para evaluar si el tercer país todavía garantiza un nivel de protección equivalente en lo esencial. En cualquier caso, esa comprobación es obligada cuando la Comisión tenga indicios que generen una duda razonable en ese sentido.

(209) Por consiguiente, la Comisión debe hacer una supervisión continuada de la situación en los EE. UU. en lo que respecta al marco jurídico y a la práctica real relacionada con el tratamiento de los datos personales evaluada en la presente Decisión. Para facilitar este proceso, los poderes públicos estadounidenses deben informar puntualmente a la Comisión de cualquier cambio sustancial en el ordenamiento jurídico estadounidense que afecte al marco jurídico objeto de la presente Decisión, así como de cualquier evolución en las prácticas relacionadas con el tratamiento de los datos personales evaluadas en la presente Decisión, tanto en lo que se refiere al tratamiento de datos personales por las entidades certificadas estadounidenses como a las limitaciones y garantías aplicables al acceso a los datos personales por parte de las autoridades públicas.

(210) Además, a fin de que la Comisión pueda desempeñar eficazmente su función de supervisión, los Estados miembros deben informarle de toda medida pertinente tomada por las autoridades nacionales de protección de datos, en particular en lo que respecta a las consultas o las reclamaciones de los interesados de la UE en relación con la transferencia de datos personales desde la UE a las entidades certificadas estadounidenses. También debe informarse a la Comisión de todo indicio de que las medidas de los poderes públicos estadounidenses responsables de la seguridad nacional o de la prevención, la investigación, la detección o la persecución de las infracciones penales no garantizan el nivel de protección necesario.

([406]) Schrems, apartado 65.

([407]) Schrems I, apartado 65: «A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta».

([408]) Schrems, apartado 76.

(211) En aplicación del artículo 45, apartado 3, del Reglamento (UE) 2016/679 ([409]), la Comisión, tras la adopción de la presente Decisión, debe revisar periódicamente si las conclusiones relativas a la adecuación del nivel de protección garantizado por los EE. UU. en el Marco de Privacidad de Datos UE-EE. UU. siguen estando justificadas de hecho y de Derecho. Dado que, en particular, el Decreto Presidencial n.º 14086 y el Reglamento sobre el Tribunal de Recurso exigen el establecimiento de nuevas vías y órganos de impugnación y la aplicación de nuevas garantías, la presente Decisión debe ser objeto de una primera revisión en el plazo de un año a partir de su entrada en vigor, a fin de verificar si todos los elementos pertinentes se han implantado plenamente y si funcionan eficazmente en la práctica. Tras la primera revisión y en función de su resultado, la Comisión debe decidir, en estrecha consulta con el comité establecido en virtud del artículo 93, apartado 1, del Reglamento (UE) 2016/679 y con el Comité Europeo de Protección de Datos, la periodicidad de las próximas revisiones ([410]).

(212) Para llevar a cabo las revisiones, la Comisión debe reunirse con el Departamento de Comercio, la Comisión Federal de Comercio y el Departamento de Transporte, acompañados, si procede, por otros Departamentos y organismos que participen en la aplicación del Marco de Privacidad de Datos UE-EE. UU., así como, respecto de las cuestiones relativas al acceso de los poderes públicos a los datos, representantes del Departamento de Justicia, la Oficina del Director de Inteligencia Nacional (incluido el responsable de la protección de las libertades civiles), otros servicios de la Comunidad de Inteligencia, el Tribunal de Recurso en Materia de Protección de Datos y abogados especiales. La participación en esta reunión debe estar abierta a los representantes de los miembros del Comité Europeo de Protección de Datos.

(213) Las revisiones deben abarcar todos los aspectos del funcionamiento de la presente Decisión respecto del tratamiento de los datos personales en los EE. UU. y, en particular: la aplicación y ejecución de los principios en materia de privacidad, prestando especial atención a las garantías establecidas para las transferencias ulteriores; la evolución de la jurisprudencia pertinente; la eficacia del ejercicio de los derechos individuales; el control y la garantía del cumplimiento de los principios en materia de privacidad; las limitaciones y garantías con respecto al acceso por los poderes públicos, especialmente la ejecución y aplicación de las garantías introducidas por el Decreto Presidencial n.º 14086, también a través de directrices y procedimientos desarrollados por los servicios de inteligencia; la interacción entre el Decreto Presidencial n.º 14086 y el artículo 702 de la Ley de Vigilancia de Inteligencia Exterior y el Decreto Presidencial n.º 12333; y la eficacia de los mecanismos de supervisión y las vías procesales (incluido el funcionamiento de la nueva vía procesal establecida en virtud del Decreto Presidencial n.º 14086). En el contexto de estas revisiones, se prestará atención también a la cooperación entre las APD y las autoridades competentes estadounidenses, especialmente a la elaboración y desarrollo de directrices y otros instrumentos interpretativos para la aplicación de los principios en materia de privacidad, así como a otros aspectos del funcionamiento del Marco.

(214) Sobre la base de la revisión, la Comisión debe elaborar un informe público que presentará al Parlamento Europeo y al Consejo.

7. SUSPENSIÓN, DEROGACIÓN O MODIFICACIÓN DE LA PRESENTE DECISIÓN

(215) Cuando la información disponible, en particular la información resultante de la labor de supervisión respecto de la presente Decisión o proporcionada por las autoridades estadounidenses o de los Estados miembros, muestre que el nivel de protección conferido a los datos transferidos con arreglo a la presente Decisión puede que ya no sea adecuado, la Comisión debe informar sin demora de ello a las autoridades competentes estadounidenses y solicitar que se tomen medidas apropiadas dentro del plazo razonable que se fije.

(216) Si, al vencer dicho plazo, las autoridades estadounidenses competentes no han tomado dichas medidas o no han demostrado satisfactoriamente de otro modo que se sigue garantizando un nivel de protección adecuado a efectos de la presente Decisión, la Comisión debe iniciar el procedimiento a que se refiere el artículo 93, apartado 2, del Reglamento (UE) 2016/679 con el fin de suspender o derogar, total o parcialmente, la presente Decisión.

(217) La Comisión también puede iniciar ese procedimiento para modificar la presente Decisión, en particular con el fin de imponer condiciones adicionales a las transferencias de datos o con el fin de limitar la conclusión de adecuación solo a las transferencias de datos para las que se siga garantizando un nivel de protección adecuado.

([409]) De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, «[e]l acto de ejecución establecerá un mecanismo de revisión periódica, […] que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional».

([410]) El artículo 45, apartado 3, del Reglamento (UE) 2016/679 establece que debe procederse a una revisión periódica «al menos cada cuatro años». Véanse también las Referencias sobre adecuación, Comité Europeo de Protección de Datos, WP 254, rev. 01.

(218) En particular, la Comisión debe iniciar el procedimiento de suspensión o derogación en los supuestos siguientes:

a) si hay indicios de que las entidades que han recibido datos personales de la UE en virtud de la presente Decisión no cumplen los principios en materia de privacidad y de que los organismos de supervisión y garantía del cumplimiento competentes no han resuelto eficazmente dicho incumplimiento;

b) si hay indicios de que las autoridades estadounidenses no cumplen las condiciones y limitaciones aplicables al acceso por parte de los poderes públicos estadounidenses, a efectos policiales y de seguridad nacional, a los datos personales transferidos en el Marco de Privacidad de Datos UE-EE. UU.; o

c) si se incumple la obligación de tramitar eficazmente las reclamaciones de los interesados de UE, en particular cuando este incumplimiento procede de la Oficina del Director de Inteligencia Nacional (incluido el responsable de la protección de las libertades civiles) o el Tribunal de Recurso en Materia de Protección de Datos.

(219) La Comisión debe considerar asimismo la posibilidad de iniciar el procedimiento conducente a la modificación, suspensión o derogación de la presente Decisión si las autoridades estadounidenses competentes no proporcionan la información o las aclaraciones necesarias para la evaluación del nivel de protección de los datos personales transferidos desde la UE a los EE. UU. o en relación con el cumplimiento de la presente Decisión. A este respecto, la Comisión debe tener en cuenta en qué medida puede obtenerse la información pertinente de otras fuentes.

(220) Por razones imperiosas de urgencia debidamente justificadas (por ejemplo, si el Decreto Presidencial n.º 14086 o el Reglamento sobre el Tribunal de Recurso se modificase de modo que disminuyese el nivel de protección descrito en la presente Decisión o si la designación, por parte del secretario de Justicia, de la UE como organización internacional cualificada a efectos de la vía de reparación se revoca), la Comisión debe hacer uso de la competencia de adoptar, de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3, del Reglamento (UE) 2016/679, actos de ejecución inmediatamente aplicables que suspendan, deroguen o modifiquen la presente Decisión.

8. **CONSIDERACIONES FINALES**

(221) El Comité Europeo de Protección de Datos publicó su correspondiente dictamen ([411]), que se ha tenido en cuenta en la elaboración de la presente Decisión.

(222) El Parlamento Europeo aprobó la resolución sobre la adecuación de la protección conferida por el marco de privacidad de datos UE-EE. UU. ([412]).

(223) Las medidas previstas por la presente Decisión se ajustan al dictamen del Comité contemplado en el artículo 93, apartado 1, del Reglamento (UE) 2016/679.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

A efectos del artículo 45 del Reglamento (UE) 2016/679, los Estados Unidos garantizan un nivel de protección adecuado de los datos personales transferidos desde la Unión a las entidades estadounidenses que figuren en la lista del Marco de Privacidad de Datos, publicada y actualizada por el Departamento de Comercio de los Estados Unidos en virtud de la sección I, punto 3, del anexo I.

Artículo 2

Cuando las autoridades competentes de los Estados miembros, a fin de proteger a los particulares en lo que respecta al tratamiento de sus datos personales, ejerzan los poderes otorgados por el artículo 58 del Reglamento (UE) 2016/679 en relación con las transferencias de datos a que se refiere el artículo 1 de la presente Decisión, el Estado miembro en cuestión informará sin demora a la Comisión.

([411]) Dictamen 5/2023 del CEPD, de 28 de febrero de 2023, sobre el Proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación de la protección de los datos personales de acuerdo con el marco de privacidad de datos UE-EE. UU.

([412]) Resolución del Parlamento Europeo, de 11 de mayo de 2023, sobre la adecuación de la protección conferida por el marco de privacidad de datos UE-EE. UU. [2023/2501(RSP)].

Artículo 3

1. La Comisión realizará un seguimiento continuo de la aplicación del marco jurídico objeto de la presente Decisión, especialmente las condiciones en que se realizan las transferencias ulteriores, se ejercen los derechos individuales y tienen acceso los poderes públicos estadounidenses a los datos transferidos en el marco de la presente Decisión, a fin de evaluar si los Estados Unidos siguen garantizando un nivel de protección adecuado a efectos del artículo 1.

2. Los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en los que se tenga constancia de que algún organismo de los Estados Unidos con facultades legales para hacer cumplir los principios en materia de privacidad expuestos en el anexo I no haya dispuesto mecanismos eficaces de detección y control que permitan detectar y sancionar en la práctica las posibles vulneraciones de los principios en materia de privacidad.

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 responsables de velar por los intereses de seguridad nacional, policiales o públicos de otro tipo en el derecho de los particulares a la protección de sus datos personales transcienda de lo necesario y proporcional, o de que no exista una protección jurídica eficaz frente a tales injerencias.

4. Un año después de la fecha de notificación de la presente Decisión a los Estados miembros y posteriormente con la periodicidad que se decida en estrecha consulta con el comité establecido en virtud del artículo 93, apartado 1, del Reglamento (UE) 2016/679 y con el Comité Europeo de Protección de Datos, la Comisión evaluará la constatación a que se refiere el artículo 1, apartado 1, sobre la base de toda la información disponible, incluida la información resultante de la revisión realizada junto con las autoridades estadounidenses competentes.

5. En caso de que la Comisión tenga indicios de que ya no se garantiza un nivel de protección adecuado, la Comisión informará de ello a las autoridades estadounidenses competentes. Si es necesario, suspenderá, modificará o derogará la presente Decisión o limitará su ámbito de aplicación de conformidad con el artículo 45, apartado 5, del Reglamento (UE) 2016/679. La Comisión podrá asimismo adoptar tal decisión cuando la falta de cooperación de los Estados Unidos le impida determinar si estos siguen garantizando un nivel de protección adecuado.

Artículo 4

Los destinatarios de la presente Decisión son los Estados miembros.

Hecho en Bruselas, el 10 de julio de 2023.

Por la Comisión
Didier Reynders
Miembro de la Comisión

ANEXO I

PRINCIPIOS DEL MARCO DE PRIVACIDAD DE DATOS UE-EE. UU. APROBADOS POR EL DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS

I. CONSIDERACIONES GENERALES

1. Si bien es cierto que los Estados Unidos (en lo sucesivo, «EE. UU.») y la Unión Europea (en lo sucesivo, «UE») comparten el compromiso de fomentar la protección de la privacidad, el Estado de Derecho y el reconocimiento de la importancia de la circulación transatlántica de los datos para nuestros respectivos ciudadanos, economías y sociedades, los Estados Unidos adoptan un planteamiento de protección de la privacidad diferente del de la UE. Los EE. UU. utilizan un planteamiento sectorial que se basa en una mezcla de legislación, reglamentación y autorregulación. El Departamento de Comercio de los EE. UU. (en lo sucesivo, «el Departamento») aprueba los principios del Marco de Privacidad de Datos UE-EE. UU., así como los principios complementarios (denominados conjuntamente «los principios en materia de privacidad») y el anexo I de los principios en materia de privacidad (en lo sucesivo, «anexo I»), en virtud de su competencia legal para fomentar, promover y desarrollar el comercio internacional (título 15, artículo 1512, del Código de Estados Unidos). Los principios en materia de privacidad fueron elaborados con la colaboración de la Comisión Europea, del sector y de otras partes interesadas para facilitar el comercio y las actividades accesorias al comercio entre los EE. UU. y la UE. Los principios en materia de privacidad, que son un componente fundamental del Marco de Privacidad de Datos UE-EE. UU., proporcionan a las entidades estadounidenses un mecanismo fiable que ampara las transferencias de datos personales a los EE. UU. desde la UE, al mismo tiempo que garantizan que los interesados de la UE sigan gozando de las garantías y la protección efectivas exigidas por la normativa europea con respecto al tratamiento de sus datos personales cuando hayan sido transferidos a países no pertenecientes a la UE. Están destinados a ser utilizados exclusivamente por las entidades estadounidenses aptas que reciban datos personales procedentes de la UE con el propósito de permitir a estas entidades certificarse en el Marco de Privacidad de Datos UE-EE. UU., y por lo tanto, beneficiarse de la decisión de adecuación de la Comisión Europea ([1]). Los principios en materia de privacidad no afectan a la aplicación del Reglamento (UE) 2016/679 (en lo sucesivo, «RGPD») ([2]), que rige el tratamiento de los datos personales en los Estados miembros de la UE, y tampoco limitan las obligaciones en materia de privacidad que son de aplicación en virtud de la normativa estadounidense.

2. Para acogerse al Marco de Privacidad de Datos UE-EE. UU. al realizar transferencias de datos personales de la UE, las entidades deberán autocertificar su cumplimiento de los principios en materia de privacidad ante el Departamento (o su delegado). Aunque acogerse al Marco de Privacidad de Datos UE-EE. UU. es completamente voluntario, su cumplimiento efectivo es obligatorio: las entidades que se autocertifiquen ante el Departamento y declaren públicamente su compromiso de cumplir los principios en materia de privacidad deberán cumplirlos íntegramente. Para acogerse al Marco de Privacidad de Datos UE-EE. UU., las entidades deberán: a) someterse a las competencias de investigación y ejecución forzosa de la Comisión Federal de Comercio, el Departamento de Transporte u otro organismo legal que garantice efectivamente el cumplimiento de los principios en materia de privacidad (en el futuro podrán incluirse como anexo otros organismos legales estadounidenses reconocidos por la UE); b) declarar públicamente su compromiso de cumplir los principios en materia de privacidad; c) publicar sus directrices en materia de privacidad de conformidad con estos principios; y d) ponerlos en práctica íntegramente ([3]). La Comisión Federal de Comercio y el Departamento de Transporte podrán obligar a las entidades incumplidoras a cesar su incumplimiento —la primera, con arreglo al artículo 5 de la Ley de la Comisión Federal de Comercio (Federal Trade Commission Act), por el que se prohíben los actos desleales o engañosos en el comercio o que afectan al mismo [título 15, artículo 45, del Código de Estados Unidos (United States Code)], y el segundo, con arreglo al título 49, artículo 41712, del Código de Estados Unidos, por el que se prohíbe a los transportistas y los agentes de venta de billetes participar en prácticas desleales o engañosas en el transporte aéreo o en la comercialización de este tipo de transporte—; también se podrá imponer el cese del incumplimiento en virtud de otras leyes o reglamentos por los que se prohíban tales actos.

([1]) Dado que la Decisión de la Comisión relativa a la adecuación de la protección conferida en el Marco de Privacidad de Datos UE-EE. UU. es de aplicación a Islandia, Liechtenstein y Noruega, el Marco de Privacidad de Datos UE-EE. UU. abarcará tanto a la UE 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]) 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).

([3]) Los principios marco del Escudo de la privacidad UE-EE. UU. quedan sustituidos por los principios del Marco de Privacidad de Datos UE-EE. UU. Véase el principio complementario sobre la autocertificación.

3. El Departamento publicará y mantendrá actualizada la lista oficial de las entidades estadounidenses que se hayan autocertificado ante el Departamento y hayan declarado su compromiso de cumplir los principios en materia de privacidad (en lo sucesivo, «lista del Marco de Privacidad de Datos»). El Marco de Privacidad de Datos UE-EE. UU. despliega sus efectos para la entidad desde la fecha en que el Departamento la inscriba en la lista del Marco de Privacidad de Datos. El Departamento eliminará de la lista del Marco de Privacidad de Datos a las entidades que se den de baja voluntariamente del Marco de Privacidad de Datos UE-EE. UU. o que no hayan realizado la revalidación anual de su certificación ante el Departamento; dichas entidades deberán: a) bien seguir aplicando los principios en materia de privacidad a la información personal que reciban en el Marco de Privacidad de Datos UE-EE. UU. y declarar al Departamento con carácter anual su compromiso de hacerlo (durante el tiempo en que conserven dicha información); b) bien conferir una protección adecuada a la información por otros medios autorizados (por ejemplo, con un contrato que contenga todos los requisitos de las cláusulas contractuales tipo adoptadas por la Comisión Europea); c) bien devolver o suprimir la información. El Departamento también eliminará de la lista del Marco de Privacidad de Datos a las entidades que hayan incumplido sistemáticamente los principios en materia de privacidad; dichas entidades deberán devolver o suprimir la información personal que recibieron en el Marco de Privacidad de Datos UE-EE. UU. La eliminación de una entidad de la lista del Marco de Privacidad de Datos significa que ya no puede seguir beneficiándose de la decisión de adecuación de la Comisión Europea para recibir información personal procedente de la UE.

4. El Departamento también publicará y mantendrá actualizado el registro oficial de las entidades estadounidenses que en algún momento se hayan autocertificado ante el Departamento, pero que ya no forman parte de la lista del Marco de Privacidad de Datos. El Departamento advertirá claramente: que estas entidades no participan en el Marco de Privacidad de Datos UE-EE. UU.; que la eliminación de la lista del Marco de Privacidad de Datos significa que dichas entidades no pueden afirmar que cumplen el Marco de Privacidad de Datos UE-EE. UU. y deben evitar cualquier declaración o práctica engañosa que sugiera su participación en dicho Marco; y que estas entidades ya no tienen derecho a beneficiarse de la decisión de adecuación de la Comisión Europea para recibir información personal procedente de la UE. La entidad que continúe afirmando su participación en el Marco de Privacidad de Datos UE-EE. UU. o que lleve a pensar por otros medios que participa en dicho Marco después de haber sido eliminada de la lista del Marco de Privacidad de Datos podrá ser objeto de medidas coercitivas de la Comisión Federal de Comercio, del Departamento de Transporte o de otros organismos de garantía del cumplimiento.

5. El cumplimiento de los principios en materia de privacidad podrá limitarse: a) en la medida necesaria para cumplir una resolución judicial o satisfacer necesidades de interés público, de seguridad nacional o policiales, incluso cuando la legislación o los reglamentos del Ejecutivo creen obligaciones contradictorias; b) por medio de una ley, una resolución judicial o un reglamento del Ejecutivo que disponga autorizaciones expresas siempre que, al acogerse a dicha autorización, la entidad pueda demostrar que su incumplimiento de los principios en materia de privacidad se limita a lo necesario para atender los intereses legítimos esenciales contemplados por dicha autorización; o c) si el RGPD tiene por efecto permitir excepciones, en las condiciones establecidas en el mismo, siempre que dichas excepciones o exenciones sean de aplicación en supuestos comparables. En este contexto, forman parte de las garantías contempladas en el Derecho estadounidense para proteger la privacidad y las libertades civiles las exigidas por el Decreto Presidencial n.º 14086 ([4]) en las condiciones establecidas en el mismo (en particular, sus requisitos de necesidad y proporcionalidad). A fin de ser coherentes con el objetivo de mejorar la protección de la privacidad, las entidades deberán esforzarse en aplicar los principios en materia de privacidad de manera completa y transparente, lo que incluye indicar en sus directrices en materia privacidad cuándo se aplicarán las excepciones a los principios en materia de privacidad contempladas en la letra b). Por esta misma razón, cuando exista la opción en virtud de los principios en materia de privacidad y/o del Derecho estadounidense, se espera que las entidades opten por el mayor nivel de protección posible.

6. Las entidades están obligadas a aplicar los principios en materia de privacidad a todos los datos personales transferidos en el Marco de Privacidad de Datos UE-EE. UU. una vez se hayan acogido al mismo. La entidad que decida extender los beneficios del Marco de Privacidad de Datos UE-EE. UU. también a la información personal de recursos humanos transferida desde la UE para usarla en el marco de la relación laboral deberá indicarlo al Departamento cuando se autocertifique y atenerse a las obligaciones que impone el principio complementario sobre la autocertificación.

([4]) Decreto Presidencial de 7 de octubre de 2022, titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos» (Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities') (en lo sucesivo, «Decreto Presidencial n.º 14086»).

7. El Derecho estadounidense se aplicará a las cuestiones relativas a la interpretación y el cumplimiento de los principios en materia de privacidad y las directrices en materia privacidad de las entidades que participen en el Marco de Privacidad de Datos UE-EE. UU., excepto si estas se han comprometido a cooperar con las autoridades de protección de datos de la UE (en lo sucesivo, «APD»). Salvo disposición en contrario, serán de aplicación todas las disposiciones de los principios en materia de privacidad cuando sea pertinente.

8. Definiciones:

   a. por «datos personales» e «información personal» se entienden los datos sobre un particular identificado o identificable a los que es de aplicación el RGPD, que los recibe de la UE una entidad estadounidense y que quedan registrados de alguna forma;

   b. por «tratamiento» de los datos personales se entiende cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación, difusión y supresión o destrucción;

   c. por «responsable del tratamiento de datos» o «responsable» se entiende una persona física o jurídica que, sola o junto con otros, determina las finalidades y medios del tratamiento de datos personales.

9. La fecha de entrada en vigor de los principios en materia de privacidad y de su anexo I es la fecha de entrada en vigor de la decisión de adecuación de la Comisión Europea.

II. **PRINCIPIOS**

1. **NOTIFICACIÓN**

a. Las entidades deberán informar a los particulares sobre:

   i. su participación en el Marco de Privacidad de Datos UE-EE. UU. y proporcionar un enlace a la lista del Marco de Privacidad de Datos o la dirección web de la misma;

   ii. los tipos de datos personales recogidos y, cuando proceda, las sucursales o sociedades subsidiarias estadounidenses de la entidad que también cumplen los principios en materia de privacidad;

   iii. su compromiso de someter a los principios en materia de privacidad todos los datos personales recibidos de la UE en el Marco de Privacidad de Datos UE-EE. UU.;

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

   v. la forma de ponerse en contacto con ellas con motivo de consultas o reclamaciones, incluido cualquier establecimiento en la UE que pueda responder a dichas consultas o reclamaciones;

   vi. el tipo o la identidad de los terceros a los que se comunica la información personal y los fines de tal comunicación;

   vii. el derecho de los particulares de acceso a sus datos personales;

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

   ix. el organismo independiente de resolución de controversias designado para tramitar las reclamaciones y ofrecer una vía de impugnación adecuada y gratuita al particular, y si se trata de: 1) el panel establecido por las APD, 2) un organismo alternativo de resolución de controversias con sede en la UE o 3) un organismo alternativo de resolución de controversias con sede en los EE. UU.;

   x. el hecho de que están sujetas a las competencias de investigación y ejecución forzosa de la Comisión Federal de Comercio, el Departamento de Transporte u otro organismo legal estadounidense autorizado;

   xi. la posibilidad, en determinadas condiciones, de que el particular solicite la incoación de un proceso arbitral vinculante ([5]);

   xii. la obligación de comunicar información personal en respuesta a solicitudes lícitas de los poderes públicos, en particular para responder a necesidades de seguridad nacional o policiales; y

   xiii. su responsabilidad respecto de las transferencias ulteriores a terceros.

([5]) Véase, en concreto, la letra c del principio de impugnación, ejecución forzosa y responsabilidad.

b. La notificación deberá hacerse en un lenguaje claro y evidente cuando se solicite por primera vez a los particulares que proporcionen a la entidad información personal o tan pronto como sea posible después, pero, en cualquier caso, antes de que la entidad utilice dicha información para una finalidad distinta de aquella para la que inicialmente la recogió o trató la entidad que la transfiere o antes de que entidad la comunique por primera vez a un tercero.

2. **OPCIÓN**

a. Las entidades deberán ofrecer a los particulares la posibilidad de oponerse a que su información personal i) se comunique a un tercero o ii) se utilice para una finalidad sustancialmente distinta de la finalidad para la que fueron recogidos inicialmente o que autorizó posteriormente el particular. Se deberán ofrecer a los particulares mecanismos claros, bien visibles e inmediatamente utilizables para que ejerzan su derecho de opción.

b. No obstante lo establecido en la letra anterior, no es necesario ofrecer la posibilidad anterior cuando la información se comunique a un tercero que actúe como agente realizando tareas por cuenta de la entidad y siguiendo sus instrucciones. Sin embargo, la entidad deberá celebrar siempre un contrato a tal efecto con el agente.

c. Si se trata de información delicada, como la información que indique el estado de salud, el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical o la información sobre la vida sexual del particular, las entidades deberán obtener el consentimiento expreso del particular si dicha información i) va a comunicarse a un tercero o ii) va a utilizarse para una finalidad distinta de la finalidad para la que fue recogida inicialmente o que autorizó posteriormente de forma expresa el particular. En cualquier caso, las entidades deberán tratar como delicada toda información personal recibida de un tercero cuando dicho tercero la considere y trate como información delicada.

3. **RESPONSABILIDAD PROACTIVA POR LAS TRANSFERENCIAS ULTERIORES**

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 celebrar un contrato con el tercero responsable del tratamiento por el que se estipule que tales datos solo se podrán tratar para finalidades limitadas y específicas que sean compatibles con el consentimiento proporcionado por el particular, y que el destinatario garantizará el mismo nivel de protección que los principios en materia de privacidad y comunicará a la entidad si ya no puede cumplir esta obligación. En el contrato se establecerá que, en caso de que se llegue a esta constatación, el tercero responsable del tratamiento dejará de tratar los datos o tomará otras medidas razonables y adecuadas para reparar la situación.

b. Para transferir datos personales a un tercero que actúe como agente, las entidades deberán: i) transferir dichos datos única y exclusivamente para finalidades limitadas y específicas; ii) cerciorarse de que el agente está obligado a garantizar como mínimo el mismo nivel de protección de la privacidad que el exigido por los principios en materia de privacidad; iii) tomar medidas razonables y apropiadas para garantizar el tratamiento efectivo por parte del agente de la información personal transferida con arreglo a las obligaciones que imponen a la entidad los principios en materia de privacidad; iv) exigir al agente que notifique a la entidad si ya no puede cumplir la obligación de garantizar el mismo nivel de protección que el exigido por los principios en materia de privacidad; v) previa recepción de notificación, en particular en el supuesto del inciso iv), tomar las medidas razonables y apropiadas para detener el tratamiento no autorizado y reparar la situación; y vi) aportar, a instancias del Departamento, un resumen o una copia representativa de las cláusulas en materia de privacidad pertinentes de su contrato con ese agente.

4. **SEGURIDAD**

a. Las entidades que creen, tengan, utilicen o difundan información personal deberán tomar medidas razonables y apropiadas para evitar su pérdida, su mal uso y consulta no autorizada, su comunicación, 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 en materia de privacidad, la información personal deberá limitarse a la información pertinente a efectos del tratamiento ([6]). Las entidades no podrán tratar la información personal de manera incompatible con la finalidad para la que fue recogida inicialmente o que autorizó posteriormente el particular. En la medida necesaria para lograr dicha finalidad, las entidades tomarán medidas razonables para que los datos personales sean fiables en relación con el uso previsto, exactos y actuales y estén completos. Las entidades deberán respetar los principios en materia de privacidad durante el tiempo que conserven dicha información.

b. La información podrá conservarse en una forma que identifique o haga identificable ([7]) al particular únicamente mientras esta conservación contribuya a alcanzar la finalidad del tratamiento con arreglo a lo dispuesto en el punto 5, letra a. Esta obligación no impide a las entidades tratar información personal por períodos más largos, por el tiempo y en la medida en que dicho tratamiento contribuya razonablemente a las finalidades siguientes, a saber, archivamiento en interés público, periodismo, literatura y arte, investigación científica o histórica y análisis estadístico. En estos casos, el tratamiento estará sujeto a los demás principios y disposiciones del Marco de Privacidad de Datos UE-EE. UU. Las entidades deberán tomar 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 resulta inexacta o ha sido tratada infringiendo los principios en materia de privacidad, excepto en dos casos: cuando el trabajo o el gasto de conceder el acceso sean desproporcionados en relación con los riesgos para la privacidad del particular dadas las circunstancias del caso o cuando con ello se vulneren los derechos de otras personas.

7. **IMPUGNACIÓN, EJECUCIÓN FORZOSA Y RESPONSABILIDAD**

a. Para que se pueda proteger eficazmente la privacidad debe haber sólidos mecanismos para exigir el cumplimiento de los principios en materia de privacidad, vías de impugnación para los particulares afectados por el incumplimiento de dichos principios y sanciones para la entidad incumplidora. Como mínimo, tales mecanismos deberán incluir:

i. órganos independientes de impugnación y vías procesales para que las reclamaciones y las controversias de los particulares puedan ser investigadas y resueltas sin demora y sin coste alguno para estos y de acuerdo con los principios en materia de privacidad, y para que se conceda una indemnización por daños y perjuicios cuando así lo establezcan el Derecho aplicable o iniciativas del sector privado;

ii. procedimientos de seguimiento para comprobar la veracidad de las afirmaciones y declaraciones de las entidades sobre sus prácticas en materia de privacidad 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 las entidades que se hayan comprometido a respetar los principios en materia de privacidad de reparar los problemas derivados de su incumplimiento y las sanciones correspondientes para ellas, que serán lo suficientemente severas para garantizar su cumplimiento.

b. Las entidades y los órganos independientes de impugnación de estas responderán rápidamente a las consultas y solicitudes de información del Departamento relacionadas con el Marco de Privacidad de Datos UE-EE. UU. Todas las entidades deberán responder sin demora a las reclamaciones relacionadas con el cumplimiento de los principios en materia de privacidad remitidas por las autoridades de los Estados miembros de la UE a través del Departamento. Las entidades que hayan decidido cooperar con las APD, en particular las entidades que tratan datos de recursos humanos, deberán responder directamente a estas autoridades en relación con la investigación y la resolución de las reclamaciones.

([6]) Dependiendo de las circunstancias, algunos ejemplos de finalidades del tratamiento compatibles pueden ser aquellas que contribuyan razonablemente a las relaciones con los clientes, el cumplimiento y los aspectos jurídicos, las auditorías, la seguridad y la prevención del fraude, la conservación o defensa de los derechos de la entidad, así como otras finalidades que se ajusten a las expectativas de una persona razonable dadas las circunstancias de la recogida de los datos.

([7]) En este contexto, se considera «identificable» al particular si, habida cuenta de los medios de identificación que es razonablemente probable que se utilicen (valorando, entre otras cosas, el coste y el tiempo necesarios para la identificación y la tecnología disponible en el momento del tratamiento) y de la forma en que se conserven los datos, el particular puede ser razonablemente identificado por la entidad o por un tercero que tenga acceso a los datos.

c. Las entidades están obligadas a arbitrar las reclamaciones y atenerse a las condiciones establecidas en el anexo I siempre que el particular haya solicitado la incoación de un proceso arbitral vinculante mediante la notificación a la entidad en cuestión de conformidad con los procedimientos y condiciones establecidos en el anexo I.

d. En el contexto de las transferencias ulteriores, las entidades participantes asumen la responsabilidad del tratamiento de la información personal que reciben en dicho Marco y posteriormente transfieren a un tercero que actúe como agente por su cuenta. Las entidades participantes serán responsables a efectos de los principios en materia de privacidad si su agente trata dicha información personal infringiendo los mismos, salvo que la entidad demuestre que no es responsable del suceso que ha provocado los daños y perjuicios.

e. Cuando la entidad sea objeto de una resolución judicial por incumplimiento o de una resolución por incumplimiento dictada por un organismo legal estadounidense (por ejemplo, la Comisión Federal de Comercio o el Departamento de Transporte) de los enumerados en los principios en materia de privacidad o en un futuro anexo de dichos principios, dicha entidad publicará las secciones pertinentes relacionadas con el Marco de Privacidad de Datos UE-EE. UU. de cualquier informe de cumplimiento o evaluación presentado al órgano jurisdiccional o al organismo legal estadounidense en la medida en que sea compatible con los requisitos de confidencialidad. El Departamento ha nombrado un punto de contacto específico para las APD en caso de problemas de cumplimiento por parte de las entidades participantes. La Comisión Federal de Comercio y el Departamento de Transporte darán prioridad a las reclamaciones remitidas por el Departamento y las autoridades de los Estados miembros de la UE relativas al incumplimiento de los principios e intercambiarán sin demora información relativa a las reclamaciones con las autoridades públicas que las hayan remitido, de conformidad con las restricciones de confidencialidad existentes.

III. PRINCIPIOS COMPLEMENTARIOS

1. Datos delicados

a. Las entidades no están obligadas a obtener el consentimiento expreso del particular por lo que respecta a los datos delicados en los casos en que el tratamiento:

i. sea de interés vital para el interesado u otra persona;

ii. sea necesario para un proceso judicial;

iii. sea necesario para proporcionar cuidados médicos o establecer un diagnóstico;

iv. se lleve a cabo en el marco de las actividades legítimas de una fundación, asociación o cualquier otra persona jurídica sin ánimo lucrativo que persiga un objetivo político, filosófico, religioso o sindical, a condición de que el tratamiento se refiera exclusivamente a los miembros de la persona jurídica o a las personas que están en contacto habitual con ella en relación con sus fines y a condición de que los datos no se comuniquen a terceros sin el consentimiento de los interesados;

v. sea necesario para cumplir las obligaciones de la entidad de Derecho laboral; o

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

2. Excepciones derivadas de la libertad de prensa

a. Habida cuenta del amparo que la Constitución de los EE. UU. brinda a la libertad de prensa, cuando el derecho a la libertad de prensa consagrado en la primera enmienda de la Constitución de los EE. UU. entre en conflicto con los intereses de la protección de privacidad, la primera enmienda deberá regir el equilibrio de tales intereses en lo tocante a las actividades de los particulares o entidades estadounidenses.

b. La información personal que se recoge para su publicación, retransmisión u otras formas de comunicación pública de material periodístico, aunque no se utilice, y la información contenida en material de archivo publicado previamente no están sujetas a los requisitos de los principios en materia de privacidad.

3. Responsabilidad subsidiaria

a. Las empresas de servicios de internet, los operadores de telecomunicaciones y otras entidades no son responsables a efectos de los principios en materia de privacidad cuando se limiten a transmitir, encaminar, intercambiar o almacenar temporalmente información por cuenta de otra entidad. El Marco de Privacidad de Datos UE-EE. UU. no crea una responsabilidad subsidiaria. Si la 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. **Ejercicio de la diligencia debida y realización de auditorías**

a. Las actividades de los bancos de inversión y las empresas de auditoría pueden conllevar el tratamiento de datos personales sin el consentimiento o el conocimiento del particular. Los principios de notificación, opción y acceso lo permiten en las circunstancias descritas a continuación.

b. Las sociedades cotizadas (*public stock corporations*) y las sociedades con concentración de los títulos de participación (*closely held companies*), incluidas las entidades participantes, están generalmente sujetas a auditorías. La eficacia de dichas auditorías, especialmente las que examinan posibles irregularidades, puede verse amenazada si se comunican sus hallazgos antes de tiempo. De igual modo, las entidades participantes involucradas en una posible fusión o absorción deberán realizar o someterse a una revisión de la «diligencia debida». Con frecuencia esto comportará la recogida y el tratamiento de datos personales tales como información sobre los altos directivos y otro personal clave. La comunicación prematura de cierta información podría frustrar la operación o incluso infringir la normativa del mercado de valores aplicable. Los bancos de inversión, los abogados especializados en diligencia debida o las empresas de auditoría pueden tratar información sin conocimiento del particular solo en la medida y durante el período necesarios para satisfacer las exigencias legales o de interés público, así como en otras circunstancias en que la aplicación de los principios en materia de privacidad perjudicaría los intereses legítimos de la entidad. Entre estos se cuenta la supervisión, llevada a cabo por los bancos de inversión o las empresas de auditoría, del cumplimiento por la entidad de sus obligaciones jurídicas y las actividades legítimas de contabilidad, así como de la necesidad de secreto relacionada con posibles adquisiciones, fusiones, empresas en participación u otras operaciones similares.

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

a. Las entidades deberán cooperar con las APD tal como se describe a continuación. En virtud del Marco de Privacidad de Datos UE-EE. UU., las entidades estadounidenses que reciban datos personales procedentes de la UE deberán utilizar mecanismos eficaces para dar cumplimiento a los principios en materia de privacidad. Más concretamente y tal como se establece en el principio de impugnación, ejecución forzosa y responsabilidad, las entidades participantes deberán establecer: a.i) vías de impugnación para los particulares a los que se refieran los datos; a.ii) procedimientos de seguimiento para comprobar la veracidad de las afirmaciones y declaraciones que han realizado sobre sus prácticas en materia de privacidad; y a.iii) la obligación de reparar por los problemas derivados del incumplimiento de los principios en materia de privacidad y las sanciones correspondientes para las entidades. Las entidades podrán satisfacer la letra a, incisos i y iii, del principio de impugnación, ejecución forzosa y responsabilidad si se cumplen las obligaciones aquí establecidas de cooperación con las APD.

b. Las entidades se comprometen a cooperar con las APD mediante la declaración adjunta al expediente de autocertificación presentado al Departamento a efectos del Marco de Privacidad de Datos UE-EE. UU. (véase el principio complementario sobre la autocertificación) de que:

i. cumplirán las obligaciones de la letra a, incisos i y iii, del principio de impugnación, ejecución forzosa y responsabilidad comprometiéndose a cooperar con las APD;

ii. cooperarán con las APD en la investigación y resolución de las reclamaciones que se formulen con arreglo a los principios en materia de privacidad; y

iii. cumplirán el dictamen de las APD cuando estas determinen que la entidad debe tomar medidas específicas para cumplir los principios en materia de privacidad, en particular medidas reparatorias o indemnizatorias en beneficio de los afectados por el incumplimiento de dichos principios, y comunicarán por escrito a las APD la toma de dichas medidas.

c. Funcionamiento de los paneles de las APD

i. Las APD cooperarán con información y dictámenes de la manera siguiente:

1. Los dictámenes de las APD los emitirá un panel informal de APD de ámbito europeo, lo que permitirá, entre otras cosas, que haya una planteamiento armonizado y coherente.

2. El panel emitirá dictámenes para las entidades estadounidenses de que se trate en relación con reclamaciones no resueltas de particulares referidas al tratamiento de información personal transferida desde la UE en el Marco de Privacidad de Datos UE-EE. UU. Estos dictámenes tendrán como finalidad la correcta aplicación de los principios en materia de privacidad y contemplarán todas las medidas de reparación para los afectados que las APD consideren adecuadas.

3. El panel emitirá dictamen respecto de las reclamaciones que le remitan las entidades de que se trate y de las reclamaciones que reciba directamente de particulares contra entidades que se hayan comprometido a cooperar con las APD en el Marco de Privacidad de Datos UE-EE. UU.; simultáneamente, animará y, en su caso, ayudará a los particulares en un primer momento a hacer uso de las vías internas de resolución de las reclamaciones que ofrezcan las entidades.

4. Solo se emitirá el dictamen una vez que las partes enfrentadas hayan dispuesto de tiempo razonable para formular sus observaciones y aportar las pruebas que deseen. El panel tratará de pronunciarse tan pronto como lo permita esta garantía procesal y, de modo general, en un plazo de sesenta días tras recibir la reclamación o producirse 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 dictamen 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 las controversias deberán comprometerse a cumplir el dictamen de las APD. Si la entidad no lo cumple transcurridos veinticinco días desde que se recibió el dictamen y no ha dado una explicación satisfactoria sobre el retraso, el panel notificará su intención ya sea de remitir la reclamación a la Comisión Federal de Comercio, el Departamento de Transporte u otro organismo federal o estatal estadounidense con competencias legales de ejecución forzosa en casos de fraude o engaño, ya sea de certificar que se ha vulnerado gravemente el acuerdo de cooperación y declarar su nulidad En este último caso, el panel informará al Departamento para que proceda a la debida corrección de la lista del Marco de Privacidad de Datos. Todo incumplimiento del compromiso de cooperar con las APD, así como de los principios en materia de privacidad, podrá desencadenar un procedimiento por práctica engañosa con arreglo al artículo 5 de la Ley de la Comisión Federal de Comercio (título 15, artículo 45, del Código de Estados Unidos), al título 49, artículo 41712, del Código de Estados Unidos o a otra norma equivalente de rango legal.

d. Las entidades que quieran que el régimen del Marco de Privacidad de Datos UE-EE. UU. se extienda a los datos de recursos humanos transferidos desde la UE en el marco de la relación laboral deberán comprometerse a cooperar con las APD en relación con estos datos (véanse los principios complementarios sobre los datos de recursos humanos).

e. Las entidades que se acojan a esta opción deberán pagar una tasa anual, concebida para sufragar los gastos de funcionamiento del panel. Además, se les podrá pedir que abonen los gastos de traducción necesarios derivados del examen por parte del panel de las reclamaciones remitidas o recibidas contra ellas. El Departamento determinará el importe de la tasa previa consulta a la Comisión Europea. El cobro de la tasa podrá correr a cargo de un tercero nombrado por el Departamento para actuar como depositario de los fondos recaudados con este fin. El Departamento cooperará estrechamente con la Comisión Europea y las APD para establecer procedimientos adecuados para la distribución de los fondos recaudados con la tasa, así como otros aspectos procedimentales y administrativos del panel. El Departamento y la Comisión Europea podrán acordar modificar la frecuencia con la que se exigirá el pago de la tasa.

6. **Autocertificación**

a. El Marco de Privacidad de Datos UE-EE. UU. despliega sus efectos para la entidad desde la fecha en que el Departamento la inscriba en la lista del Marco de Privacidad de Datos. El Departamento solo inscribirá en la lista del Marco de Privacidad de Datos a aquellas entidades respecto de las que haya comprobado que el expediente inicial de autocertificación presentado está completo, y eliminará de dicha lista a las entidades que se den de baja voluntariamente, no realicen la revalidación anual de su certificación o incumplan sistemáticamente los principios en materia de privacidad (véase el principio complementario sobre la resolución de controversias y la ejecución forzosa).

b. Para autocertificarse inicialmente o revalidar posteriormente la certificación a efectos del Marco de Privacidad de Datos UE-EE. UU., las entidades deberán, en cada ocasión y por medio de un representante de la entidad que se autocertifique o que revalide la certificación (según proceda) su cumplimiento de los principios en materia de privacidad, presentar al Departamento un expediente que contenga al menos la información siguiente ([8]):

([8]) El expediente deberá presentarlo, a través del sitio web del Departamento dedicado al Marco de Privacidad de Datos, una persona perteneciente a la entidad y autorizada para actuar por cuenta de la entidad y de cualquiera de sus filiales amparadas en relación con su cumplimiento de los principios en materia de privacidad.

i. el nombre de la entidad estadounidense que se autocertifica o revalida la certificación, así como el nombre de las filiales o sucursales estadounidenses que también cumplan los citados principios y que la entidad quiera que queden amparadas por el Marco;

ii. una descripción de las actividades de la entidad en lo relativo a la información personal que se vaya a recibir procedente de la UE en el Marco de Privacidad de Datos UE-EE. UU.;

iii. una descripción de las directrices en materia privacidad pertinentes de la entidad respecto de dicha información personal, con indicación de:

1. si la entidad tiene un sitio web público, la dirección del sitio web en el que aparecen las directrices en materia privacidad, o, si la entidad no tiene un sitio web público, dónde se pueden consultar estas; y

2. la fecha en que comenzaron a aplicarse;

iv. una oficina de contacto de la entidad para la tramitación de las reclamaciones, las solicitudes de acceso y cualquier otra cuestión relacionada con los principios en materia de privacidad ([9]), en particular:

1. nombres y apellidos, cargos (según proceda), direcciones de correo electrónico y números de teléfono de las personas correspondientes o de las oficinas de contacto correspondientes de la entidad; y

2. la dirección postal pertinente de la entidad en los EE. UU.;

v. el organismo legal pertinente que tenga competencia para conocer de las reclamaciones contra la entidad por posibles prácticas desleales o engañosas y por el incumplimiento de las leyes o reglamentos en materia de privacidad (y que figurarán en los principios en materia de privacidad o en un futuro anexo de dichos principios);

vi. el nombre de cualquier programa de privacidad en el que la entidad participe;

vii. el método de verificación (es decir, autoevaluación o verificación externa del cumplimiento, incluido el tercero que las realice) ([10]); y

viii. los órganos independientes de impugnación y las vías procesales disponibles para investigar las reclamaciones no resueltas relacionadas con los principios en materia de privacidad ([11]).

c. Cuando la entidad quiera que el régimen del Marco de Privacidad de Datos UE-EE. UU. se extienda a la información de recursos humanos transferida desde la UE para usarla en el marco de la relación laboral, podrá hacerlo cuando un organismo legal de los enumerados en los principios en materia de privacidad o en un futuro anexo de dichos principios tenga competencia para conocer de las reclamaciones contra la entidad derivadas del tratamiento de información de recursos humanos. Asimismo, la entidad deberá indicarlo en el expediente inicial de autocertificación, así como en los expedientes posteriores de revalidación, y expresar su compromiso de cooperar con las autoridades de la UE pertinentes de conformidad con los principios complementarios sobre los datos de recursos humanos y la función de las APD (según proceda), y que cumplirá los dictámenes de dichas autoridades. La entidad también deberá presentar al Departamento una copia de sus directrices en materia privacidad de recursos humanos y proporcionar información sobre el lugar en el que los empleados afectados pueden consultarlas.

([9]) La persona de contacto principal de la entidad o el representante de la entidad no pueden ser personal externo (por ejemplo, un asesor o un consultor externos).

([10]) Véase el principio complementario sobre la verificación.

([11]) Véase el principio complementario sobre la resolución de controversias y la ejecución forzosa.

d. El Departamento establecerá y publicará la lista del Marco de Privacidad de Datos, en la que figurarán las entidades que hayan presentado un expediente de autocertificación inicial completo, y actualizará dicha lista en función de los expedientes de revalidación anual de la certificación completos que se presenten, así como de las notificaciones recibidas con arreglo al principio complementario sobre la resolución de controversias y la ejecución forzosa. La revalidación de la certificación deberá realizarse con carácter anual, como mínimo; de lo contrario, la entidad será eliminada de la lista del Marco de Privacidad de Datos y no podrá seguir disfrutando del régimen del Marco de Privacidad de Datos UE-EE. UU. Todas las entidades inscritas en la lista del Marco de Privacidad de Datos por el Departamento deberán contar con directrices en materia privacidad pertinentes que cumplan el principio de notificación y declarar en dichas directrices que cumplen los principios en materia de privacidad ([12]). Si están disponibles en internet, las directrices en materia privacidad de la entidad deberán incluir un enlace al sitio web del Departamento sobre el Marco de Privacidad de Datos y otro enlace al sitio web o al formulario del órgano independiente de impugnación con competencia para investigar las reclamaciones no resueltas relativas a los principios en materia de privacidad.

e. Los principios en materia de privacidad son de aplicación inmediatamente después de la autocertificación. Las entidades participantes que se hubieran autocertificado con arreglo a los principios marco del Escudo de la privacidad UE-EE. UU. tendrán que actualizar sus directrices en materia privacidad para hacer referencia, en su lugar, a los «principios del Marco de Privacidad de Datos UE-EE. UU.». Dichas entidades deberán introducir esta referencia lo antes posible y, en cualquier caso, a más tardar tres meses después de la fecha de entrada en vigor de los principios del Marco de Privacidad de Datos UE-EE. UU.

f. Las entidades deberán someter a los principios en materia de privacidad todos los datos personales recibidos de la UE en el Marco de Privacidad de Datos UE-EE. UU. El compromiso de cumplir los principios en materia de privacidad no está limitado en el tiempo a los datos personales recibidos durante el período en el que la entidad esté acogida al Marco de Privacidad de Datos UE-EE. UU.; dicho compromiso significa que la entidad seguirá aplicando los principios en materia de privacidad a dichos datos mientras los almacene o siempre que los utilice o comunique, aunque posteriormente se dé de baja en el Marco de Privacidad de Datos UE-EE. UU. por algún motivo. Toda entidad que pretenda darse de baja en el Marco de Privacidad de Datos UE-EE. UU. deberá notificarlo previamente al Departamento. Tal notificación también deberá indicar qué hará la entidad con los datos personales que haya recibido en el Marco de Privacidad de Datos UE-EE. UU. (es decir, conservar, devolver o suprimir los datos y, si conservara los datos, los medios autorizados por los que garantizará la protección de los datos). La entidad que se dé de baja en el Marco de Privacidad de Datos UE-EE. UU., pero quiera conservar estos datos, deberá, bien declarar al Departamento con carácter anual su compromiso de seguir aplicando los principios en materia de privacidad a los datos, bien conferir una protección «adecuada» a la información por otros medios autorizados (por ejemplo, con un contrato que contenga todos los requisitos de las cláusulas contractuales tipo adoptadas por la Comisión Europea); de lo contrario, la entidad deberá devolver o suprimir la información ([13]). La entidad que se dé de baja en el Marco de Privacidad de Datos UE-EE. UU. deberá eliminar de las directrices en materia privacidad pertinentes toda referencia al Marco que insinúe que la entidad continúa participando en el Marco y que está amparada por este.

([12]) Las entidades que se autocertifiquen por primera vez no podrán afirmar que participan en el Marco de Privacidad de Datos UE-EE. UU. en sus directrices en materia privacidad más recientes hasta que el Departamento les notifique que pueden hacerlo. La entidad deberá presentar al Departamento un proyecto de directrices en materia privacidad, que deberá ser coherente con los principios en materia de privacidad, cuando presente su expediente de autocertificación inicial. Una vez que el Departamento haya determinado que el expediente inicial de autocertificación que ha presentado la entidad está completo, el Departamento notificará a la entidad que debe ultimar sus directrices en materia privacidad (por ejemplo, publicar, si procede) coherente con el Marco de Privacidad de Datos UE-EE. UU. La entidad deberá notificar al Departamento la ultimación de las directrices en materia privacidad pertinentes tan pronto la lleve a cabo; solo entonces el Departamento inscribirá a la entidad en la lista del Marco de Privacidad de Datos.

([13]) Si, al darse de baja, la entidad opta por conservar los datos personales que haya recibido en el Marco de Privacidad de Datos UE-EE. UU. y declara al Departamento con carácter anual que va a seguir aplicando los principios en materia de privacidad a dichos datos, la entidad deberá probar al Departamento con carácter anual desde su baja (es decir, hasta que la entidad confiera una protección «adecuada» a tales datos por otros medios autorizados o devuelva o suprima todos esos datos y lo notifique al Departamento) lo que ha hecho con esos datos personales, lo que hará con los datos personales que siga conservando y quién será el punto de contacto permanente para las preguntas relacionadas con los principios en materia de privacidad.

g. La entidad que deje de existir como persona jurídica independiente a resultas de un cambio sustancial de su situación, como una fusión, una absorción, la bancarrota o la disolución, deberá notificarlo previamente al Departamento. La notificación también deberá indicar si la entidad resultante del cambio sustancial i) seguirá participando en el Marco de Privacidad de Datos UE-EE. UU. con una autocertificación existente, ii) hará una nueva autocertificación a efectos del Marco (por ejemplo, cuando la nueva entidad o la entidad superviviente no disponga de una autocertificación con la que participar en el Marco) o iii) establecerá otras garantías, como un acuerdo escrito por el que se asegure la aplicación continuada de los principios en materia de privacidad a los datos personales que la entidad haya recibido en el Marco de Privacidad de Datos UE-EE. UU. y que conservará. Si no se dan lo supuestos de los incisos i), ii) o iii), los datos que se hayan recibido en el Marco de Privacidad de Datos UE-EE. UU. deberán devolverse o suprimirse inmediatamente.

h. Cuando la entidad deje de estar amparada por el Marco de Privacidad de Datos UE-EE. UU. por el motivo que sea, deberá eliminar todas las declaraciones que den a entender que continúa participando en el Marco de Privacidad de Datos UE-EE. UU. o tiene derecho a estar amparada por el Marco de Privacidad de Datos UE-EE. UU. También deberá eliminar la marca de certificación del Marco de Privacidad de Datos UE-EE. UU. en caso de que la utilice. Todo engaño en la información dada a conocer al público referente al cumplimiento de la entidad de los principios en materia de privacidad podrá ser perseguible por la Comisión Federal de Comercio, el Departamento de Transporte u otro organismo público competente. Los engaños en la información transmitida al Departamento podrán ser punibles en el marco de la Ley de declaraciones falsas (False Statements Act; título 18, artículo 1001, del Código de Estados Unidos).

7. **Verificación**

a. Las entidades deberán establecer procedimientos de seguimiento para verificar que las afirmaciones y declaraciones de estas sobre sus prácticas en materia de privacidad relativas al Marco de Privacidad de Datos UE-EE. UU. son ciertas y que tales prácticas se aplican de la manera indicada y de conformidad con los principios en materia de privacidad.

b. Para cumplir los requisitos de verificación del principio de impugnación, ejecución forzosa y responsabilidad, las entidades deberán verificar las afirmaciones y declaraciones mencionadas mediante la autoevaluación o mediante verificaciones por terceros.

c. Cuando la entidad haya optado por la autoevaluación, dicha verificación deberá demostrar que sus directrices en materia de privacidad en relación con la información personal recibida de la UE son exactas, completas y de consulta inmediata, que se ajustan a los principios en materia de privacidad y que se aplican integralmente (es decir, que se cumplen). Asimismo, deberá indicar: que los particulares reciben información sobre las vías internas de resolución de reclamaciones y de los órganos independientes de impugnación a los que presentar las reclamaciones; que la entidad dispone de procedimientos de formación de los empleados a estos efectos y que se aplicarán sanciones en caso de incumplimiento; y que existen procedimientos internos para efectuar periódicamente revisiones objetivas del cumplimiento de todo lo anterior. Un directivo u otro representante autorizado de la entidad deberá firmar la declaración de que se ha realizado la autoevaluación como mínimo una vez al año; dicha declaración deberá proporcionarse a petición de los particulares o en el contexto de investigaciones o reclamaciones por incumplimiento.

d. Cuando la entidad haya optado por la verificación externa del cumplimiento, dicha verificación deberá demostrar que sus directrices en materia de privacidad en relación con la información personal recibida de la UE son exactas, completas y de consulta inmediata, que se ajustan a los principios en materia de privacidad y que se aplican integralmente (es decir, que se cumplen). También deberá indicar que los particulares reciben información sobre las vías de resolución de las reclamaciones. Son métodos de verificación válidos, a título meramente enunciativo, las auditorías, las comprobaciones aleatorias, el uso de «señuelos» o de herramientas tecnológicas, según se considere apropiado. El verificador externo o un directivo u otro representante autorizado de la entidad deberá firmar la declaración de que se ha realizado la verificación externa, con resultado satisfactorio, como mínimo una vez al año; dicha declaración deberá proporcionarse a petición de los particulares o en el contexto de investigaciones o reclamaciones por incumplimiento.

e. Las entidades deberán conservar los documentos que prueben por escrito la implantación de sus prácticas en materia de privacidad respecto del Marco de Privacidad de Datos UE-EE. UU. y proporcionarlos previa petición, en el contexto de investigaciones o reclamaciones por incumplimiento, al organismo independiente de resolución de controversias responsable de la investigación de las reclamaciones o al organismo competente en materia de prácticas desleales y engañosas. Las entidades deberán responder inmediatamente a las consultas y demás solicitudes de información del Departamento relacionadas con el cumplimiento de los principios en materia de privacidad.

8. **Acceso**

a. El principio de acceso en la práctica

i. De acuerdo con los principios en materia de privacidad, el derecho de acceso es fundamental para la protección de la privacidad. En particular, permite a los particulares verificar la exactitud de la información existente sobre ellas. El principio de acceso otorga a los particulares el derecho a:

1. obtener la confirmación de la entidad de si esta trata o no datos personales relacionados con el particular ([14]);

2. que se les proporcionen esos datos para que puedan verificar su exactitud y la licitud del tratamiento; y

3. pedir que se corrijan, modifican o supriman los datos cuando sean inexactos o se hayan tratado en vulneración de los principios en materia de privacidad.

ii. Los particulares no estarán obligados a justificar las solicitudes de acceso a sus datos personales. En su respuesta a las solicitudes de acceso de los particulares, las entidades deberán primero considerar la motivación de dichas solicitudes. Por ejemplo, si la solicitud de acceso es vaga o muy amplia, la entidad puede dialogar con el particular para comprender mejor los motivos de la solicitud y localizar la información correspondiente. La entidad podrá preguntar con qué parte o partes de la entidad se puso en contacto el particular o sobre la naturaleza de la información que sea objeto de la solicitud de acceso, o de su uso.

iii. Al ser fundamental el principio de acceso, las entidades siempre deberán procurar, con buena fe, conceder acceso. Por ejemplo, cuando deba protegerse determinada información y esta se distinga fácilmente de la información personal objeto de la solicitud de acceso, la entidad deberá expurgar la información protegida y comunicar la restante. Si la entidad decide limitar el acceso en un supuesto concreto, deberá comunicar al particular que solicitó el acceso la debida justificación e indicar el punto de contacto al que plantear consultas ulteriores.

b. Trabajo o gasto ocasionados por el acceso

i. El derecho de acceso a los datos personales podrá limitarse en circunstancias excepcionales en las que puedan vulnerarse los derechos legítimos de terceros o cuando el trabajo o el gasto de conceder el acceso sean desproporcionados en relación con los riesgos para la privacidad del particular en cuestión. El trabajo y el gasto son factores importantes y deberán tenerse en cuenta, pero no son factores determinantes para decidir si es razonable conceder el acceso.

ii. Por ejemplo, si la información personal se utiliza para tomar decisiones que afecten sustancialmente al particular (por ejemplo, la denegación o la concesión de cuestiones importantes como un seguro, un préstamo hipotecario o un trabajo), entonces, de conformidad con las demás disposiciones de los presentes principios complementarios, la entidad deberá comunicar esta información aun cuando hacerlo sea relativamente difícil o caro. Si la información personal solicitada no es delicada o no se utilizará para tomar decisiones que afecten sustancialmente al particular, pero es fácilmente accesible y poco costosa de proporcionar, la entidad deberá conceder acceso a dicha información.

c. Información comercial confidencial

i. La información comercial confidencial es información que la entidad ha protegido para que no se publique, porque su publicación supondría una ventaja para sus competidores. Las entidades podrán denegar o limitar el acceso en la medida en que la concesión del acceso pleno revele su información comercial confidencial, como en el caso de predicciones de mercado o clasificaciones elaboradas por la entidad, o información comercial confidencial de un tercero que esté sujeta a la obligación contractual de confidencialidad.

([14]) 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 comunican los datos personales.

ii. Cuando la información comercial confidencial pueda distinguirse fácilmente de la información personal objeto de la solicitud de acceso, la entidad deberá expurgar la información comercial confidencial y comunicar la información no confidencial.

d. Organización de las bases de datos

i. El acceso puede concederse mediante la comunicación de la información personal pertinente por parte de la entidad al particular, sin que el particular acceda a la base de datos de la entidad.

ii. El acceso deberá concederse únicamente en la medida en que la entidad tenga en esta información personal. El principio de acceso no comporta en sí ninguna obligación de conservar, mantener, reorganizar o reestructurar los archivos de información personal.

e. Supuestos en que puede limitarse el acceso

i. Teniendo en cuenta que las entidades deben procurar, con buena fe, conceder a los particulares acceso a sus datos personales, las circunstancias en las que las entidades podrán limitar este acceso están tasadas y las razones de dicha limitación deberán ser específicas. De conformidad con el RGPD, las entidades podrán limitar el acceso a la información en la medida en que su comunicación pueda interferir con la protección de intereses públicos preponderantes, 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 con fines de investigación o estadísticos. Entre otros motivos para denegar o limitar el acceso, cabe citar los siguientes:

1. interferencia en la aplicación o el cumplimiento coercitivo del Derecho o en acciones judiciales particulares, especialmente la prevención, investigación o detección de delitos o el derecho a un juicio justo;

2. cuando la comunicación vulnere los derechos legítimos o intereses importantes de terceros;

3. vulneración de prerrogativas u obligaciones jurídicas o profesionales;

4. obstaculización de investigaciones sobre la seguridad de los empleados o de procedimientos de resolución de reclamaciones laborales, de planificación del relevo de los empleados y de reestructuración societaria; o

5. perjuicio para la confidencialidad necesaria para las funciones de control, inspección o regulación relacionadas con la buena gestión económica o financiera, o para negociaciones presentes o futuras relativas a la entidad.

ii. Las entidades que se acojan a una excepción tendrán que demostrar al particular por qué es necesario y los motivos por los que procede limitar el acceso, así como indicar el punto de contacto al que plantear consultas ulteriores.

f. Derecho a obtener confirmación y cobro de una tasa por los gastos inherentes a la concesión del acceso

i. Los particulares tienen derecho a obtener confirmación de si la 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 tasa que no sea excesiva.

ii. El cobro de la tasa podrá justificarse, por ejemplo, cuando las solicitudes de acceso sean manifiestamente abusivas, en particular por su carácter repetitivo.

iii. No podrá denegarse el acceso por motivo de su coste si el particular se ofrece a sufragarlo.

g. Solicitudes de acceso repetitivas u obstructivas

i. Las entidades podrán establecer límites razonables en cuanto al número de veces que responderá en un período determinado las solicitudes de acceso de cada particular. Al fijar estos límites, las entidades deberán 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. Solicitudes de acceso fraudulentas

i. Las entidades no estarán obligadas a conceder acceso a menos que reciban información suficiente para confirmar la identidad del particular que presenta la solicitud.

i. Plazo para responder

i. Las entidades deberán responder a las solicitudes de acceso en un plazo razonable, de una manera razonable y en una forma que sea fácilmente comprensible para el particular. La entidad que proporcione información a los interesados de manera periódica podrá atender la solicitud de acceso del particular por medio de dicha comunicación periódica, siempre que ello no suponga un retraso excesivo.

9. **Datos de recursos humanos**

a. Ámbito de aplicación del Marco de Privacidad de Datos UE-EE. UU.

i. Cuando las entidades ubicadas en la UE transfieran información personal de sus empleados (pasada o presente) obtenida en el marco de la relación laboral a la matriz, la filial o a una empresa de servicios no asociada ubicados en los EE. UU. que participen en el Marco de Privacidad de Datos UE-EE. UU., la transferencia estará amparada por el Marco de Privacidad de Datos UE-EE. UU. En tal caso, la recogida de la información y su tratamiento previo a la transferencia deberán haber respetado la normativa del Estado miembro de la UE donde se haya recogido y cualquier condición o limitación aplicable a su transferencia de conformidad con la normativa vigente.

ii. Los principios en materia de privacidad solamente son de aplicación cuando se transfieran datos sobre particulares identificados o identificables de manera individualizada o se acceda a ellos. Los informes estadísticos basados en datos agregados sobre empleo que no contengan datos personales o el uso de datos anonimizados no plantean problemas desde el punto de vista de la privacidad.

b. Aplicación de los principios de notificación y opción

i. Las entidades estadounidenses que hayan recibido información sobre los empleados en el Marco de Privacidad de Datos UE-EE. UU. podrán comunicarla a terceros o utilizarla con fines distintos exclusivamente con arreglo a los principios de notificación y de opción. Por ejemplo, cuando las entidades estadounidenses pretendan utilizar la información personal obtenida a través de la relación laboral para fines no laborales, como comunicaciones de publicitarias, deberán brindar a los particulares afectados la posibilidad de ejercer su derecho de opción antes de hacerlo, a menos que estos hayan dado su consentimiento a la utilización de la información para tales fines. Dicho uso deberá ser compatible con los fines para los que la información personal ha sido recogida o para los que, posteriormente, haya dado su consentimiento el particular. Es más, esta posibilidad no se utilizará para limitar sus oportunidades laborales ni para sancionarlos.

ii. Debe advertirse que algunas condiciones de aplicación general a las transferencias procedentes de los Estados miembros de la UE podrán prohibir otros usos de la información incluso después de su transferencia fuera de la UE, y que tales condiciones deben respetarse.

iii. Además, los empleadores deberán procurar razonablemente tener en cuenta las preferencias de sus empleados en cuanto a la protección de su privacidad, como, por ejemplo, limitar el acceso a los datos personales, anonimizar determinados datos o 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 de opción en la medida y por el 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

i. El principio complementario sobre el acceso ofrece directrices sobre los motivos con que se podrá justificar la denegación o limitación del acceso previa petición en el ámbito de los recursos humanos. Por supuesto, los empleadores de la UE deberán cumplir la normativa local y garantizar que los empleados de la UE 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 Marco de Privacidad de Datos UE-EE. UU. exige a las entidades que traten estos datos en los EE. UU. que cooperen a la hora de conceder el acceso directamente o a través del empleador de la UE.

d. Garantía del cumplimiento

i. En la medida en que la información se utilice exclusivamente en el marco de la relación laboral, la entidad de la UE es la responsable principal de los datos ante el empleado. De ello se deduce que, cuando los empleados de la UE planteen reclamaciones sobre la vulneración de sus derechos de protección de datos y no estén satisfechos con el resultado de los procedimientos de verificación interna, reclamación y recurso (o con cualquier procedimiento de resolución de reclamaciones laborales derivados de contratos con entidades sindicales), deben dirigirse a la agencia de protección de datos o a la autoridad laboral, nacional o regional, del Estado correspondiente. Se incluyen también los casos en que el supuesto tratamiento inadecuado de la información personal sea responsabilidad de la entidad estadounidense que haya recibido la información a través del empleador y, por consiguiente, suponga una posible vulneración de los principios en materia de privacidad. Este será el método más eficiente para atender los derechos y obligaciones, que con frecuencia se solapan, impuestos por la normativa laboral local y por los convenios colectivos, así como por la normativa sobre protección de datos.

ii. Las entidades estadounidenses participantes que utilicen datos de recursos humanos transferidos desde la UE en el marco de la relación laboral y que deseen que dichas transferencias también estén amparadas por el Marco de Privacidad de Datos UE-EE. UU. deberán comprometerse a cooperar en las investigaciones de las autoridades de la UE competentes y a acatar sus dictámenes en dichos casos.

e. Aplicación del principio de responsabilidad proactiva por las transferencias ulteriores

i. Para las necesidades operativas ocasionales relacionadas con el trabajo de las entidades participantes en relación con los datos personales transferidos en el Marco de Privacidad de Datos UE-EE. UU., como la reserva de un vuelo o de una habitación de hotel o la contratación de un seguro, podrán 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 del tratamiento, a diferencia de lo que exige el principio de responsabilidad proactiva por las transferencias ulteriores, siempre y cuando la entidad participante haya cumplido los principios de notificación y de opción.

10. **Contratos obligatorios para las transferencias ulteriores**

a. Contratos de tratamiento de datos

i. Cuando se transfieran datos personales desde la UE a los EE. UU. únicamente a efectos de su tratamiento, se exigirá un contrato, independientemente de la participación del encargado del tratamiento en el Marco de Privacidad de Datos UE-EE. UU.

ii. Los responsables del tratamiento de datos de la UE están obligados a suscribir un contrato cuando se realice una transferencia a efectos meramente de tratamiento, independientemente de que la operación de tratamiento se realice dentro o fuera de la UE y de que el encargado del tratamiento participe o no en el Marco de Privacidad de Datos UE-EE. UU. La finalidad del contrato es garantizar que el encargado del tratamiento:

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

2. disponga medidas técnicas y organizativas apropiadas para proteger los datos personales contra la destrucción accidental o ilícita, la pérdida accidental, la modificación, la comunicación o el acceso no autorizados, y sepa si se autoriza la transferencia ulterior; y

3. teniendo en cuenta la naturaleza del tratamiento, ayude al responsable del tratamiento a responder a los particulares que ejerzan los derechos que les confieren los principios en materia de privacidad.

iii. Dado que las entidades participantes confieren una protección adecuada, los contratos con dichas entidades a efectos meramente de tratamiento no requieren autorización previa.

b. Transferencias dentro de un grupo de sociedades de capital o entidades vinculadas

i. Cuando se produce una transferencia de información personal entre dos responsables del tratamiento pertenecientes a un grupo de sociedades de capital o entidades vinculadas, no siempre se exige la suscripción de un contrato en virtud del principio de responsabilidad proactiva por las transferencias ulteriores. Los responsables del tratamiento pertenecientes a un grupo de sociedades de capital o entidades vinculadas podrán basar estas transferencias en otros instrumentos, como la normativa societaria vinculante de la UE u otros instrumentos intragrupo (por ejemplo, programas de cumplimiento y control), que garanticen la continuidad de la protección de la información personal de conformidad con los principios en materia de privacidad. En el caso de estas transferencias, la entidad participante seguirá siendo responsable del cumplimiento de los principios en materia de privacidad.

c. Transferencias entre responsables del tratamiento

i. Para las transferencias entre responsables del tratamiento, no es necesario que el responsable del tratamiento destinatario sea una entidad participante o cuente con un órgano independiente de impugnación. La entidad participante deberá suscribir un contrato con el responsable externo del tratamiento destinatario que confiera el mismo nivel de protección que el Marco de Privacidad de Datos UE-EE. UU., sin incluir el requisito de que el responsable externo del tratamiento sea una entidad participante en el Marco o tenga un órgano independiente de impugnación, siempre y cuando ofrezca otro medio equivalente.

11. **Resolución de controversias y ejecución forzosa**

a. El principio de impugnación, ejecución forzosa y responsabilidad establece los requisitos para la ejecución forzosa del Marco de Privacidad de Datos UE-EE. UU. En el principio complementario sobre la verificación se establece cuándo se entiende que se cumplen los requisitos de la letra a, inciso ii, del principio anterior. Este principio complementario se refiere a la letra a, incisos i y iii, donde se exigen órganos independientes de impugnación. Estas vías de impugnación pueden adoptar diferentes formas, pero deben cumplir los requisitos que impone el principio de impugnación, ejecución forzosa y responsabilidad. Las entidades pueden cumplirlos de la manera siguiente: i) cumplimiento de los programas de protección de la privacidad concebidos por el sector privado que incorporen los principios en materia de privacidad en sus reglas y cuenten con mecanismos de ejecución forzosa eficaces, similares a los descritos en el principio de impugnación, ejecución forzosa y responsabilidad; ii) cumplimiento de lo dispuesto por las autoridades de supervisión establecidas legal o reglamentariamente que prevean la tramitación de las reclamaciones individuales y la resolución de las controversias; o iii) compromiso de cooperación con las APD establecidas en la UE o con sus representantes autorizados.

b. Esta lista se ofrece a título ilustrativo y no es de ninguna manera taxativa. El sector privado podrá establecer otros mecanismos para la ejecución forzosa, siempre que cumplan los requisitos que imponen el principio de impugnación, ejecución forzosa y responsabilidad y los principios complementarios. Téngase en cuenta que los requisitos que impone el principio de impugnación, ejecución forzosa y responsabilidad se añaden al requisito de que las medidas del ámbito autorregulatorio deben ser ejecutables con arreglo al artículo 5 de la Ley de la Comisión Federal de Comercio (título 15, artículo 45, del Código de Estados Unidos), por el que se prohíben los actos desleales o engañosos, con arreglo al título 49, artículo 41712, del Código de Estados Unidos, por el que se prohíbe a los transportistas y los agentes de venta de billetes participar en prácticas desleales o engañosas en el transporte aéreo o en la comercialización de este tipo de transporte, o con arreglo a otras leyes o reglamentos por los que se prohíban tales actos.

c. Con el objeto de garantizar el cumplimiento del Marco de Privacidad de Datos UE-EE. UU. y para coadyuvar a la administración del programa, las entidades, así como sus órganos independientes de impugnación, deberán proporcionar información sobre el Marco cuando así lo solicite el Departamento. Asimismo, las entidades deberán responder sin demora a las reclamaciones relacionadas con su cumplimiento de los principios en materia de privacidad remitidas por las APD a través del Departamento. 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 normativa estadounidense.

d. Órganos de impugnación

i. Se alentará a los particulares a presentar las reclamaciones a la entidad correspondiente antes de dirigirse a los órganos independientes de impugnación. Las entidades deberán responder al particular en el plazo de los cuarenta y cinco días siguientes a la recepción de la reclamación. La independencia de dichos órganos de impugnación es una cuestión de hecho que puede demostrarse por su imparcialidad y por la transparencia de su composición y de su financiación, o porque los avale una trayectoria reconocida. De conformidad con lo dispuesto en el principio de impugnación, ejecución forzosa y responsabilidad, las vías de impugnación que se ofrezcan a los particulares deberán ser gratuitas y poder activarse inmediatamente. Los organismos independientes de resolución de controversias deberán admitir a trámite todas las reclamaciones que reciban de los particulares, a menos que estén manifiestamente infundadas o sean insustanciales, lo cual no impedirá que el organismo independiente de resolución de controversias con competencia respecto de la vía de impugnación establezca condiciones para la admisión a trámite; sin embargo, dichas condiciones deberán ser transparentes y justificarse debidamente (por ejemplo, no admitir a trámite las reclamaciones cuyo objeto no esté comprendido en el ámbito de aplicación del programa o cuya competencia corresponda a otro organismo) y no deberán obstaculizar el compromiso de admitir a trámite las reclamaciones legítimas. Además, los órganos de impugnación deberán proporcionar a los particulares, cuando presenten la reclamación, toda la información disponible sobre el funcionamiento del procedimiento de resolución de controversias, en particular, la notificación de las prácticas de protección de la privacidad que siguen esos órganos, de conformidad con los principios en materia de privacidad. También deberán colaborar en el desarrollo de herramientas tales como formularios normalizados de reclamación para facilitar la resolución de las reclamaciones.

ii. Los órganos independientes de impugnación deberán incluir en sus sitios web públicos información sobre los principios en materia de privacidad y los servicios que prestan en el Marco de Privacidad de Datos UE-EE. UU. Dicha información deberá incluir los elementos siguientes: 1) información sobre los requisitos de los principios en materia de privacidad relativos a los órganos independientes de impugnación, o un enlace a ellos; 2) un enlace al sitio web del Departamento sobre el Marco de Privacidad de Datos; 3) la explicación de que sus servicios de resolución de controversias a efectos del Marco de Privacidad de Datos UE-EE. UU. son gratuitos para los particulares; 4) la descripción de cómo pueden presentarse las reclamaciones relacionadas con los principios en materia de privacidad; 5) el plazo de tramitación de las reclamaciones relacionadas con dichos principios; 6) la descripción de todas las medidas de reparación posibles.

iii. Los órganos independientes de impugnación deberán publicar un informe anual que contenga estadísticas agregadas sobre los servicios de resolución de controversias. Dicho informe anual expondrá: 1) el número total de reclamaciones relacionadas con los principios en materia de privacidad que se hayan recibido durante el año de referencia; 2) la naturaleza de las reclamaciones recibidas; 3) las medidas tomadas respecto de la calidad de la solución de controversias, como, por ejemplo, la duración de la tramitación de las reclamaciones; y 4) el resultado de las reclamaciones tramitadas, a saber, el número y el tipo de medidas de reparación dictadas o de sanciones impuestas.

iv. Como se establece en el anexo I, los particulares podrán recurrir al arbitraje, respecto de reclamaciones no resueltas, para que se determine si la entidad participante en cuestión ha incumplido las obligaciones que le imponen los principios en materia de privacidad para con el particular en cuestión y si dicho incumplimiento se encuentra total o parcialmente sin reparar. Esta vía de impugnación solo servirá para esos fines; no se podrá utilizar, por ejemplo, por lo que respecta a las excepciones a los principios en materia de privacidad ([15]) ni con respecto a la adecuación del Marco de Privacidad de Datos UE-EE. UU. En este procedimiento arbitral, el Panel del Marco de Privacidad de Datos UE-EE. UU. (tribunal arbitral compuesto por entre uno y tres árbitros, según acuerden las partes) tiene competencia para imponer medidas específicas, equitativas y no monetarias (como la corrección, la supresión o la devolución de los datos del particular en cuestión o el acceso a estos) con las que reparar la vulneración de los principios en materia de privacidad en lo que se refiere exclusivamente al particular. Los particulares y las entidades participantes podrán, en virtud de la Ley federal de arbitraje (Federal Arbitration Act), solicitar la revisión y la ejecución forzosa judiciales de los laudos arbitrales de conformidad con la normativa estadounidense.

e. Medidas de reparación y sanciones:

i. Las medidas de reparación que dicte el organismo independiente de resolución de controversias deberán tener como finalidad que la entidad: corrija o revierta los efectos del incumplimiento, en la medida de lo posible; adecue cualquier tratamiento que haga en el futuro a los principios en materia de privacidad; y, cuando proceda, interrumpa el tratamiento de los datos personales del particular que haya presentado la reclamación. Las sanciones tienen que ser lo suficientemente severas para que la entidad cumpla los principios en materia de privacidad. La existencia de una gama de sanciones con distintos grados de gravedad permitirá a los organismos de resolución de controversias responder apropiadamente a los

([15]) Principios en materia de privacidad, consideraciones generales, punto 5.

diferentes niveles de incumplimiento. Podrá imponerse como sanción la publicidad de los incumplimientos constatados y la obligación de suprimir los datos en determinadas circunstancias ([16]). Otras sanciones podrán ser la suspensión y la eliminación del sello, la indemnización a los particulares por los perjuicios sufridos como consecuencia del incumplimiento y la imposición de obligaciones de hacer o no hacer. Los organismos independientes de resolución de controversias del sector privado y los órganos del ámbito autorregulatorio deberán notificar el incumplimiento de sus resoluciones por parte de las entidades participantes a los organismos del Ejecutivo competentes o al órgano jurisdiccional competente, si procede, y al Departamento.

f. Impugnación ante la Comisión Federal de Comercio

i. La Comisión Federal de Comercio se ha comprometido a examinar con carácter prioritario las reclamaciones por incumplimiento de los principios en materia de privacidad remitidas por i) los organismos del ámbito autorregulatorio en materia de privacidad y otros organismos independientes de resolución de controversias; ii) los Estados miembros de la UE; y iii) el Departamento, para determinar si se ha vulnerado el artículo 5 de la Ley de la Comisión Federal de Comercio, por el que se prohíben los actos o prácticas desleales o engañosos en el comercio. Si la Comisión Federal de Comercio ve indicios de que se ha vulnerado el artículo 5, podrá tratar de solucionar el asunto solicitando una resolución administrativa de cese de las prácticas impugnadas o acudiendo a la corte federal distrital (*federal district court*) competente; si se estima su pretensión, la corte podrá dictar una resolución judicial al mismo efecto. Son ejemplos de indicios de vulneración las declaraciones falsas de cumplimiento de los principios en materia de privacidad o de participación en el Marco de Privacidad de Datos UE-EE. UU. por parte de las entidades que, bien ya no participan en el Marco de Privacidad de Datos UE-EE. UU., bien nunca se autocertificaron ante el Departamento. La Comisión Federal de Comercio podrá solicitar la imposición de sanciones pecuniarias si se incumplen las órdenes administrativas de cese, así como ejercer acciones judiciales civiles o penales en los casos de incumplimiento de resoluciones judiciales federales; la Comisión notificará al Departamento las actuaciones de este tipo que emprenda. El Departamento anima a los organismos del Ejecutivo a que le notifiquen el resultado final de dichas reclamaciones remitidas o de otras resoluciones respecto del cumplimiento de los principios en materia de privacidad.

g. Incumplimiento sistemático

i. Si la entidad incumple sistemáticamente los principios en materia de privacidad, perderá el derecho a acogerse al Marco de Privacidad de Datos UE-EE. UU. Las entidades que hayan incumplido sistemáticamente los principios en materia de privacidad serán eliminadas por el Departamento de la lista del Marco de Privacidad de Datos y deberán devolver o suprimir la información personal que hubiesen recibido con arreglo al Marco de Privacidad de Datos UE-EE. UU.

ii. Se considera que se produce incumplimiento sistemático cuando la entidad que haya autocertificado su cumplimiento de los principios en materia de privacidad ante el Departamento se niegue a cumplir la resolución del organismo del ámbito autorregulatorio en materia de privacidad, del organismo de resolución de controversias independiente o del organismo público, o cuando uno de estos organismos considere que la entidad incumple con frecuencia los principios en materia de privacidad, hasta el punto de que su declaración de cumplimiento deja de ser creíble. Cuando dicho pronunciamiento proceda de un organismo distinto del Departamento, la entidad deberá comunicarlo sin demora al Departamento. El incumplimiento de esta obligación podrá ser punible en el marco de la Ley de declaraciones falsas (título 18, artículo 1001, del Código de Estados Unidos). Las entidades que se den de baja en un programa de protección de la privacidad del ámbito autorregulatorio gestionado por el sector privado o que dejen de someterse a un órgano independiente de resolución de controversias no quedan eximidas de su obligación de cumplir los principios en materia de privacidad, y su incumplimiento podría dar lugar a un incumplimiento sistemático.

iii. El Departamento eliminará de la lista del Marco de Privacidad de Datos a las entidades que incumplan sistemáticamente, también en respuesta a las notificaciones que reciba de la propia entidad, del organismo del ámbito autorregulatorio en materia de privacidad, de otro organismo independiente de resolución de controversias o de un organismo público competente, pero solo después de haber dado notificado a la entidad con treinta días de antelación y de haberle brindado la oportunidad de responder ([17]). En consecuencia, la lista del Marco de Privacidad de Datos publicada por el Departamento aclarará qué entidades están amparadas por el Marco de Privacidad de Datos UE-EE. UU. y cuáles ya no lo están.

iv. La entidad que solicite someterse a un organismo del ámbito autorregulatorio con el fin de volver a acogerse al Marco de Privacidad de Datos UE-EE. UU. deberá proporcionar a dicho organismo información completa sobre su participación anterior en el Marco de Privacidad de Datos UE-EE. UU.

([16]) Los organismos independientes de resolución de controversias tienen discrecionalidad para decidir cuándo aplican estas sanciones. El carácter delicado 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 la entidad ha recogido, utilizado o comunicado información incumpliendo manifiestamente los principios en materia de privacidad.

([17]) El Departamento indicará en la notificación el plazo, que será necesariamente inferior a treinta días, en el que la entidad puede responder.

12. **Plazo para el ejercicio del derecho a oponerse**

a. En general, la finalidad del principio de opción es garantizar que la información personal se utilice y comunique de manera coherente con las expectativas y elecciones del particular. Por tanto, los particulares deberán tener la posibilidad de oponerse a que su información personal se utilice con fines de mercadotecnia directa en cualquier momento, siempre que se respeten los plazos razonables establecidos por la entidad, como el tiempo necesario para que esta pueda aplicar dicha decisión del particular. Asimismo, las entidades pueden exigir información suficiente para confirmar la identidad del particular que se opone. En los EE. UU., los particulares pueden ejercer este derecho mediante un programa central de oposición. En cualquier caso, a los particulares se les deberá ofrecer un mecanismo inmediatamente utilizable y asequible para ejercer su derecho.

b. De la misma forma, la entidad puede utilizar la información para determinados fines de mercadotecnia directa cuando sea inviable brindar al particular la oportunidad de oponerse antes de utilizar la información, siempre que le brinde de inmediato la oportunidad (y en cualquier momento, previa petición) de negarse (sin coste alguno para el particular) a recibir posteriores comunicaciones de mercadotecnia directa y que la entidad cumpla los deseos del particular.

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 ayuda física, podrán ser transferidas a entidades radicadas fuera de la UE en diversas circunstancias. En virtud del RGPD, a falta de una decisión de adecuación, los datos personales solo pueden transmitirse a un tercer país si se ofrecen garantías adecuadas de protección de los datos de conformidad con el artículo 46 del RGPD o, en situaciones específicas, si se cumple alguna de las condiciones del artículo 49 del RGPD (por ejemplo, cuando el interesado haya dado explícitamente su consentimiento a la transferencia). Las entidades estadounidenses que participan en el Marco de Privacidad de Datos UE-EE. UU. confieren una protección adecuada a los datos personales y, por tanto, pueden recibir transferencias de datos de la UE en virtud del artículo 45 del RGPD, sin tener que establecer un instrumento para las transferencias de conformidad con el artículo 46 del RGPD ni cumplir las condiciones del artículo 49 del RGPD. Dado que el Marco de Privacidad de Datos UE-EE. UU. incluye reglas específicas para la información delicada, dicha información (que puede ser preciso recoger, por ejemplo, en relación con las necesidades de ayuda física de los clientes) puede incluirse en las transferencias a entidades participantes. No obstante, en todos los casos, la entidad que transfiere la información ha de cumplir la normativa del Estado miembro de la UE en el que opera, que, por ejemplo, puede imponer condiciones especiales para el tratamiento de datos delicados.

14. **Productos médicos y farmacéuticos**

a. Aplicación de la normativa del Estado miembro de la UE o de los principios en materia de privacidad

i. La normativa de los Estados miembros o de la UE se aplica a la recogida de los datos personales y a todo tratamiento previo a su transferencia a los EE. UU. Los principios en materia de privacidad se aplican a los datos una vez que se hayan transferido a los EE. UU. Los datos personales utilizados con fines de investigación farmacéutica u otros fines deberán ser anonimizados cuando resulte adecuado.

b. Investigaciones científicas futuras

i. Los datos personales conseguidos en estudios de investigación médica o farmacéutica suelen desempeñar un valioso papel en futuras investigaciones científicas. Cuando se transfieran datos personales recogidos para un estudio de investigación a una entidad estadounidense en el Marco de Privacidad de Datos UE-EE. UU., la entidad podrá utilizar los datos en una nueva actividad de investigación científica si lo notifica con la debida antelación y brinda oportunidad para oponerse. En la notificación se proporcionará información sobre el uso concreto que se dará a los datos, a saber, seguimiento, otros estudios o mercadotecnia.

ii. Se sobreentiende que no podrán especificarse todos los usos futuros de los datos, ya que estos pueden resultar de un nuevo enfoque respecto de los datos originales, de nuevos descubrimientos y avances médicos y de novedades normativas y de salud pública. Por consiguiente, la notificación deberá incluir, si procede, una referencia al posible uso de los datos personales en futuras actividades de investigación médica y farmacéutica que todavía se desconocen. Será necesario obtener un nuevo consentimiento si el uso 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

i. Los participantes podrán decidir por sí mismos o a instancias de terceros retirarse de un ensayo clínico en cualquier momento. No obstante, los datos recogidos con anterioridad a que se retiren 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 consintieron en participar.

d. Transferencias con fines regulatorios y de supervisión

i. Las empresas de productos farmacéuticos y sanitarios tienen autorización para comunicar datos personales obtenidos en ensayos clínicos realizados en la UE a las autoridades reguladoras de los EE. UU. con fines regulatorios y de supervisión. Se autorizan transferencias similares a terceros que no sean las autoridades reguladoras, como filiales de las empresas u otros investigadores, siempre que se haga con arreglo a los principios de notificación y opción.

e. Estudios enmascarados

i. Muchas veces, para garantizar la objetividad de los ensayos clínicos, se priva a los participantes y, con frecuencia, también a los investigadores, de la información sobre el tratamiento que recibe cada participante. Dar esa información podría poner en peligro la validez de los estudios de investigación y de sus resultados. A los participantes en estos ensayos clínicos (denominados «estudios enmascarados») no se les proporcionará acceso a los datos sobre su tratamiento durante el ensayo si se les explicó tal limitación cuando se unieron al ensayo y si la comunicación de dicha información puede poner en peligro la integridad de la investigación.

ii. Consentir en participar 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 o, subsidiariamente, a la entidad patrocinadora.

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

i. Las empresas de productos farmacéuticos y sanitarios no están obligadas a aplicar los principios en materia de privacidad en lo relativo a los principios de notificación, opción, responsabilidad proactiva, transferencia ulterior y acceso en las actividades que realizan para controlar la eficacia y la seguridad de los productos, entre ellas informar sobre circunstancias adversas y hacer seguimiento a los pacientes o personas que utilicen determinados medicamentos o productos sanitarios, en la medida en que el cumplimiento de los principios en materia de privacidad afecte al cumplimiento de los requisitos regulatorios. Esto se aplica tanto a los informes de los profesionales sanitarios dirigidos a las empresas de productos farmacéuticos y sanitarios, como a los de estas a los organismos del Ejecutivo, como la Administración de Alimentos y Medicamentos (Food and Drug Administration).

g. Datos codificados

i. 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. La clave original solo la conoce el investigador, de modo que solo él puede identificar al sujeto investigado en determinadas circunstancias (por ejemplo, cuando es necesario un seguimiento médico). Las transferencias de datos codificados de esta forma desde la UE a los EE. UU. que sean datos personales en virtud de la normativa de la UE quedarán sujetas a los principios en materia de privacidad.

15. **Información de registros públicos e información de acceso público**

a. Las entidades deberán aplicar los principios de seguridad, de integridad de los datos y limitación de la finalidad y de recurso, ejecución forzosa y responsabilidad a los datos personales obtenidos de fuentes de acceso público. Estos principios se aplicarán también a los datos personales obtenidos de registros públicos, por ejemplo, los registros de organismos públicos o entidades a cualquier nivel que sean de consulta pública.

b. No es necesario aplicar los principios de notificación, opción y responsabilidad proactiva por las transferencias ulteriores a la información de registros públicos siempre que no se combine con información de registros no públicos y se cumplan las condiciones de consulta establecidas por el organismo competente. Asimismo, no es necesario, por lo general, aplicar los principios de notificación, opción y responsabilidad proactiva por las transferencias ulteriores a la información de dominio público a menos que el remitente europeo indique que dicha información está sujeta a limitaciones que imponen la aplicación de tales principios por parte de la entidad para los fines que tenga previsto. Las entidades no son responsables del uso de la información por quienes la obtengan de fuentes publicadas.

c. Cuando se descubra que la entidad ha hecho pública intencionadamente información personal contraviniendo los principios en materia de privacidad para beneficiarse de estas excepciones o que otros puedan hacerlo, la entidad dejará de estar amparada por el Marco de Privacidad de Datos UE-EE. UU.

d. No es necesario aplicar el principio de acceso a la información de 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 el organismo 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 deberán dar acceso a toda la información, siempre que no le sean de aplicación otras excepciones permitidas.

e. Como sucede con la información de registros públicos, no es necesario dar 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 las tarifas habituales por responder a las solicitudes de acceso. Alternativamente, los particulares podrán solicitar el acceso a su información directamente a través de la entidad que haya compilado los datos inicialmente.

16. **Solicitudes de acceso de los poderes públicos**

a. Con el objeto de garantizar la transparencia de las solicitudes lícitas de acceso a información personal procedentes de los poderes públicos, las entidades participantes podrán publicar voluntariamente informes periódicos de transparencia sobre el número de solicitudes de información personal que reciban de las autoridades públicas por razones de seguridad nacional o policiales, siempre y cuando dicha comunicación esté permitida en virtud de la normativa aplicable.

b. La información proporcionada por las entidades participantes en estos informes, junto con la información publicada por la Comunidad de Inteligencia y otra información, podrá ser utilizada para contribuir a la revisión conjunta anual del funcionamiento del Marco de Privacidad de Datos UE-EE. UU. de conformidad con los principios en materia de privacidad.

c. La falta de la notificación contemplada en la letra a, inciso xii, del principio de notificación no impedirá que la entidad responda a las solicitudes lícitas, ni condicionará su capacidad para hacerlo.

ANEXO I: MODELO DE ARBITRAJE

El presente anexo fija el régimen que las entidades participantes en el Marco de Privacidad de Datos UE-EE. UU. están obligadas a seguir al arbitrar las reclamaciones, de conformidad con el principio de impugnación, ejecución forzosa y responsabilidad. El arbitraje vinculante descrito a continuación vale para ciertas reclamaciones no resueltas respecto de los datos amparados por el Marco de Privacidad de Datos UE-EE. UU. La finalidad de esta figura es ofrecer un mecanismo facultativo para los particulares, rápido, independiente y equitativo con el que hallar una solución para las posibles vulneraciones de los principios en materia de privacidad no resueltas mediante ningún otro de los mecanismos del Marco de Privacidad de Datos UE-EE. UU.

A. **Ámbito de aplicación**

Los particulares podrán recurrir al arbitraje, respecto de reclamaciones no resueltas, para que se determine si la entidad participante en cuestión ha incumplido las obligaciones que le imponen los principios en materia de privacidad para con el particular en cuestión y si dicho incumplimiento se encuentra total o parcialmente sin reparar. Esta vía de impugnación solo servirá para esos fines; no se podrá utilizar, por ejemplo, por lo que respecta a las excepciones a los principios en materia de privacidad ([1]) ni con respecto a la adecuación del Marco de Privacidad de Datos UE-EE. UU.

B. **Reparación posible**

En el procedimiento arbitral, el Panel del Marco de Privacidad de Datos UE-EE. UU. (tribunal arbitral compuesto por entre uno y tres árbitros, según acuerden las partes) tiene competencia para imponer medidas específicas, equitativas y no monetarias (como la corrección, la supresión o la devolución de los datos del particular en cuestión o el acceso a estos) con las que reparar la vulneración de los principios en materia de privacidad en lo que se refiere exclusivamente al particular. Esta es la única competencia del Panel del Marco de Privacidad de Datos UE-EE. UU. en materia de reparación. Al ponderar la reparación, el tribunal arbitral debe tener en cuenta las demás medidas de reparación ya dictadas a resultas de otros procesos derivados del Marco de Privacidad de Datos UE-EE. UU. No se contempla la posibilidad de conceder indemnizaciones, condenar en costas, imponer el reembolso de tasas u honorarios, ni otras medidas reparatorias. Cada parte asume los honorarios de sus abogados.

C. **Requisitos para el arbitraje**

Para poder solicitar la incoación de un proceso arbitral, los particulares deberán haber: 1) planteado la vulneración directamente a la entidad y dado a esta la oportunidad de resolver la cuestión dentro del plazo establecido en la letra d, inciso i, del principio complementario sobre la resolución de controversias y la ejecución forzosa; 2) acudido al órgano independiente de impugnación contemplado en los principios en materia de privacidad, que no tiene coste alguno para el particular; y 3) planteado el asunto a través de su APD al Departamento y dado a este la oportunidad de hacer todo cuanto pueda para resolver el asunto en los plazos indicados en la carta de la Administración de Comercio Internacional (International Trade Administration), adscrita al Departamento, sin coste alguno para el particular.

No se podrá solicitar la incoación de un proceso arbitral por vulneración de los principios en materia de privacidad si dicha vulneración: 1) ya se sometió anteriormente a otro proceso arbitral vinculante; 2) ha sido objeto de una sentencia judicial firme en un proceso del que el particular fuera parte; o 3) ya haya sido resuelta anteriormente por convenio transaccional entre las partes. Por otra parte, tampoco se podrá solicitar la incoación de un proceso arbitral si la APD correspondiente: 1) tiene competencia para resolver la reclamación en virtud del principio complementario sobre la función de las autoridades de protección de datos o el principio complementario sobre los datos de recursos humanos; o 2) tiene competencia para resolver la vulneración objeto de reclamación directamente con la entidad. La competencia que tenga la APD correspondiente para resolver la reclamación contra un responsable del tratamiento de la UE no impide que se solicite la incoación de un proceso arbitral contra una persona jurídica distinta no sujeta a la competencia de la APD.

D. **Naturaleza vinculante de los laudos**

Solicitar la incoación de un proceso arbitral vinculante es una facultad que tienen los particulares. Los laudos arbitrales serán vinculantes para todas las partes del arbitraje. Una vez solicitada, el particular renuncia a solicitar reparación por la misma vulneración a otro organismo, con la excepción de que, si las medidas equitativas y no monetarias no van a reparar totalmente la vulneración, la solicitud de la incoación de un proceso arbitral por parte del particular no será óbice para demandar por la vía judicial una indemnización por daños y perjuicios.

([1]) Principios en materia de privacidad, consideraciones generales, punto 5.

E. **Revisión y ejecución forzosa**

Los particulares y las entidades participantes podrán, en virtud de la Ley federal de arbitraje (Federal Arbitration Act), solicitar la revisión y la ejecución forzosa judiciales de los laudos arbitrales de conformidad con la normativa estadounidense ([2]). Tales demandas deben presentarse ante la corte federal distrital en cuya demarcación judicial se encuentre el centro de actividad principal de la entidad participante.

Esta opción de arbitraje tiene por objeto resolver controversias concretas; los laudos arbitrales no están pensados para servir de precedente argumentativo o vinculante en asuntos que impliquen a otras partes, como en arbitrajes futuros, en órganos jurisdiccionales de la UE o de los EE. UU. o en procedimientos ante la Comisión Federal de Comercio.

F. **Tribunal arbitral**

Las partes escogerán a los árbitros que formarán el tribunal arbitral de la lista de árbitros que se describe a continuación.

De conformidad con la normativa aplicable, el Departamento y la Comisión Europea elaborarán una lista de como mínimo diez árbitros, elegidos en función de su independencia, integridad y especialización. En relación con este proceso, se aplicará cuanto sigue:

Los árbitros:

1) permanecerán en la lista durante un período de tres años, siempre que no concurran circunstancias excepcionales o proceda su eliminación por causa justificada, renovable por el Departamento, previa notificación a la Comisión Europea, por períodos adicionales de tres años;

2) no podrán recibir instrucciones de ninguna de las partes, ni de ninguna entidad participante, ni de ninguna otra autoridad pública u organismo de garantía del cumplimiento de los EE. UU., de la UE o de un Estado miembro de la UE, ni estar asociados a ninguno de ellos; y

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

([2]) El capítulo 2 de la Ley federal de arbitraje establece que las cláusulas compromisorias y los laudos arbitrales que se deriven de relaciones jurídicas, contractuales o no, consideradas mercantiles, como un negocio jurídico, un contrato o un acuerdo de los descritos en el artículo 2 de la Ley federal de arbitraje, están amparados por el Convenio sobre el reconocimiento y ejecución de las sentencias arbitrales extranjeras, de 10 de junio de 1958 [Colección de tratados y otros acuerdos internacionales de los EE. UU. (United States Treaties and Other International Agreements), volumen 21, página 2519; Serie de tratados y otras normas internacionales (Treaties and Other International Acts Series), n.º 6997 («Convenio de Nueva York»)] (título 9, artículo 202, del Código de Estados Unidos). Dispone asimismo que las cláusulas o los laudos que se deriven de dicha relación entre ciudadanos estadounidenses se considera que no están amparados por el Convenio de Nueva York salvo que esa relación comprenda bienes en el extranjero, contemple la ejecución voluntaria o forzosa en el extranjero o presente puntos de conexión razonable de otro tipo con uno o más países extranjeros (*ibidem*). En virtud del capítulo 2, toda parte en el arbitraje puede solicitar a cualquier órgano jurisdiccional que tenga jurisdicción en virtud de ese capítulo que dicte una resolución que homologue el laudo contra las demás partes en el arbitraje. El órgano jurisdiccional debe homologar el laudo a menos que concurra alguno de los motivos de denegación o aplazamiento del reconocimiento o de la ejecución del laudo especificados en el Convenio de Nueva York (*ibidem*, artículo 207). En el capítulo 2 se establece además que las cortes federales distritales estadounidenses tienen jurisdicción para conocer de las acciones o procesos derivados del Convenio de Nueva York, independientemente de la cuantía litigiosa (*ibidem*, artículo 203).
En el capítulo 2 también se establece que se aplica el capítulo 1 a las acciones y procesos contemplados en el capítulo 2 en la medida en que el capítulo 1 no contravenga al capítulo 2 o al Convenio de Nueva York, tal como fue ratificado por los EE. UU. (*ibidem*, artículo 208). A su vez, en el capítulo 1 se dispone que las cláusulas escritas en contratos mercantiles por las que se estipule resolver mediante arbitraje las controversias derivadas de dicho contrato o del negocio jurídico subyacente o la negativa a ejecutar voluntariamente la totalidad o parte de este, así como los acuerdos por escrito por los que las partes se comprometan a someter a arbitraje controversias presentes derivadas de dicho contrato, negocio jurídico o negativa, son válidas y ejecutables por la vía forzosa y no se pueden resolver salvo que existan motivos legales o derivados del principio de equidad para la resolución del contrato (*ibidem*, artículo 2). En el capítulo 1 se dispone además que cualquier parte del arbitraje puede solicitar al órgano jurisdiccional especificado una resolución que homologue el laudo; el órgano jurisdiccional debe dictar tal resolución salvo que el laudo haya sido anulado, modificado o subsanado de conformidad con los artículos 10 y 11 de la Ley federal de arbitraje (*ibidem*, artículo 9).

G. **Procedimiento arbitral**

El Departamento y la Comisión Europea han acordado, de conformidad con el Derecho aplicable, aprobar reglas que rijan el procedimiento de arbitraje del Panel del Marco de Privacidad de Datos UE-EE. UU. ([3]). En caso de que sea necesario modificar dichas reglas, el Departamento y la Comisión Europea deberán acordar la modificación o aprobar un conjunto diferente de procedimientos arbitrales estadounidenses existentes y bien establecidos, según proceda, con sujeción a las consideraciones siguientes:

1. Los particulares podrán solicitar la incoación de un proceso arbitral vinculante siempre que se cumplan los requisitos para el arbitraje antes mencionados, enviando una «notificación» a la entidad. La notificación deberá contener un resumen de las medidas, contempladas en el apartado C, emprendidas para resolver la reclamación, una descripción de la supuesta vulneración y, a discreción del particular, documentos justificativos y demás medios probatorios y/o un análisis de la normativa aplicable a la reclamación en cuestión.

2. Se sustanciará el proceso de tal modo que se garantice que la vulneración objeto de la reclamación por el particular no dé lugar a medidas de reparación o procesos por duplicado.

3. La impugnación ante la Comisión Federal de Comercio podrá sustanciarse de forma paralela al arbitraje.

4. Ningún representante de los EE. UU., de la UE, de un Estado miembro de la UE o de alguna autoridad pública u organismo de garantía del cumplimiento podrá participar en estos arbitrajes, si bien, a petición de los particulares de la UE, las APD podrán ayudarles únicamente a preparar la notificación, pero sin poder consultar el contenido ni ningún otro documento relacionado con estos arbitrajes.

5. El arbitraje se desarrollará en los EE. UU., y el particular podrá elegir participar por videoconferencia o por teléfono, posibilidad que no supondrá coste alguno para el mismo. No se exigirá la participación presencial.

6. El idioma del arbitraje será el inglés, salvo que las partes acuerden lo contrario. Previa solicitud motivada y teniendo en cuenta si el particular está representado por un abogado, se prestará servicio de interpretación en las audiencias arbitrales, así como de traducción de los documentos del arbitraje, sin coste alguno para el particular, salvo que el Panel del Marco de Privacidad de Datos UE-EE. UU. decida que, dadas las circunstancias del arbitraje en concreto, esto supondría un gasto injustificado o desproporcionado.

7. Los documentos y medios probatorios presentados a los árbitros serán tratados confidencialmente y solo se utilizarán en relación con el arbitraje.

8. Si es necesario, podrá autorizarse la revelación de contenido confidencial; dicha información será tratada confidencialmente por las partes y solo se utilizará en relación con el arbitraje.

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

([3]) El Centro Internacional de Resolución de Controversias (International Centre for Dispute Resolution), que es la división internacional de la Asociación Estadounidense de Arbitraje (American Arbitration Association) (denominadas conjuntamente en lo sucesivo «el CIRC y la AEA»), fue seleccionado por el Departamento para gestionar los arbitrajes y administrar el fondo arbitral contemplados en el anexo I de los principios en materia de privacidad. El 15 de septiembre de 2017, el Departamento y la Comisión Europea acordaron aprobar un conjunto de reglas de arbitraje con las que regular los procesos arbitrales vinculantes descritos en el anexo I de los principios en materia de privacidad, así como un código de conducta para los árbitros que sea coherente con las normas éticas generalmente aceptadas para los árbitros mercantiles y con el anexo I de los principios en materia de privacidad. El Departamento y la Comisión Europea acordaron adaptar las reglas de arbitraje y el código de conducta para reflejar las actualizaciones en el Marco de Privacidad de Datos UE-EE. UU., y el Departamento cooperará con el CIRC y la AEA para poner en práctica dichas actualizaciones.

H. **Coste**

Los árbitros deberán tomar medias razonables para minimizar el coste o las tasas de los arbitrajes.

De conformidad con la normativa aplicable, el Departamento facilitará la administración de un fondo al que las entidades participantes deberán aportar en función de, entre otros factores, el tamaño de la entidad; con dicho fondo se sufragará el coste del arbitraje, incluidos los honorarios de los árbitros, hasta ciertos máximos. El fondo lo gestionará un tercero, que informará regularmente al Departamento sobre las operaciones del fondo. El Departamento colaborará periódicamente con el tercero para analizar el funcionamiento del fondo, incluida la necesidad de ajustar el importe de las aportaciones o del importe máximo que sufraga el fondo del coste del arbitraje, y tendrá en cuenta, entre otros aspectos, el número de arbitrajes y el coste y la duración de los arbitrajes, con el entendimiento de que no se deberá imponer una carga económica excesiva a las entidades participantes. El Departamento notificará a la Comisión Europea el resultado de dichos análisis con el tercero y le notificará por adelantado cualquier ajuste del importe de las aportaciones. Los honorarios de los abogados no quedan comprendidos por esta disposición ni por ningún fondo contemplado en esta disposición.

ANEXO II

DEPARTAMENTO DE COMERCIO DE LOS ESTADOS UNIDOS
Secretaria de Comercio
Washington, D.C. 20230

6 de julio de 2023

Excmo. Sr. D. Didier Reynders
Comisario de Justicia
Commission européenne / Europese Commissie
Rue de la Loi / Wetstraat 200
1049 Bruxelles/Brussel
BÉLGICA

Estimado comisario Reynders:

En nombre de los Estados Unidos («EE. UU.»), me complace remitirle el siguiente conjunto de documentos sobre el Marco de Privacidad de Datos UE-EE. UU. que, sumados a el Decreto Presidencial n.º 14086, titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos», y al título 28, parte 201, del Código de Reglamentos Federales, por el que se modifica la normativa del Departamento de Justicia para crear el Tribunal de Recurso en Materia de Protección de Datos, son el resultado de las negociaciones importantes y minuciosas llevadas a cabo para reforzar las garantías de la privacidad y las libertades civiles. El resultado de dichas negociaciones ha sido una serie de garantías con las que asegurar que las actividades de inteligencia de señales estadounidenses sean necesarias y proporcionadas para cumplir los objetivos de seguridad nacional que se fijen, así como un nuevo procedimiento para que los particulares de la Unión Europea («UE») puedan solicitar reparación si consideran que han sido objeto de actividades ilícitas de inteligencia de señales, que conjuntamente garantizarán la privacidad de los datos personales de la UE. El Marco de Privacidad de Datos UE-EE. UU. sustentará una economía digital inclusiva y competitiva. Debemos sentirnos orgullosos de las mejoras que se han plasmado en dicho Marco, que reforzarán la protección de la privacidad en todo el mundo. Estos documentos, junto con el Decreto Presidencial, las disposiciones del Código de Reglamentos Federales y otros documentos de acceso público, proporcionan una base muy sólida para que la Comisión Europea pueda de nuevo adoptar una decisión de adecuación ([1]).

Se adjuntan los documentos siguientes:

— los principios del Marco de Privacidad de Datos UE-EE. UU., así como los principios complementarios (denominados conjuntamente «los principios en materia de privacidad») y el anexo I de los principios en materia de privacidad (anexo que fija el régimen que las entidades participantes están obligadas a seguir al arbitrar ciertas reclamaciones no resueltas respecto de los datos personales amparados por los principios en materia de privacidad);

— una carta de la Administración de Comercio Internacional, adscrita al Departamento y que administra el programa del Marco de Privacidad de Datos, en la que se describen los compromisos que asume nuestro Departamento para garantizar el funcionamiento eficaz del Marco de Privacidad de Datos UE-EE. UU.;

— una carta de la Comisión Federal de Comercio en la que se describen sus competencias de garantía del cumplimiento respecto de los principios en materia de privacidad;

— una carta del Departamento de Transporte en la que se describen sus competencias de garantía del cumplimiento respecto de los principios en materia de privacidad;

— una carta de la Oficina del Director de Inteligencia Nacional sobre las garantías y limitaciones aplicables a las autoridades de seguridad nacional estadounidenses; y

— una carta del Departamento de Justicia sobre las garantías y las limitaciones aplicables al acceso a los datos por parte del Ejecutivo estadounidense a efectos policiales o en aras del interés público.

([1]) Dado que la Decisión de la Comisión relativa a la adecuación de la protección conferida en el Marco de Privacidad de Datos UE-EE. UU. es de aplicación a Islandia, Liechtenstein y Noruega, el Marco de Privacidad de Datos UE-EE. UU. abarcará tanto a la UE como a estos tres países.

Todo el conjunto de documentos relativos al Marco de Privacidad de Datos UE-EE. UU. se publicará en el sitio web del Departamento sobre el Marco de Privacidad de Datos, y los principios en materia de privacidad y el anexo I de dichos principios entrarán en vigor en la fecha de entrada en vigor de la decisión de adecuación de la Comisión Europea.

Puede estar seguro de que los EE. UU. asumen estos compromisos con la máxima seriedad. Esperamos poder seguir colaborando con usted a medida que se ponga en práctica el Marco de Privacidad de Datos UE-EE. UU. y cuando nos embarquemos juntos en la siguiente fase de este proceso.

Atentamente,

Gina M. Raimondo

ANEXO III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12 de diciembre de 2022

Excmo. Sr. D. Didier Reynders
Comisario de Justicia
Commission européenne / Europese Commissie
Rue de la Loi / Wetstraat 200
1049 Bruxelles/Brussel
BÉLGICA

Estimado comisario Reynders:

En nombre de la Administración de Comercio Internacional, me complace comunicarle los compromisos asumidos por el Departamento de Comercio («Departamento») para garantizar la protección de los datos personales merced a su administración y supervisión del programa del Marco de Privacidad de Datos. La ultimación del Marco de Privacidad de Datos UE-EE. UU. es un logro importante para la privacidad y para las empresas a ambos lados del Atlántico, ya que dará a los particulares de la UE la confianza en que sus datos estarán protegidos y en que tendrán vías de impugnación para articular las preocupaciones relacionadas con sus datos; por otro lado, posibilitará que miles de empresas sigan realizando inversiones y actividades comerciales transatlánticas que aprovechen a nuestras respectivas economías y ciudadanos. El Marco de Privacidad de Datos UE-EE. UU. es el reflejo de años de arduo trabajo y colaboración con usted y con sus compañeros de la Comisión Europea. Esperamos poder seguir colaborando con la Comisión para garantizar que este esfuerzo conjunto produzca los resultados queridos.

El Marco de Privacidad de Datos UE-EE. UU. traerá considerables ventajas tanto para los particulares como para las empresas. En primer lugar, ofrece un conjunto destacado de garantías de la privacidad de los datos de los particulares de la UE transferidos a los EE. UU. Exige que las entidades estadounidenses participantes: elaboren directrices en materia privacidad que respeten el Marco de Privacidad de Datos UE-EE. UU.; se comprometan públicamente a cumplir los principios del Marco de Privacidad de Datos UE-EE. UU., así como los principios complementarios (denominados conjuntamente «los principios en materia de privacidad») y el anexo I de los principios en materia de privacidad (anexo que fija el régimen que las entidades participantes están obligadas a seguir al arbitrar ciertas reclamaciones no resueltas respecto de los datos personales amparados por los principios en materia de privacidad), de modo que el compromiso sea exigible por la vía de la ejecución forzosa en virtud del Derecho estadounidense ([1]); revaliden cada año la certificación de su cumplimiento ante el Departamento; ofrezcan a los particulares de la UE un servicio de resolución de las controversias gratuito e independiente; y se sometan a las competencias de investigación y ejecución forzosa de los organismos legales estadounidenses enumerados en los principios en materia de privacidad (la Comisión Federal de Comercio y el Departamento de Transporte) o de los organismos legales estadounidenses enumerados en un futuro anexo de dichos principios. Si bien autocertificarse es completamente voluntario, una vez que la entidad se compromete públicamente a cumplir el Marco de Privacidad de Datos UE-EE. UU., su compromiso pasa a ser exigible por la vía de la ejecución forzosa

([1]) Las entidades que autocertificaron su compromiso de cumplir los principios marco del Escudo de la privacidad UE-EE. UU. y quieran acogerse al Marco de Privacidad de Datos UE-EE. UU. deben cumplir los «principios del Marco de Privacidad de Datos UE-EE. UU.». Este compromiso de cumplir los principios del Marco de Privacidad de Datos UE-EE. UU. tiene que plasmarse en las directrices en materia privacidad de dichas entidades participantes lo antes posible y, en cualquier caso, a más tardar tres meses después de la fecha de entrada en vigor de los principios del Marco de Privacidad de Datos UE-EE. UU. (véase la letra e del principio complementario sobre la autocertificación).

en virtud del Derecho estadounidense por la Comisión Federal de Comercio, el Departamento de Transporte u otro organismo legal estadounidense, dependiendo de cuál tenga competencia en relación con la entidad participante. En segundo lugar, el Marco de Privacidad de Datos UE-EE. UU. permitirá que las empresas estadounidenses, incluidas las filiales de empresas europeas radicadas en los EE. UU., reciban datos personales de la UE y con ello se facilitará la circulación de datos que contribuye al comercio transatlántico. La circulación de datos entre los EE. UU. y la UE es, numéricamente, de las mayores del mundo y sustenta la relación económica entre los EE. UU. y la UE, que asciende a 7,1 billones USD y está detrás de millones de puestos de trabajo a ambos lados del Atlántico. Las empresas que se basan en la circulación transatlántica de datos pertenecen a todo tipo de sectores y, entre ellas, se cuentan las principales empresas de la lista Fortune 500, así como muchas pymes. La circulación transatlántica de los datos permite que las entidades estadounidenses puedan tratar los datos necesarios para ofertar bienes y servicios y brindar oportunidades laborales a los particulares europeos.

El Departamento se ha comprometido a colaborar estrechamente y de manera productiva con nuestros homólogos de la UE para administrar y supervisar eficazmente el programa del Marco de Privacidad de Datos. Este compromiso se traduce en el desarrollo y la mejora continua por parte del Departamento de una serie de recursos para ayudar a las entidades con el proceso de autocertificación, la creación de un sitio web para proporcionar información específica a las partes interesadas, la cooperación con la Comisión Europea y las autoridades de protección de datos europeas («APD») para elaborar guías que aclaren los elementos importantes del Marco de Privacidad de Datos UE-EE. UU., las actividades de divulgación para que se comprendan mejor las obligaciones de las entidades en materia de protección de datos, y la supervisión y la garantía del cumplimiento por parte de las entidades de los requisitos del programa.

La cooperación que hemos venido desarrollando con nuestros estimados homólogos de la UE permitirá al Departamento garantizar que el Marco de Privacidad de Datos UE-EE. UU. funcione eficazmente. El Ejecutivo estadounidense tiene un largo historial de colaboración con la Comisión Europea de promoción de los principios compartidos sobre la protección de los datos; merced a esta colaboración hemos superado las diferencias de nuestros respectivos ordenamientos jurídicos y fomentado al mismo tiempo el comercio y el crecimiento económico en la UE y los EE. UU. Creemos que el Marco de Privacidad de Datos UE-EE. UU., que es un ejemplo de esta cooperación, reúne los requisitos para que la Comisión Europea pueda adoptar una nueva decisión de adecuación que permita a las entidades acogerse al Marco para transferir datos personales de la UE a los EE. UU. respetando el Derecho de la UE.

Administración y supervisión del programa del Marco de Privacidad de Datos por parte del Departamento de Comercio

El Departamento se compromete firmemente a administrar y supervisar eficazmente el programa del Marco de Privacidad de Datos y tomará las medidas necesarias y consignará recursos adecuados para garantizar ese resultado. Publicará y mantendrá actualizada la lista oficial de las entidades estadounidenses que se hayan autocertificado ante el Departamento y hayan declarado su compromiso de cumplir los principios en materia de privacidad («lista del Marco de Privacidad de Datos»), y la actualizará en función de los expedientes de revalidación anual de la certificación que presenten las entidades participantes, y de las entidades que se den de baja voluntariamente, no realicen la revalidación anual de su certificación de conformidad con los procedimientos del Departamento o incumplan sistemáticamente dichos principios. También publicará y mantendrá actualizado el registro oficial de las entidades estadounidenses que ya no formen parte de la lista del Marco de Privacidad de Datos, con indicación en cada caso del motivo de dicha eliminación. La lista y el registro oficiales antes mencionados serán de consulta pública en el sitio web del Departamento sobre el Marco de Privacidad de Datos. Dicho sitio web incluirá una explicación destacada que indique que las entidades eliminadas de la lista del Marco de Privacidad de Datos no podrán declarar que participan en el Marco de Privacidad de Datos UE-EE. UU., que lo cumplen o que pueden recibir información personal de conformidad con dicho Marco. No obstante, tales entidades deben seguir aplicando los principios en materia de privacidad a la información personal que hayan recibido cuando aún participaban en el Marco de Privacidad de Datos UE-EE. UU. mientras conserven dicha información. El Departamento, en aras de su compromiso integral y continuado con la administración y supervisión eficaces del programa del Marco de Privacidad de Datos, se encargará específicamente de lo siguiente:

Verificar los requisitos para la autocertificación

— El Departamento, antes de dar por concluida la autocertificación inicial o la revalidación anual de la certificación por parte de la entidad (denominadas conjuntamente, «autocertificación») y de incluir o mantener a la entidad en la lista del Marco de Privacidad de Datos, verificará que la entidad ha cumplido, como mínimo, los requisitos pertinentes establecidos en el principio complementario sobre la autocertificación en relación con la información que la entidad deba aportar en el expediente de autocertificación que presente al Departamento y que ha presentado en el momento oportuno unas directrices en materia de privacidad pertinentes que informen a los particulares de los trece elementos enumerados en el principio de notificación. El Departamento verificará que la entidad:

— ha especificado la entidad que presenta el expediente de autocertificación, así como cualquier filial o sucursal estadounidense de la entidad que se autocertifica que también se compromete a cumplir los principios en materia de privacidad y a la que la entidad desea extender su autocertificación;

— ha aportado la información de contacto exigida de la entidad (por ejemplo, información de contacto de personas u oficinas específicas dentro de la entidad que se autocertifica responsables de tramitar las reclamaciones, las solicitudes de acceso y cualquier otra cuestión que surja en relación con el Marco de Privacidad de Datos UE-EE. UU.);

— ha especificado las finalidades para las que la entidad pretende recoger y utilizar la información personal recibida de la UE;

— ha indicado qué información personal pretende recibir de la UE en el Marco de Privacidad de Datos UE-EE. UU. y, por lo tanto, estaría cubierta por su autocertificación;

— si la entidad dispone de un sitio web público, ha proporcionado la dirección web en la que las directrices en materia de privacidad pertinentes se pueden consultar o, si la entidad no dispone de un sitio web público, ha proporcionado al Departamento una copia de las directrices en materia de privacidad pertinentes y ha puesto a disposición de los particulares afectados dichas directrices en materia de privacidad (es decir, los empleados afectados, si las directrices en materia de privacidad pertinentes son directrices de privacidad del ámbito de los recursos humanos, o cualquier persona, si las directrices en materia de privacidad pertinentes no son directrices de privacidad del ámbito de los recursos humanos);

— ha incluido en sus directrices en materia de privacidad pertinentes en el momento oportuno (es decir, inicialmente solo en el proyecto de directrices aportado en el expediente presentado para la autocertificación inicial; en caso contrario, en las directrices en materia de privacidad definitivas y, cuando proceda, publicadas) la declaración de que cumple los principios en materia de privacidad y enlace al sitio web del Departamento sobre el Marco de Privacidad de Datos (por ejemplo, la página de inicio o el sitio web de la lista del Marco de Privacidad de Datos);

— ha incluido en sus directrices en materia de privacidad pertinentes en el momento oportuno los doce elementos enumerados en el principio de notificación (por ejemplo, la posibilidad, en determinadas condiciones, de que el particular de la UE afectado solicite la incoación de un proceso arbitral vinculante; la obligación de comunicar la información personal en respuesta a solicitudes lícitas de los poderes públicos, en particular con fines de seguridad nacional o policiales; y su responsabilidad en casos de transferencias ulteriores a terceros);

— ha indicado el organismo legal pertinente que tenga competencia para conocer de las reclamaciones contra la entidad por posibles prácticas desleales o engañosas y por el incumplimiento de las leyes o reglamentos en materia de privacidad (y que debe figurar en los principios en materia de privacidad o en un futuro anexo de dichos principios);

— ha indicado el nombre de cualquier programa de privacidad en el que la entidad participe;

— ha indicado si el método pertinente (es decir, los procedimientos de seguimiento que debe establecer) para verificar su cumplimiento de los principios en materia de privacidad es la «autoevaluación» (es decir, la verificación interna) o la «verificación externa» (es decir, la realizan terceros) y, si se indicó que el método pertinente es la verificación externa, ha indicado también el tercero que ha realizado dicha verificación externa;

— ha indicado el órgano independiente de impugnación adecuado para tramitar las reclamaciones presentadas en relación con los principios en materia de privacidad sin coste para el particular afectado:

  — si la entidad ha seleccionado como órgano independiente de impugnación un organismo de resolución alternativa de controversias del sector privado, ha incluido en sus directrices en materia de privacidad pertinentes un enlace o la dirección web del correspondiente sitio web o formulario de reclamación del organismo para investigar las reclamaciones no resueltas presentadas en relación con los principios en materia de privacidad;

  — si la entidad está obligada (es decir, con respecto a los datos de recursos humanos transferidos desde la UE en el marco de la relación laboral) a cooperar con las APD pertinentes en la investigación y resolución de las reclamaciones presentadas en relación con los principios en materia de privacidad o, si decide hacerlo *motu proprio*, ha declarado su compromiso de cooperar con las APD y que cumplirá el dictamen correspondiente de tomar medidas específicas para cumplir los principios.

— El Departamento también verificará que el expediente de autocertificación que presenten las entidades es coherente con sus directrices en materia de privacidad pertinentes. Cuando las entidades que se autocertifiquen deseen extender su autocertificación a filiales o sucursales estadounidenses suyas que tengan directrices en materia privacidad propias y pertinentes, el Departamento revisará también las directrices en materia privacidad pertinentes de dichas filiales o sucursales para asegurarse de que incluyan todos los elementos exigidos por el principio de notificación.

— El Departamento colaborará con los organismos legales correspondientes (por ejemplo, la Comisión Federal de Comercio y el Departamento de Transporte) para verificar que las entidades están realmente sujetas a la competencia del organismo legal pertinente indicado en el expediente de autocertificación, cuando el Departamento vea indicios para dudar de que estén sujetas a la competencia de ese organismo.

— El Departamento colaborará con los organismos de resolución alternativa de controversias del sector privado para verificar que las entidades están dadas de alta realmente antes esos organismos indicados en sus expediente de autocertificación como órgano independiente de impugnación; también colaborará con dichos organismos para verificar que las entidades están dadas de alta realmente para la verificación externa del cumplimiento indicada en sus expediente de autocertificación, cuando dichos organismos puedan ofrecer ambos tipos de servicios.

— El Departamento colaborará con el tercero seleccionado por el Departamento para actuar como depositario de los fondos recaudados a través de la tasa del panel de la APD (es decir, la tasa anual destinada a sufragar el coste de funcionamiento del panel de la APD) para verificar que las entidades han pagado la tasa del año correspondiente, cuando las entidades hayan indicado a las APD como el órgano independiente de impugnación pertinente.

— El Departamento colaborará con el tercero seleccionado por el Departamento para gestionar los arbitrajes y administrar el fondo arbitral contemplados en el anexo I de los principios en materia de privacidad, a fin de verificar que las entidades han contribuido a dicho fondo arbitral.

— Cuando el Departamento detecte algún problema durante su revisión de los expedientes de autocertificación de las entidades, les informará de que deben resolver esos problemas en el plazo razonable que fije el Departamento ([2]). El Departamento también les informará de que la falta de respuesta dentro de los plazos fijados por el Departamento o cualquier otro incumplimiento de la obligación de completar su autocertificación de conformidad con los procedimientos del Departamento tendrá como consecuencia que se entiendan desistidas dichas autocertificaciones, y de que cualquier engaño sobre la participación de la entidad en el Marco de Privacidad de Datos UE-EE. UU. o sobre su cumplimiento puede desencadenar actuaciones de garantía del cumplimiento por parte de la Comisión Federal de Comercio, el Departamento de Transporte u otro organismo público pertinente. El Departamento informará a las entidades a través de los medios de contacto que estas le hayan comunicado.

Facilitar la cooperación con los organismos de resolución alternativa de controversias que prestan servicios relacionados con los principios en materia de privacidad

— El Departamento colaborará con los organismos de resolución alternativa de controversias del sector privado que ejerzan de órganos independientes de impugnación, a los que se puede acudir para que investiguen las reclamaciones no resueltas en relación con los principios en materia de privacidad, para verificar que cumplen, como mínimo, los requisitos derivados del principio complementario sobre la resolución de controversias y la ejecución forzosa. El Departamento verificará lo siguiente.

  — Que incluyen información en sus sitios web públicos sobre los principios en materia de privacidad y los servicios que prestan en el Marco de Privacidad de Datos UE-EE. UU., que debe incluir: 1) información sobre los requisitos de los principios en materia de privacidad relativos a los órganos independientes de impugnación, o un enlace a ellos; 2) un enlace al sitio web del Departamento sobre el Marco de Privacidad de Datos; 3) la explicación de que sus servicios de resolución de controversias en el Marco de Privacidad de Datos UE-EE. UU. son gratuitos para los particulares; 4) la descripción de cómo pueden presentarse las reclamaciones relacionadas con los principios en materia de privacidad; 5) el plazo de tramitación de las reclamaciones relacionadas con dichos principios; 6) la descripción de todas las vías de reparación posibles. El Departamento notificará oportunamente a dichos organismos los cambios sustanciales en materia de supervisión y administración por parte del Departamento del programa del Marco de Privacidad de Datos cuando tales cambios sean inminentes o ya se hayan realizado y sean relevantes para la función que desempeñan esos organismos en el Marco de Privacidad de Datos UE-EE. UU.

([2]) Por ejemplo, por lo que se refiere a la revalidación de la certificación, se espera que las entidades resuelvan esos problemas en un plazo de cuarenta y cinco días; el Departamento puede fijar un plazo diferente si lo considera adecuado.

— Que publican un informe anual con estadísticas agregadas sobre sus servicios de resolución de controversias, que debe incluir: 1) el número total de reclamaciones relacionadas con los principios en materia de privacidad que se hayan recibido durante el año de referencia; 2) la naturaleza de las reclamaciones recibidas; 3) las medidas tomadas respecto de la calidad de la solución de controversias, como, por ejemplo, la duración de la tramitación de las reclamaciones; y 4) el resultado de las reclamaciones tramitadas, a saber, el número y el tipo de medidas de reparación dictadas o de sanciones impuestas. El Departamento dará a dichos organismos instrucciones específicas y complementarias sobre la información que deben proporcionar en los informes anuales que elaboren para dar cumplimiento a los requisitos (por ejemplo, enumerando los criterios específicos que deben cumplir las reclamaciones para ser consideradas una reclamación relacionada con los principios en materia de privacidad a efectos del informe anual), con indicación de otro tipo de información que deben proporcionar (por ejemplo, si el organismo también presta servicios de verificación relacionados con los principios en materia de privacidad, la explicación de cómo evita cualquier conflicto de intereses real o potencial en situaciones en las que presta a una misma entidad tanto servicios de verificación como servicios de resolución de controversias). Las instrucciones adicionales del Departamento también especificarán la fecha en la que los informes anuales de los organismos deben publicarse para el período de referencia pertinente.

Colaborar con las entidades que quieran darse de baja o que hayan sido eliminadas de la lista del Marco de Privacidad de Datos

— Si la entidad quiere darse de baja en el Marco de Privacidad de Datos UE-EE. UU., el Departamento le exigirá que elimine de sus directrices en materia de privacidad pertinentes toda referencia al Marco que insinúe que continúa participando en el Marco y que puede recibir datos personales de conformidad con el Marco (véase la descripción del compromiso del Departamento de detectar las declaraciones falsas de participación). El Departamento también exigirá a la entidad que cumplimente y envíe al Departamento un cuestionario adecuado para verificar:

  — su intención de darse de baja;

  — qué hará con los datos personales que recibió en el Marco de Privacidad de Datos UE-EE. UU. mientras participó en este: a) conservar dichos datos, seguir aplicándoles los principios en materia de privacidad y declarar anualmente al Departamento su compromiso de seguir aplicando los principios a dichos datos; b) conservar dichos datos y conferir una protección «adecuada» a dichos datos por otros medios autorizados; o c) devolver o suprimir dichos datos en una fecha determinada; y

  — quién, dentro de la entidad, ejercerá de punto de contacto permanente para las cuestiones relacionadas con los principios en materia de privacidad.

— Si la entidad escogió la opción a), el Departamento también le pedirá que cumplimente y envíe al Departamento anualmente desde que se dé de baja (es decir, antes del primer aniversario de su baja, así como cada aniversario posterior, a menos que la entidad confiera una protección «adecuada» a dichos datos por otros medios autorizados o devuelva o suprima dichos datos y lo notifique al Departamento) un cuestionario adecuado para verificar lo que ha hecho con esos datos personales, qué hará con cualquiera de esos datos personales que siga conservando y quién, dentro de la entidad, ejercerá de punto de contacto permanente para las cuestiones relacionadas con los principios en materia de privacidad.

— Si la entidad ha dejado vencer su autocertificación (es decir, no ha realizado la revalidación anual de su certificación de cumplimiento de los principios en materia de privacidad, ni ha sido eliminada de la lista del Marco de Privacidad de Datos por alguna otra razón, como la baja voluntaria), el Departamento le pedirá que cumplimente y envíe al Departamento un cuestionario adecuado para verificar si quiere darse de baja o revalidar su certificación:

  — y, si quiere darse de baja, verificará qué hará con los datos personales que recibió en el Marco de Privacidad de Datos UE-EE. UU. mientras participó en este (véase la descripción anterior de lo que las entidades deben verificar si quieren darse de baja);

  — y, si tiene la intención de revalidar su certificación, verificar que, durante el tiempo en que estuvo vencida su certificación, aplicó los principios en materia de privacidad a los datos personales recibidos en el Marco de Privacidad de Datos UE-EE. UU. y aclarar qué medidas tomará para resolver las cuestiones pendientes que han retrasado la revalidación de su certificación.

— Si la entidad es eliminada de la lista del Marco de Privacidad de Datos por alguna de las razones siguientes: a) baja voluntaria del Marco de Privacidad de Datos UE-EE. UU., b) no haber completado la revalidación anual de la certificación de su cumplimiento de los principios en materia de privacidad (es decir, bien porque inició el trámite, pero no lo completó a su debido tiempo, bien porque nunca lo inició); o c) «incumplimiento sistemático»; el Departamento enviará una notificación a los contactos indicados en el expediente de autocertificación de la entidad en la que se especifique el motivo de su eliminación y se explique que debe dejar de declarar explícita o implícitamente que participa en el Marco de Privacidad de Datos UE-EE. UU. o lo cumple y que puede recibir datos personales en el Marco. La notificación, que también podrá incluir otra información adaptada al motivo de la eliminación, indicará que las entidades que representen falsamente su participación en el Marco de Privacidad de Datos UE-EE. UU., especialmente cuando den a entender que participan en el Marco tras haber sido eliminadas de la lista del Marco de Privacidad de Datos, podrán ser objeto de medidas coercitivas por parte de la Comisión Federal de Comercio, el Departamento de Transporte u otro organismo público pertinente.

Detectar y corregir las declaraciones falsas de participación

— De forma continuada, cuando la entidad: a) se dé de baja voluntariamente en el Marco de Privacidad de Datos UE-EE. UU., b) no haya completado la revalidación anual de la certificación de su cumplimiento de los principios en materia de privacidad (es decir, bien porque inició el trámite, pero no lo completó a su debido tiempo, bien porque nunca lo inició); c) sea eliminada del Marco por su «incumplimiento sistemático»; o d) no haya completado la autocertificación inicial de su cumplimiento de los principios (es decir, porque inició el trámite, pero no lo completó a su debido tiempo); el Departamento tomará de oficio medidas para verificar que las directrices en materia de privacidad pertinentes publicadas por la entidad no contienen referencias al Marco que insinúen que participa en el Marco y que puede recibir datos personales de conformidad con el Marco. En caso de que el Departamento constate que estas referencias no han sido eliminadas, informará a la entidad de que, si procede, remitirá el asunto al organismo pertinente para que tome las medidas oportunas si la entidad continúa declarando con engaño que participa en el Marco de Privacidad de Datos UE-EE. UU. El Departamento informará a la entidad a través de los medios de contacto que esta le haya comunicado o, cuando proceda, a través de otros medios. En caso de que la entidad no elimine las referencias ni autocertifique su cumplimiento del Marco de Privacidad de Datos UE-EE. UU. de conformidad con los procedimientos del Departamento, este remitirá de oficio el asunto a la Comisión Federal de Comercio, al Departamento de Transporte o a cualquier otro organismo de garantía del cumplimiento competente o, cuando proceda, tomará las medidas necesarias para garantizar que se utilice correctamente la marca de certificación del Marco de Privacidad de Datos UE-EE. UU.

— El Departamento tomará medidas para detectar las declaraciones falsas sobre la participación en el Marco de Privacidad de Datos UE-EE. UU. y el uso indebido de la marca de certificación del Marco, especialmente por parte de entidades que, a diferencia de las descritas antes, nunca han iniciado el proceso de autocertificación (por ejemplo, realizando búsquedas específicas en internet para hallar referencias al Marco en las directrices en materia privacidad de las entidades). Cuando, con estas medidas, el Departamento detecte declaraciones falsas de participación en el Marco de Privacidad de Datos UE-EE. UU. y usos indebidos de la marca de certificación del Marco, informará a la entidad de que, si procede, remitirá el asunto al organismo pertinente para que tome las medidas oportunas si la entidad continúa declarando con engaño que participa en el Marco. El Departamento informará a la entidad a través de los medios de contacto que, en su caso, esta le haya comunicado o, cuando proceda, a través de otros medios. En caso de que la entidad no elimine las referencias ni autocertifique su cumplimiento del Marco de Privacidad de Datos UE-EE. UU. de conformidad con los procedimientos del Departamento, este remitirá de oficio el asunto a la Comisión Federal de Comercio, al Departamento de Transporte o a cualquier otro organismo de garantía del cumplimiento competente o, cuando proceda, tomará las medidas necesarias para garantizar que se utilice correctamente la marca de certificación del Marco de Privacidad de Datos UE-EE. UU.

— El Departamento revisará y tramitará sin demora las reclamaciones específicas y no insustanciales sobre las declaraciones falsas de participación en el Marco de Privacidad de Datos UE-EE. UU. que reciba (por ejemplo, las reclamaciones recibidas de las APD, los organismos de resolución alternativa de controversias del sector privado que actúen como órganos independientes de impugnación, los interesados, las empresas de la UE y de los EE. UU. y otros tipos de terceros).

— El Departamento podrá tomar otras medidas correctoras adecuadas. Los engaños en la información transmitida al Departamento podrán ser punibles en el marco de la Ley de declaraciones falsas (título 18, artículo 1001, del Código de Estados Unidos).

Realizar de oficio revisiones y evaluaciones periódicas del cumplimiento del programa del Marco de Privacidad de Datos

— De forma continuada, el Departamento tratará de supervisar el cumplimiento efectivo por parte de las entidades del Marco de Privacidad de Datos UE-EE. UU. a fin de detectar problemas que puedan justificar medidas de seguimiento. En particular, el Departamento llevará a cabo, de oficio, inspecciones sin aviso rutinarias de entidades participantes seleccionadas aleatoriamente, así como inspecciones sin aviso *ad hoc* de entidades participantes específicas cuando se detecten posibles deficiencias en el cumplimiento (por ejemplo, las puestas en conocimiento del Departamento por terceros) para verificar: a) que el punto o puntos de contacto responsables de la tramitación de las reclamaciones, las solicitudes de acceso y otras cuestiones que surjan en el Marco de Privacidad de Datos UE-EE. UU. están disponibles; b) cuando proceda, que las directrices en materia de privacidad públicas de la entidad se pueden visualizar sin restricciones tanto en el sitio web público de la entidad como a través de un enlace en la lista del Marco de Privacidad de Datos; c) que las directrices en materia de privacidad de la entidad siguen cumpliendo los requisitos para la autocertificación descritos en los principios en materia de privacidad; y d) que el órgano independiente de impugnación indicado por la entidad está disponible para conocer de las reclamaciones relacionadas con el Marco de Privacidad de Datos UE-EE. UU. El Departamento también hará un seguimiento proactivo de las noticias para buscar denuncias de las que se desprendan indicios creíbles de incumplimiento por parte de las entidades participantes.

— Como parte de su labor de garantía del cumplimiento, el Departamento exigirá a las entidades participantes que cumplimenten y envíen al Departamento el cuestionario pormenorizado cuando: a) el Departamento reciba reclamaciones específicas y no insustanciales sobre el cumplimiento de Marco de Privacidad de Datos UE-EE. UU. por parte de la entidad; b) la entidad no responda satisfactoriamente a las solicitudes del Departamento respecto de información relacionada con el Marco; o c) haya indicios creíbles de que la entidad no cumple sus compromisos en el Marco de Privacidad de Datos UE-EE. UU. Cuando el Departamento haya enviado el cuestionario pormenorizado a la entidad y esta no lo responda satisfactoriamente, informará a la entidad de que, si procede, remitirá el asunto al organismo competente para que tome las medidas oportunas si el Departamento no recibe una respuesta oportuna y satisfactoria de la entidad. El Departamento informará a la entidad a través de los medios de contacto que esta le haya comunicado o, cuando proceda, a través de otros medios. Si la entidad no responde oportuna y satisfactoriamente, el Departamento remitirá el asunto de oficio a la Comisión Federal de Comercio, al Departamento de Transporte o a cualquier otro organismo de garantía del cumplimiento competente o tomará las medidas necesarias para garantizar el cumplimiento. Cuando sea necesario, el Departamento consultará a las autoridades competentes de protección de datos sobre estas revisiones del cumplimiento.

— El Departamento evaluará periódicamente la administración y la supervisión del programa del Marco de Privacidad de Datos para garantizar que su labor de seguimiento, incluida la realizada con herramientas de búsqueda (por ejemplo, para comprobar si han dejado de funcionar los enlaces a las directrices en materia de privacidad de las entidades participantes), es adecuada para tratar los problemas existentes y cualquier problema nuevo que surja.

Adaptar el sitio web del Marco de Privacidad de Datos al público destinatario

El Departamento adaptará el sitio web del Marco de Privacidad de Datos para centrarse en los públicos destinatarios siguientes: particulares de la UE, empresas de la UE, empresas estadounidenses y APD. La inclusión de material especialmente destinado a los particulares de la UE y a las empresas de la UE facilitará la transparencia en muchos aspectos. Por lo que se refiere a los particulares de la UE, el sitio web explicará claramente: 1) los derechos que otorga el Marco de Privacidad de Datos UE-EE. UU. a los particulares de la UE; 2) los órganos de impugnación a los que los particulares de la UE pueden acudir cuando crean que la entidad vulnera su compromiso de cumplir con los principios en materia de privacidad; y 3) cómo buscar la información sobre la autocertificación de la entidad a efectos del Marco de Privacidad de Datos UE-EE. UU. Por lo que se refiere a las empresas de la UE, facilitará la verificación de: 1) si la entidad participa en el Marco de Privacidad de Datos UE-EE. UU.; 2) el tipo de información amparada por la autocertificación de la entidad a efectos del Marco; 3) las directrices en materia de privacidad que se aplican a la información amparada; y 4) el método que utiliza la entidad para verificar su cumplimiento de los principios en materia de privacidad. Por lo que se refiere a los particulares estadounidenses, explicará claramente: 1) las ventajas de la participación en el Marco de Privacidad de Datos UE-EE. UU.; 2) cómo participar en el Marco, así como el proceso para revalidar la certificación y para darse de baja en el Marco; y 3) cómo administran los EE. UU. el Marco y cómo velan por su cumplimiento. La inclusión de material especialmente destinado a las APD (por ejemplo, información sobre el punto de contacto específico del Departamento para las APD y un enlace al contenido relacionado con los principios en materia de privacidad que figura en el sitio web de la Comisión Federal de Comercio) facilitará tanto la cooperación como la transparencia. El Departamento también colaborará sobre una base *ad hoc* con la Comisión Europea y el Comité Europeo de Protección de Datos para desarrollar material de interés adicional (por ejemplo, respuestas a preguntas frecuentes) para su uso en el sitio web del Marco de Privacidad de Datos, que facilitará la administración y supervisión eficientes del programa del Marco de Privacidad de Datos.

Facilitar la cooperación con las APD

Para incrementar las oportunidades de cooperación con las APD, el Departamento nombrará un punto de contacto específico para actuar de enlace con las APD. En los casos en que la APD crea que una entidad participante no está cumpliendo los principios en materia de privacidad, en particular a raíz de una reclamación de un particular de la UE, la APD podrá dirigirse al punto de contacto nombrado por el Departamento para solicitar un control más pormenorizado de la entidad. El Departamento hará todo cuanto esté en su mano para facilitar la resolución de la reclamación con la entidad participante. En el plazo de los noventa días siguientes a la recepción de la reclamación, el Departamento informará a la APD de los avances realizados. El punto de contacto también recibirá las remisiones que se le remitan relativas a entidades que declaren falsamente participar en el Marco de Privacidad de Datos UE-EE. UU. Llevará un registro de todas las reclamaciones remitidas por las APD al Departamento, y este incluirá, en la revisión conjunta que se describe a continuación, un informe en el que se analice el conjunto de las reclamaciones recibidas cada año. El punto de contacto colaborará con las APD en la búsqueda de información relacionada con la autocertificación de la entidad en concreto o con su anterior participación en el Marco de Privacidad de Datos UE-EE. UU. y responderá a las consultas de las APD relacionadas con el cumplimiento de los requisitos específicos del Marco. El Departamento también cooperará con la Comisión Europea y el Comité Europeo de Protección de Datos en los aspectos procesales y administrativos del panel de la APD, especialmente el establecimiento de procedimientos adecuados para la distribución de los fondos recaudados con la tasa del panel de la APD. Entendemos que la Comisión Europea colaborará con el Departamento para facilitar la resolución de cualquier cuestión que pueda surgir en relación con dichos procedimientos. Por otra parte, el Departamento proporcionará a las APD material relacionado con el Marco de Privacidad de Datos UE-EE. UU. para que lo incluyan en sus propios sitios webs con el fin de aumentar la transparencia para los particulares y las empresas de la UE. Que haya un mejor conocimiento del Marco de Privacidad de Datos UE-EE. UU. y los derechos y responsabilidades que comporta debería facilitar la detección de los problemas que puedan surgir, a fin de poder resolverlos adecuadamente.

Cumplir las obligaciones que le impone el anexo I de los principios en materia de privacidad

El Departamento cumplirá los compromisos derivados del anexo I de los principios en materia de privacidad, en particular administrar la lista de árbitros elegidos, de consuno con la Comisión Europea, por su independencia, integridad y conocimientos especializados; también ayudará, según proceda, al tercero seleccionado por el Departamento para gestionar los arbitrajes y administrar el fondo arbitral contemplados en el anexo I de los principios en materia de privacidad ([3]). El Departamento colaborará con el tercero para verificar, entre otros aspectos, que este cuenta con un sitio web con aclaraciones sobre el procedimiento de arbitraje, que deben explicar: 1) cómo incoar el proceso y presentar los documentos; 2) la lista de árbitros publicada por el Departamento y cómo seleccionar a los árbitros de dicha lista; 3) el procedimiento arbitral y el código de conducta de los árbitros aprobados por el Departamento y la Comisión Europea ([4]); y 4) la recaudación de la tasa y el pago de los honorarios de los árbitros. Además, el Departamento colaborará periódicamente con el tercero para analizar el funcionamiento del fondo arbitral, incluida la necesidad de ajustar el importe de las aportaciones o del importe máximo que sufraga el fondo del coste del arbitraje, y tendrá en cuenta, entre otros aspectos, el número de arbitrajes y el coste y la duración de los arbitrajes, con el entendimiento de que no se deberá imponer una carga económica excesiva a las entidades participantes. El Departamento notificará a la Comisión Europea el resultado de dichos análisis con el tercero y le notificará por adelantado cualquier ajuste del importe de las aportaciones.

Realizar revisiones conjuntas del funcionamiento del Marco de Privacidad de Datos UE-EE. UU.

El Departamento y otros organismos, según proceda, tendrán reuniones periódicas con la Comisión Europea, las APD interesadas y los representantes correspondientes del Comité Europeo de Protección de Datos en las que el Departamento proporcionará información actualizada sobre el Marco de Privacidad de Datos UE-EE. UU. Estas reuniones incluirán un debate sobre las cuestiones de actualidad relacionadas con el funcionamiento, la aplicación, la supervisión y el cumplimiento del programa del Marco de Privacidad de Datos. También podrán incluir, en su caso, un debate de temas relacionados, como otros mecanismos de transferencia de datos amparados por las garantías del Marco de Privacidad de Datos UE-EE. UU.

([3]) El Centro Internacional de Resolución de Controversias (International Centre for Dispute Resolution), que es la división internacional de la Asociación Estadounidense de Arbitraje (American Arbitration Association) (denominadas conjuntamente en lo sucesivo «el CIRC y la AEA»), fue seleccionado por el Departamento para gestionar los arbitrajes y administrar el fondo arbitral contemplados en el anexo I de los principios en materia de privacidad.

([4]) El 15 de septiembre de 2017, el Departamento y la Comisión Europea acordaron aprobar un conjunto de reglas de arbitraje con las que regular los procesos arbitrales vinculantes descritos en el anexo I de los principios en materia de privacidad, así como un código de conducta para los árbitros que sea coherente con las normas éticas generalmente aceptadas para los árbitros mercantiles y con el anexo I de los principios en materia de privacidad. El Departamento y la Comisión Europea acordaron adaptar las reglas de arbitraje y el código de conducta para reflejar las actualizaciones en el Marco de Privacidad de Datos UE-EE. UU., y el Departamento cooperará con el CIRC y la AEA para poner en práctica dichas actualizaciones.

Cambios normativos

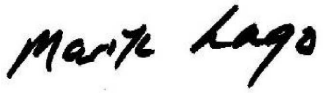
El Departamento procurará razonablemente informar a la Comisión Europea de los cambios normativos importantes en los EE. UU. en la medida en que sean pertinentes para el Marco de Privacidad de Datos UE-EE. UU. en el ámbito de la protección de la privacidad de los datos y de las limitaciones y garantías aplicables al acceso a los datos personales por parte de las autoridades estadounidenses y su posterior uso.

Acceso de los poderes públicos estadounidenses a los datos personales

En los EE. UU. se han aprobado el Decreto Presidencial n.º 14086, titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos», y el nuevo título 28, parte 201, del Código de Reglamentos Federales, por el que se modifica la normativa del Departamento de Justicia para crear el Tribunal de Recurso en Materia de Protección de Datos, que confieren una protección sólida a los datos personales respecto del acceso de los poderes públicos a los datos con fines de seguridad nacional. Esta protección comprende: el refuerzo de las garantías de la privacidad y las libertades civiles para asegurar que las actividades de inteligencia de señales estadounidenses sean necesarias y proporcionadas para cumplir los objetivos de seguridad nacional que se fijen; una nueva vía de impugnación de la que sea responsable una autoridad independiente que pueda dictar resoluciones vinculantes; y la mejora de la supervisión rigurosa y por niveles existente de las actividades de inteligencia de señales estadounidenses. Con estas garantías, los particulares de la UE pueden pedir reparación a través de un nueva vía multiinstancia en la que se incluye el Tribunal de Recurso en Materia de Protección de Datos, tribunal independiente compuesto por personas elegidas no pertenecientes al Ejecutivo estadounidense que tienen plena competencia para pronunciarse respecto de las pretensiones y dictar directamente medidas reparatorias en caso necesario. El Departamento publicará el registro de los particulares de la UE que presenten reclamaciones que reúnan los requisitos del Decreto Presidencial n.º 14086 y el título 28, parte 201, del Código de Reglamentos Federales. Cinco años después de la fecha de la presente carta y posteriormente cada cinco años, el Departamento se pondrá en contacto con los organismos pertinentes para saber si se ha desclasificado la información relativa a las reclamaciones mencionadas antes o de cualquier recurso presentado al Tribunal de Recurso en Materia de Protección de Datos. Si dicha información ha sido desclasificada, el Departamento colaborará con la APD pertinente para informar al particular de la UE. Estas mejoras confirman que los datos personales de la UE transferidos a los EE. UU. se tratarán de manera respetuosa con los requisitos normativos de la UE con respecto al acceso de los poderes públicos a los datos.

Gracias a los principios en materia de privacidad, el Decreto Presidencial n.º 14086, el título 28, parte 201, del Código de Reglamentos Federales y las cartas y documentos adjuntos, así como los compromisos del Departamento en relación con la administración y la supervisión del programa del Marco de Privacidad de Datos UE-EE. UU., esperamos que la Comisión Europea considere que el Marco de Privacidad de Datos UE-EE. UU. confiere una protección adecuada según el Derecho de la UE y que se puedan seguir realizando transferencias de datos desde la UE a las entidades que participan en dicho Marco. También esperamos que las transferencias a entidades estadounidenses realizadas al amparo de las cláusulas contractuales tipo de la UE o de la normativa societaria vinculante de la UE se vean aún más facilitadas por dichas medidas.

Atentamente,



Marisa Lago

ANEXO IV

ESTADOS UNIDOS DE AMÉRICA
Comisión Federal de Comercio
WASHINGTON, D.C. 20580

Oficina de la presidenta

9 de junio de 2023

Sr. D. Didier Reynders
Comisario de Justicia
Commission européenne / Europese Commissie
Rue de la Loi / Wetstraat 200
1049 Bruxelles/Brussel
BÉLGICA

Estimado comisario Reynders:

La Comisión Federal de Comercio de los EE. UU. quisiera describir su función de garantía del cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. La Comisión Federal de Comercio lleva mucho tiempo comprometida con la protección de los consumidores y la privacidad a través de las fronteras, y estamos comprometidos con la garantía del cumplimiento de los aspectos de este Marco relacionados con el sector comercial. La Comisión Federal de Comercio viene desempeñando esta función desde el año 2000 en relación con el marco del puerto seguro UE-EE. UU. y, más recientemente, desde 2016, en relación con el marco del Escudo de la privacidad UE-EE. UU. ([1]). El 16 de julio de 2020, el Tribunal de Justicia de la Unión Europea («TJUE») invalidó la decisión de adecuación de la Comisión Europea sobre el marco del Escudo de la privacidad UE-EE. UU., por cuestiones distintas de los principios comerciales por cuyo cumplimiento velaba la Comisión Federal de Comercio. Desde entonces, los Estados Unidos («EE. UU.») y la Comisión Europea han negociado el Marco de Privacidad de Datos UE-EE. UU. para dar respuesta a las cuestiones planteadas en dicha sentencia del TJUE.

Me dirijo a usted para confirmar el compromiso de la Comisión Federal de Comercio de garantizar con decisión el cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. En particular, reafirmamos nuestro compromiso en tres ámbitos clave: 1) las investigaciones y la priorización de la remisión de las reclamaciones; 2) solicitar órdenes y hacer un seguimiento; y 3) la cooperación en materia de garantía del cumplimiento con las autoridades de protección de datos («APD») de la UE.

I. **Introducción**

a. **Garantía del cumplimiento en materia de privacidad y labor política de la Comisión Federal de Comercio**

La Comisión Federal de Comercio tiene amplias competencias en materia de ejecución forzosa civil para promover la protección de los consumidores y la competencia en el mercado. Como parte integral de su cometido de proteger a los consumidores, la Comisión Federal de Comercio asume la garantía del cumplimiento de una amplia gama de normas para

([1]) Carta de la presidenta Edith Ramírez a Věra Jourová, comisaria de Justicia, Consumidores e Igualdad de Género de la Comisión Europea, en la que se describen las actividades de garantía del cumplimiento del nuevo marco del Escudo de la privacidad UE-EE. UU. por parte de la Comisión Federal de Comercio (29 de febrero de 2016), disponible en inglés en https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. La Comisión Federal de Comercio también se había comprometido a garantizar el cumplimiento del marco del puerto seguro UE-EE. UU. Carta de Robert Pitofsky, presidente de la Comisión Federal de Comercio, a John Mogg, director de la Dirección General de Mercado Interior de la Comisión Europea (14 de julio de 2000), disponible en inglés en https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. La presente carta sustituye los compromisos anteriores.

proteger la privacidad y la seguridad de los consumidores y sus datos. La norma fundamental por cuyo cumplimiento vela la Comisión Federal de Comercio, a saber, la Ley de la Comisión Federal de Comercio, prohíbe los actos o prácticas desleales y engañosos en el comercio o que afecten al comercio ([2]). La Comisión Federal de Comercio también asume la garantía del cumplimiento de leyes específicas de protección de la información sanitaria, crediticia y relativa a otras cuestiones económicas, así como de la información en línea sobre menores, y ha aprobado reglamentos de desarrollo de dichas leyes ([3]).

La Comisión Federal de Comercio también ha emprendido recientemente numerosas iniciativas para reforzar nuestra labor en materia de privacidad. En agosto de 2022, la Comisión Federal de Comercio anunció que está estudiando la posibilidad de aprobar reglas para atajar la vigilancia comercial perjudicial y la seguridad laxa de los datos ([4]). El objetivo del proyecto es contar con un registro público sólido con el que poder decidir si la Comisión Federal de Comercio debe aprobar reglas en materia de vigilancia comercial y prácticas relativas a la seguridad de los datos, y cómo deberían ser dichas reglas. Hemos tomado debida nota de las observaciones de las partes interesadas de la Unión Europea («UE») sobre esta y otras iniciativas.

Nuestras conferencias «PrivacyCon» siguen reuniendo a investigadores destacados para debatir los últimos estudios y tendencias relacionados con la privacidad de los consumidores y la seguridad de los datos. También hemos aumentado nuestra capacidad para seguir el ritmo de los avances tecnológicos que son causa de gran parte de nuestra labor en materia de privacidad, creando un equipo cada vez mayor de técnicos e investigadores interdisciplinarios. También anunciamos, como ya sabe, un diálogo conjunto con usted y sus compañeros de la Comisión Europea, para tratar temas relacionados con la privacidad, como las interfaces engañosas y los modelos de negocio caracterizados por una recogida de datos generalizada ([5]). A su vez, hemos publicado recientemente el informe dirigido al Congreso sobre los perjuicios asociados al uso de la inteligencia artificial para tratar el tema de los perjuicios en línea señalados por el Congreso. En este informe se expresaba inquietud en relación con la inexactitud, el sesgo, la discriminación y la perversión de la vigilancia comercial ([6]).

b. **Garantías jurídicas de los EE. UU. que benefician a los consumidores de la UE**

El Marco de Privacidad de Datos UE-EE. UU. se inserta en el contexto más amplio de las medidas del ámbito de la privacidad tomadas por los EE. UU., que protegen a los consumidores de la UE de diferentes maneras. La prohibición de la Ley de la Comisión Federal de Comercio de los actos o prácticas desleales o engañosos no se limita a la protección de los consumidores estadounidenses frente a las empresas estadounidenses, ya que comprende aquellas prácticas que: 1) causen o sea probable que causen perjuicios razonablemente previsibles en los EE. UU. o 2) impliquen un hacer o un no hacer determinante para modificar el comportamiento del consumidor en los EE. UU. Además, la Comisión Federal de Comercio puede servirse de todas las medidas de reparación disponibles para la protección de los consumidores nacionales también para proteger a los consumidores extranjeros ([7]).

La Comisión Federal de Comercio también vela por el cumplimiento de otras leyes específicas cuyas garantías se extienden a los consumidores no estadounidenses, como la Ley de protección de la privacidad infantil en internet. Esta Ley exige, por ejemplo, que los operadores de sitios web y de servicios en línea dirigidos a menores o de sitios web para todos los públicos que recojan a sabiendas información personal de menores de trece años lo notifiquen a los padres y obtengan consentimiento parental verificable. Los sitios web radicados en los EE. UU. y los servicios prestados en dicho país que

([2]) Título 15, artículo 45, letra a), del Código de Estados Unidos. La Comisión Federal de Comercio no tiene competencia en materia penal ni en materia de seguridad nacional. Tampoco puede participar en la mayoría de las demás actuaciones del Ejecutivo. Además, existen determinadas excepciones a la competencia de la Comisión Federal de Comercio sobre las actividades comerciales, en particular relacionadas con los bancos, las aerolíneas, el sector de los seguros y las actividades de mero transportista de las empresas de servicios de telecomunicaciones. La Comisión Federal de Comercio tampoco tiene competencia sobre la mayoría de las entidades sin ánimo de lucro, pero sí la tiene sobre las entidades benéficas u otras entidades sin ánimo de lucro que en realidad operan con ánimo de lucro. La Comisión Federal de Comercio también tiene competencia sobre las entidades sin ánimo de lucro que operan en beneficio de sus miembros con ánimo de lucro, especialmente si proporcionan ventajas económicas sustanciales a dichos miembros. En algunos casos, la competencia de la Comisión Federal de Comercio coincide con la de otras autoridades policiales. Hemos desarrollado una sólida relación de trabajo con las autoridades federales y estatales y colaboramos estrechamente con ellas para coordinar las investigaciones o remitirlas, si procede.

([3]) Véase la página web sobre privacidad y seguridad de la Comisión Federal de Comercio: https://www.ftc.gov/business-guidance/privacy-security.

([4]) Véase el comunicado de prensa de la Comisión Federal de Comercio acerca de la posibilidad de aprobar reglas para atajar la vigilancia comercial perjudicial y la seguridad laxa de los datos (11 de agosto de 2022), disponible en inglés en https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) Véase el comunicado de prensa conjunto de Didier Reynders, comisario de Justicia de la Comisión Europea, y Lina Khan, presidenta de la Comisión Federal de Comercio de los EE. UU. (30 de marzo de 2022), disponible en inglés en https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) Véase el comunicado de prensa de la Comisión Federal de Comercio en el que alerta sobre los riegos de usar la inteligencia artificial para atajar problemas en internet (16 de junio de 2022), disponible en inglés en https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) Título 15, artículo 45, letra a), punto 4, subletra B), del Código de Estados Unidos. Se entiende que los actos o prácticas desleales o engañosos comprenden los actos o prácticas relacionados con el comercio internacional que: i) causen o sea probable que causen perjuicios razonablemente previsibles en los EE. UU. o ii) impliquen un hacer o un no hacer determinante para modificar el comportamiento del consumidor en los EE. UU. Título 15, artículo 45, letra a), punto 4, subletra A), del Código de Estados Unidos.

estén sujetos a la Ley de protección de la privacidad infantil en internet y recojan información personal de menores extranjeros deben hacerlo de conformidad con dicha Ley. Los sitios web radicados en el extranjero y los servicios prestados en el extranjero deben también hacerlo de conformidad con la Ley de protección de la privacidad infantil en internet si se dirigen a menores estadounidenses o si recogen a sabiendas información personal de menores estadounidenses. Además de las leyes federales estadounidenses por cuyo cumplimiento vela la Comisión Federal de Comercio, otras leyes federales y de los Estados federados relativas a la protección de los consumidores, las violaciones de la seguridad de los datos y la privacidad pueden ofrecer garantías adicionales a los consumidores de la UE.

c. **Actividad de garantía del cumplimiento de la Comisión Federal de Comercio**

La Comisión Federal de Comercio incoó procesos relativos tanto al marco del puerto seguro UE-EE. UU. como al marco del Escudo de la privacidad UE-EE. UU. y siguió emprendiendo actividades de garante del cumplimiento del Escudo de la privacidad UE-EE. UU. incluso después de la invalidación por el TJUE de la decisión de adecuación sobre el marco del Escudo de la privacidad UE-EE. UU. ([8]). Varias de las reclamaciones recientes de la Comisión Federal de Comercio han ido referidas a empresas que vulneraron las disposiciones del Escudo de la privacidad UE-EE. UU., como los procesos contra Twitter ([9]), CafePress ([10]) y Flo ([11]). En el proceso contra Twitter, la Comisión Federal de Comercio consiguió que se multase a Twitter con 150 millones USD por su incumplimiento de una resolución anterior de la Comisión Federal de Comercio respecto de prácticas que afectaban a más de 140 millones de clientes y que vulneraban el principio 5 del Escudo de la privacidad UE-EE.UU. (integridad de los datos y limitación de la finalidad). Además, en dicha resolución se imponía a Twitter la obligación de permitir a los usuarios utilizar métodos seguros de autenticación multifactorial con los que los usuarios no tengan que dar sus números de teléfono.

En el asunto CafePress, la Comisión Federal de Comercio alegó que la empresa no protegió debidamente la información delicada de los consumidores, ocultó una violación importante de la seguridad de los datos e incumplió los principios 2 (opción), 4 (seguridad) y 6 (acceso) del Escudo de la privacidad UE-EE. UU. La resolución de la Comisión Federal de Comercio obligaba a la empresa a sustituir las medidas de autenticación inadecuadas por la autenticación multifactorial, a limitar sustancialmente la cantidad de datos que recoge y conserva, a cifrar los números de la Seguridad Social y a contar con un tercero que evalúe sus programas de seguridad de la información y entregue a la Comisión Federal de Comercio una copia que pueda hacerse pública.

En el asunto Flo, la Comisión Federal de Comercio alegó que la aplicación de seguimiento de la fertilidad comunicaba información sanitaria de los usuarios a empresas de análisis de datos pese al compromiso asumido de preservar la privacidad de dicha información. En la reclamación de la Comisión Federal de Comercio se señala específicamente el trato que tuvo la empresa con los consumidores de la UE y que Flo vulneró los principios del Escudo de la privacidad UE-EE. UU. 1 (notificación), 2 (opción), 3 (responsabilidad por una transferencia ulterior) y 5 (integridad de los datos y limitación de la finalidad). Entre otros aspectos, la resolución de la Comisión Federal de Comercio obliga a Flo a notificar a los usuarios afectados la comunicación de su información personal y a ordenar a los terceros que hayan recibido información sanitaria de los usuarios que la destruyan. Y lo que es más importante, las resoluciones de la Comisión Federal de Comercio protegen a los consumidores de todo el mundo que tratan con empresas estadounidenses, no tan solo a los consumidores que hayan presentado una reclamación.

Muchos asuntos incoados en el marco del puerto seguro UE-EE. UU. y del Escudo de la privacidad UE-EE. UU. se referían a entidades que completaron la autocertificación inicial ante el Departamento de Comercio y no renovaron anualmente su autocertificación, pero seguían afirmando participar en esos regímenes. Otros asuntos tenían que ver con declaraciones falsas de participación de entidades que nunca completaron la autocertificación inicial ante el Departamento de Comercio. De cara al futuro, esperamos centrar nuestra labor proactiva de garantía del cumplimiento en los tipos de vulneraciones sustanciales de los principios del Marco de Privacidad de Datos UE-EE. UU. alegadas en asuntos como el de Twitter, CafePress y Flo. Mientras tanto, el Departamento de Comercio llevará y supervisará el proceso de autocertificación, administrará la lista oficial de participantes en el Marco de Privacidad de Datos UE-EE. UU. y resolverá las demás cuestiones relativas a las declaraciones de participación en el programa ([12]). Es importante señalar que las entidades que afirman participar en el Marco de Privacidad de Datos UE-EE. UU. pueden ser objeto de medidas sustanciales de garantía del cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU., incluso por no autocertificarse o no revalidar la autocertificación ante el Departamento de Comercio.

([8]) En el apéndice A se relacionan los procesos resueltos por la Comisión Federal de Comercio relativos al puerto seguro y al Escudo de la privacidad.

([9]) Véase el comunicado de prensa de la Comisión Federal de Comercio sobre el proceso de esta contra Twitter por el uso engañoso de los datos de seguridad de las cuentas para su venta con fines publicitarios (25 de mayo de 2022), disponible en inglés en https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) Véase el comunicado de prensa de la Comisión Federal de Comercio sobre el proceso de esta contra CafePress por encubrimiento de la violación de la seguridad de los datos (15 de marzo de 2022), disponible en inglés en https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) Véase el comunicado de prensa de la Comisión Federal de Comercio sobre la resolución contra Flo Health, la aplicación de seguimiento de la fertilidad que compartió datos sanitarios delicados con Facebook, Google y otras empresas (22 de junio de 2021), disponible en inglés en https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Carta de Marisa Lago, subsecretaria del Departamento de Comercio para el Comercio Internacional, al Excmo. Sr. Didier Reynders, comisario de Justicia, Comisión Europea (12 de diciembre de 2022).

II. **Investigaciones y priorización de las reclamaciones remitidas**

Al igual que hizo en el marco del puerto seguro UE-EE. UU. y en el marco del Escudo de la privacidad UE-EE. UU., la Comisión Federal de Comercio se compromete a dar prioridad a las reclamaciones remitidas por el Departamento de Comercio y los Estados miembros de la UE respecto de los principios del Marco de Privacidad de Datos UE-EE. UU. También daremos prioridad a reclamaciones remitidas por incumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. por parte de las entidades del ámbito autorregulatorio en materia de privacidad y de otros organismos independientes de resolución de controversias.

Para facilitar la remisión de reclamaciones en el Marco de Privacidad de Datos UE-EE. UU. por los Estados miembros de la UE, la Comisión Federal de Comercio ha creado un procedimiento estandarizado de remisión y proporcionado instrucciones a los Estados miembros de la UE sobre el tipo de información más útil para la Comisión Federal de Comercio al investigar reclamaciones remitidas. Como parte de esta iniciativa, la Comisión Federal de Comercio ha nombrado un punto de contacto para la remisión de reclamaciones por parte de los Estados miembro de la UE. Resulta muy útil que la autoridad remitente realice una investigación preliminar de la posible vulneración y que coopere con la Comisión Federal de Comercio en la investigación.

Tras la remisión de una reclamación por el Departamento de Comercio, un Estado miembro de la UE, una entidad del ámbito autorregulatorio u otro organismo independiente de resolución de controversias, la Comisión Federal de Comercio puede tomar una serie de medidas para resolver las cuestiones planteadas. Por ejemplo, podemos revisar las directrices en materia privacidad de la entidad, obtener más información directamente de la entidad o de terceros, pedir más información al remitente, evaluar si existe un patrón de vulneraciones o un número significativo de consumidores afectados, determinar si la remisión afecta a cuestiones que son de competencia del Departamento de Comercio, valorar si sería útil informar a los participantes en el mercado y, si procede, iniciar un proceso para exigir el cumplimiento.

Además de dar prioridad a las remisiones del Departamento de Comercio, los Estados miembros de la UE, las entidades del ámbito autorregulatorio en materia de privacidad u otros organismos independientes de resolución de controversias respecto de los principios del Marco de Privacidad de Datos UE-EE. UU. ([13]), la Comisión Federal de Comercio seguirá investigando de oficio las vulneraciones significativas de los principios del Marco de Privacidad de Datos UE-EE. UU. utilizando una serie de instrumentos. Como parte del programa de la Comisión Federal de Comercio de investigar problemas en materia de privacidad y seguridad relativos a las entidades mercantiles, esta ha examinado sistemáticamente si la entidad en cuestión declaraba participar en el Escudo de la privacidad UE-EE. UU. Si hacía tales declaraciones y la investigación revelaba claras vulneraciones de los principios del Escudo de la privacidad UE-EE. UU., la Comisión Federal de Comercio sumaba la alegación de vulneración del Escudo de la privacidad UE-EE. UU. al proceso. Mantendremos este planteamiento proactivo, ahora con respecto a los principios del Marco de Privacidad de Datos UE-EE. UU.

III. **Solicitar órdenes y hacer un seguimiento**

La Comisión Federal de Comercio también reafirma su compromiso de solicitar que se dicten resoluciones para garantizar el cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. y hacer un seguimiento de las mismas. Exigiremos el cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. con diversas obligaciones de hacer o no hacer en las futuras órdenes de la Comisión Federal de Comercio en relación con dichos principios. El incumplimiento de las resoluciones administrativas de la Comisión Federal de Comercio puede comportar sanciones pecuniarias de hasta 501,20 USD por incumplimiento, o de 50,120 USD por día si es un incumplimiento continuado ([14]), que, en el caso de las prácticas que afecten a muchos consumidores, pueden ascender a millones de dólares. Las resoluciones de constatación de la avenencia de la entidad incluyen disposiciones en materia de presentación de informes y de cumplimiento. Las entidades sujetas a una de estas resoluciones deben conservar los documentos que demuestren su cumplimiento durante un cierto número de años. Estas resoluciones también deben comunicarse a los empleados responsables de garantizar su cumplimiento.

La Comisión Federal de Comercio hace un seguimiento sistemático del cumplimiento de las resoluciones aún en curso respecto de los principios del Escudo de la privacidad UE-EE. UU., como hace de todas sus resoluciones, y emprende acciones judicial para exigir su cumplimiento cuando es necesario ([15]). Y lo que es más importante, las resoluciones de la Comisión Federal de Comercio seguirán protegiendo a los consumidores de todo el mundo que tratan con empresas estadounidenses, no tan solo a los consumidores que hayan presentado una reclamación. Por último, la Comisión Federal de Comercio publicará en línea la lista de las empresas objeto de resoluciones dictadas para exigir el cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. ([16]).

([13]) Aunque la Comisión Federal de Comercio no resuelve las reclamaciones individuales de consumidores ni media en estas, sí que confirma que dará prioridad a las reclamaciones remitidas por las APD de la UE relacionadas con los principios del Marco de Privacidad de Datos UE-EE. UU. Asimismo, la Comisión Federal de Comercio utiliza las reclamaciones que figuran en su base de datos Consumer Sentinel, a la que pueden acceder otras autoridades policiales, para detectar las tendencias, fijar las prioridades y determinar posibles investigaciones. Los particulares de la UE pueden utilizar el mismo sistema de reclamación de que disponen los consumidores estadounidenses para enviar su reclamación a la Comisión Federal de Comercio: https://reportfraud.ftc.gov/. Respecto de las reclamaciones de particulares relacionadas con los principios del Marco de Privacidad de Datos UE-EE. UU., no obstante, sería más práctico que los particulares de la UE envíen sus reclamaciones a la APD de su Estado miembro o a un organismo independiente de resolución de controversias.

([14]) Título 15, artículo 45, letra m), del Código de Estados Unidos; título 16, artículo 1.98, del Código de Reglamentos Federales. Este importe se ajusta periódicamente en función de la inflación.

([15]) El año pasado, la Comisión Federal de Comercio votó a favor de racionalizar el proceso de investigación de los infractores reincidentes. Véase el comunicado de prensa de la Comisión Federal de Comercio sobre la autorización de las investigaciones de las prioridades clave para la garantía del cumplimiento (1 de julio de 2021), disponible en inglés en https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) Véase la página de la Comisión Federal de Comercio sobre el Escudo de la privacidad: https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Cooperación con las APD de la UE para la garantía del cumplimiento**

La Comisión Federal de Comercio reconoce la importante función que pueden desempeñar las APD de la UE con respecto al cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. y anima a que aumenten las consultas y a que se mejore la cooperación en el ámbito de la garantía del cumplimiento. De hecho, es cada vez más necesario contar con un planteamiento coordinado respecto de las dificultades que plantean la evolución actual del mercado digital y los modelos de negocio con un uso intensivo de datos. La Comisión Federal de Comercio intercambiará información sobre las reclamaciones remitidas con las autoridades remitentes, en particular sobre el estado de las reclamaciones remitidas, de conformidad con la normativa y las limitaciones aplicables en materia de confidencialidad. En la medida en que sea viable por el número y tipo de remisiones, la información proporcionada incluirá una valoración de las cuestiones remitidas, en particular una descripción de las cuestiones importantes planteadas y cualquier medida tomada para resolver el incumplimiento de la normativa en el ámbito de competencia de la Comisión Federal de Comercio. La Comisión Federal de Comercio hará observaciones a la autoridad remitente sobre los tipos de remisiones con el objeto de aumentar la eficacia de las medidas para hacer frente a las conductas ilícitas. En caso de que la autoridad remitente solicite información sobre el estado de una determinada reclamación a efectos de incoar su propio proceso de garantía del cumplimiento, la Comisión Federal de Comercio responderá teniendo en cuenta el número de reclamaciones remitidas objeto de análisis y de conformidad con las exigencias normativas y en materia de confidencialidad.

La Comisión Federal de Comercio también colaborará estrechamente con las APD de la UE para prestar ayuda en materia de garantía del cumplimiento. En los casos en que proceda, esto podrá suponer el intercambio de información y la ayuda en investigaciones de conformidad con la Ley estadounidense de seguridad en internet (SAFE WEB Act), por la que se autoriza a la Comisión Federal de Comercio a ayudar a los autoridades policiales extranjeras cuando dichas autoridades realicen actuaciones respecto de normas que prohíban prácticas sustancialmente similares a las prohibidas por las normas de las que es garante la Comisión Federal de Comercio ([17]). Como parte de esta ayuda, la Comisión Federal de Comercio puede compartir la información relacionada con una investigación que haya realizado, dictar medidas obligatorias en nombre de la APD de la UE que lleve a cabo su propia investigación y tomar testimonio oral a testigos o partes a efectos del proceso de garantía del cumplimiento de la APD, de conformidad con los requisitos de la Ley de seguridad en internet. La Comisión Federal de Comercio ejerce generalmente esta competencia para ayudar a otras autoridades de todo el mundo en casos de protección de la privacidad y de los consumidores.

Además de las consultas a las APD de la UE remitentes sobre cuestiones de casos concretos, la Comisión Federal de Comercio se compromete a participar en reuniones periódicas con los representantes designados del Comité Europeo de Protección de Datos para debatir, en términos generales, cómo mejorar la cooperación para garantizar el cumplimiento del Marco. Participará también, junto con los representantes del Departamento de Comercio, de la Comisión Europea y del Comité Europeo de Protección de Datos, en la revisión periódica del Marco de Privacidad de Datos UE-EE. UU. para hablar de su aplicación. Asimismo, fomenta el desarrollo de herramientas que mejoren la cooperación en materia de garantía del cumplimiento con las APD de la UE, así como con otras autoridades del ámbito de la protección de la privacidad de todo el mundo. La Comisión Federal de Comercio se complace en declarar su compromiso de hacer cumplir los aspectos del Marco de Privacidad de Datos UE-EE. UU. relativos al sector comercial. Consideramos que la colaboración con nuestros interlocutores de la UE es una parte fundamental de la protección de la privacidad tanto de nuestros ciudadanos como de los suyos.

Atentamente,

Lina M. Khan
Presidenta, Comisión Federal de Comercio

([17]) A la hora de determinar si debe ejercer la competencia que le otorga la Ley de seguridad en internet, la Comisión Federal de Comercio considera, entre otros aspectos: a) si el organismo solicitante ha aceptado prestar o prestará ayuda recíproca a la Comisión Federal de Comercio; b) si el cumplimiento de la solicitud perjudicaría intereses públicos de los EE. UU.; y c) si la investigación o el proceso de garantía del cumplimiento del organismo solicitante se refiere a actos o prácticas que causen o sea probable que causen un perjuicio a un número considerable de personas [título 15, artículo 46, letra j), apartado 3, del Código de Estados Unidos]. Esta facultad no se puede ejercer respecto de la garantía del cumplimiento de la normativa en materia de competencia.

Apéndice A

Garantía del cumplimiento en relación con el Escudo de la privacidad y el puerto seguro

	N.º de expediente/sumario de la CFC	**Asunto**	**Enlace**
1	Expediente de la Comisión Federal de Comercio n.º 2023062 Asunto n.º 3:22-cv-03070 (Distrito Norte de California)	US c. **Twitter, Inc.**	Twitter
2	Expediente de la Comisión Federal de Comercio n.º 192 3209	Residual Pumpkin Entity, LLC (antiguamente llamada **CafePress**), y PlanetArt, LLC (anteriormente operando con el nombre **CafePress**)	CafePress
3	Expediente de la Comisión Federal de Comercio n.º 192 3133 Sumario n.º C-4747	Flo Health, Inc.	Flo Health
4	Expediente de la Comisión Federal de Comercio n.º 192 3050 Sumario n.º C-4723	Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	Expediente de la Comisión Federal de Comercio n.º 192 3092 Sumario n.º C-4709	T&M Protection, LLC	T&M Protection
6	Expediente de la Comisión Federal de Comercio n.º 192 3084 Sumario n.º C-4704	TDARX, Inc.	TDARX
7	Expediente de la Comisión Federal de Comercio n.º 192 3093 Sumario n.º C-4706	Global Data Vault, LLC	Global Data
8	Expediente de la Comisión Federal de Comercio n.º 192 3078 Sumario n.º C-4703	Incentive Services, Inc.	Incentive Services
9	Expediente de la Comisión Federal de Comercio n.º 192 3090 Sumario n.º C-4705	Click Labs, Inc.	Click Labs
10	Expediente de la Comisión Federal de Comercio n.º 182 3192 Sumario n.º C-4697	Medable, Inc.	Medable
11	Expediente de la Comisión Federal de Comercio n.º 182 3189 Sumario n.º 9386	NTT Global Data Centers Americas, Inc., como sucesora de **RagingWire Data Centers, Inc.**	RagingWire
12	Expediente de la Comisión Federal de Comercio n.º 182 3196 Sumario n.º C-4702	Thru, Inc.	Thru
13	Expediente de la Comisión Federal de Comercio n.º 182 3188 Sumario n.º C-4698	DCR Workforce, Inc.	DCR Workforce
14	Expediente de la Comisión Federal de Comercio n.º 182 3194 Sumario n.º C-4700	LotaData, Inc.	LotaData
15	Expediente de la Comisión Federal de Comercio n.º 182 3195 Sumario n.º C-4701	EmpiriStat, Inc.	EmpiriStat

16	Expediente de la Comisión Federal de Comercio n.º 182 3193 Sumario n.º C-4699	214 Technologies, Inc. (también conocida como **Trueface.ai**)	Trueface.ai
17	Expediente de la Comisión Federal de Comercio n.º 182 3107 Sumario n.º 9383	Cambridge Analytica, LLC	Cambridge Analytica
18	Expediente de la Comisión Federal de Comercio n.º 182 3152 Sumario n.º C-4685	SecureTest, Inc.	SecurTest
19	Expediente de la Comisión Federal de Comercio n.º 182 3144 Sumario n.º C-4664	VenPath, Inc.	VenPath
20	Expediente de la Comisión Federal de Comercio n.º 182 3154 Sumario n.º C-4666	SmartStart Employment Screening, Inc.	SmartStart
21	Expediente de la Comisión Federal de Comercio n.º 182 3143 Sumario n.º C-4663	**mResourceLLC** (también conocida como Loop Works LLC)	mResource
22	Expediente de la Comisión Federal de Comercio n.º 182 3150 Sumario n.º C-4665	Idmission LLC	IDmission
23	Expediente de la Comisión Federal de Comercio n.º 182 3100 Sumario n.º C-4659	ReadyTech Corporation	ReadyTech
24	Expediente de la Comisión Federal de Comercio n.º 172 3173 Sumario n.º C-4630	Decusoft, LLC	Decusoft
25	Expediente de la Comisión Federal de Comercio n.º 172 3171 Sumario n.º C-4628	Tru Communication, Inc.	Tru
26	Expediente de la Comisión Federal de Comercio n.º 172 3172 Sumario n.º C-4629	Md7, LLC	Md7
30	Expediente de la Comisión Federal de Comercio n.º 152 3198 Sumario n.º C-4543	**Jhayrmaine Daniels** (también conocida como **California Skate-Line)**	Jhayrmaine Daniels
31	Expediente de la Comisión Federal de Comercio n.º 152 3190 Sumario n.º C-4545	Dale Jarrett Racing Adventure, Inc.	Dale Jarrett
32	Expediente de la Comisión Federal de Comercio n.º 152 3141 Sumario n.º C-4540	Golf Connect, LLC	Golf Connect
33	Expediente de la Comisión Federal de Comercio n.º 152 3202 Sumario n.º C-4546	Inbox Group, LLC	Inbox Group
34	Expediente de la Comisión Federal de Comercio n.º 152 3187 Sumario n.º C-4542	IOActive, Inc.	IOActive
35	Expediente de la Comisión Federal de Comercio n.º 152 3140 Sumario n.º C-4549	Jubilant Clinsys, Inc.	Jubilant
36	Expediente de la Comisión Federal de Comercio n.º 152 3199 Sumario n.º C-4547	Just Bagels Manufacturing, Inc.	Just Bagels

37	Expediente de la Comisión Federal de Comercio n.º 152 3138 Sumario n.º C-4548	NAICS Association, LLC	NAICS
38	Expediente de la Comisión Federal de Comercio n.º 152 3201 Sumario n.º C-4544	One Industries Corp.	One Industries
39	Expediente de la Comisión Federal de Comercio n.º 152 3137 Sumario n.º C-4550	Pinger, Inc.	Pinger
40	Expediente de la Comisión Federal de Comercio n.º 152 3193 Sumario n.º C-4552	SteriMed Medical Waste Solutions	SteriMed
41	Expediente de la Comisión Federal de Comercio n.º 152 3184 Sumario n.º C-4541	Contract Logix, LLC	Contract Logix
42	Expediente de la Comisión Federal de Comercio n.º 152 3185 Sumario n.º C-4551	Forensics Consulting Solutions, LLC	Forensics Consulting
43	Expediente de la Comisión Federal de Comercio n.º 152 3051 Sumario n.º C-4526	American Int'l Mailing, Inc.	AIM
44	Expediente de la Comisión Federal de Comercio n.º 152 3015 Sumario n.º C-4525	TES Franchising, LLC	TES
45	Expediente de la Comisión Federal de Comercio n.º 142 3036 Sumario n.º C-4459	American Apparel, Inc.	American Apparel
46	Expediente de la Comisión Federal de Comercio n.º 142 3026 Sumario n.º C-4469	Fantage.com, Inc.	Fantage
47	Expediente de la Comisión Federal de Comercio n.º 142 3017 Sumario n.º C-4461	Apperian, Inc.	Apperian
48	Expediente de la Comisión Federal de Comercio n.º 142 3018 Sumario n.º C-4462	Atlanta Falcons Football Club, LLC	Atlanta Falcons
49	Expediente de la Comisión Federal de Comercio n.º 142 3019 Sumario n.º C-4463	Baker Tilly Virchow Krause, LLP	Baker Tilly
50	Expediente de la Comisión Federal de Comercio n.º 142 3020 Sumario n.º C-4464	BitTorrent, Inc.	BitTorrent
51	Expediente de la Comisión Federal de Comercio n.º 142 3022 Sumario n.º C-4465	Charles River Laboratories, Int'l	Charles River
52	Expediente de la Comisión Federal de Comercio n.º 142 3023 Sumario n.º C-4466	DataMotion, Inc.	DataMotion
53	Expediente de la Comisión Federal de Comercio n.º 142 3024 Sumario n.º C-4467	**DDC Laboratories, Inc.** (también conocida como DNA Diagnostics Center)	DDC
54	Expediente de la Comisión Federal de Comercio n.º 142 3028 Sumario n.º C-4470	Level 3 Communications, LLC	Level 3

55	Expediente de la Comisión Federal de Comercio n.º 142 3025 Sumario n.º C-4468	**PDB Sports, Ltd.** (también conocida como Denver Broncos Football Club, LLP)	Broncos
56	Expediente de la Comisión Federal de Comercio n.º 142 3030 Sumario n.º C-4471	Reynolds Consumer Products, Inc.	Reynolds
57	Expediente de la Comisión Federal de Comercio n.º 142 3031 Sumario n.º C-4472	Receivable Management Services Corporation	Receivable Mgmt
58	Expediente de la Comisión Federal de Comercio n.º 142 3032 Sumario n.º C-4473	Tennessee Football, Inc.	Tennessee Football
59	Expediente de la Comisión Federal de Comercio n.º 102 3058 Sumario n.º C-4369	Myspace LLC	Myspace
60	Expediente de la Comisión Federal de Comercio n.º 092 3184 Sumario n.º C-4365	Facebook, Inc.	Facebook
61	Expediente de la Comisión Federal de Comercio n.º 092 3081 Demanda civil n.º 09-CV-5276 (Distrito Central de California)	FTC c. Javian Karnani y **Balls of Kryptonite, LLC** (también conocida como Bite Size Deals, LLC, y Best Priced Brands, LLC)	Balls of Kryptonite
62	Expediente de la Comisión Federal de Comercio n.º 102 3136 Sumario n.º C-4336	Google, Inc.	Google
63	Expediente de la Comisión Federal de Comercio n.º 092 3137 Sumario n.º C-4282	World Innovators, Inc.	World Innovators
64	Expediente de la Comisión Federal de Comercio n.º 092 3141 Sumario n.º C-4271	Progressive Gaitways LLC	Progressive Gaitways
65	Expediente de la Comisión Federal de Comercio n.º 092 3139 Sumario n.º C-4270	Onyx Graphics, Inc.	Onyx Graphics
66	Expediente de la Comisión Federal de Comercio n.º 092 3138 Sumario n.º C-4269	ExpatEdge Partners, LLC	ExpatEdge
67	Expediente de la Comisión Federal de Comercio n.º 092 3140 Sumario n.º C-4281	Directors Desk LLC	Directors Desk
68	Expediente de la Comisión Federal de Comercio n.º 092 3142 Sumario n.º C-4272	Collectify LLC	Collectify

ANEXO V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6 de julio de 2023

Comisario Didier Reynders
Commission européenne / Europese Commissie
Rue de la Loi / Wetstraat 200
1049 Bruxelles/Brussel
BÉLGICA

Estimado comisario Reynders:

El Departamento de Transporte de los EE. UU. quisiera describir su función de garantía del cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. Este Marco desempeña un papel fundamental en la protección de los datos personales proporcionados en operaciones comerciales en un mundo cada vez más interconectado. Permitirá a las empresas realizar operaciones importantes en la economía mundial y, al mismo tiempo, garantizará la protección de la privacidad de los consumidores de la UE.

El Departamento de Transporte manifestó públicamente por primera vez su compromiso de velar por el cumplimiento del marco del puerto seguro UE-EE. UU. en la carta enviada a la Comisión Europea hace más de veintidós años, compromiso que se reiteró y amplió por medio de la carta de 2016 relativa al marco del Escudo de la privacidad UE-EE. UU. En dichas cartas, se comprometió a hacer cumplir con firmeza los principios de privacidad del puerto seguro UE-EE. UU. y, posteriormente, los principios marco del Escudo de la privacidad UE-EE. UU. Por medio de la presente, quisiera renovar este compromiso haciéndolo extensible a los principios del Marco de Privacidad de Datos UE-EE. UU.

En particular, el Departamento de Transporte confirma su compromiso en los siguientes ámbitos clave: 1) priorización de la investigación de las posibles vulneraciones de los principios del Marco de Privacidad de Datos UE-EE. UU.; 2) actuaciones adecuadas de garantía del cumplimiento contra las entidades que realicen declaraciones falsas o engañosas en cuanto a su participación en el Marco de Privacidad de Datos UE-EE. UU.; y 3) seguimiento y publicidad de las resoluciones de ejecución forzosa por vulneración de los principios del Marco de Privacidad de Datos UE-EE. UU. A continuación, ofrecemos información sobre cada uno de estos compromisos y, para contextualizar, los antecedentes pertinentes sobre las competencias del Departamento de Transporte para la protección de la privacidad de los consumidores y la garantía del cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU.

1. **Antecedentes**

A. Competencias del Departamento de Transporte en materia de privacidad

El Departamento de Transporte declara su compromiso inquebrantable de garantizar la privacidad de la información proporcionada por los consumidores a las aerolíneas y a los agentes de venta de billetes.

La competencia del Departamento de Transporte para tomar medidas en este ámbito se contempla en el título 49, artículo 41712, del Código de Estados Unidos, por el que se prohíbe a los transportistas y los agentes de venta de billetes participar en prácticas desleales o engañosas en el transporte aéreo o en la comercialización de este tipo de transporte. El artículo 41712 sigue el modelo del artículo 5 de la Ley de la Comisión Federal de Comercio (título 15, artículo 45, del Código de Estados Unidos). Recientemente, el Departamento de Transporte ha aprobado un reglamento en el que se define en qué consisten las prácticas desleales y engañosas de forma coherente con los precedentes del Departamento de Transporte y de la Comisión Federal de Comercio (título 28, parte 399, artículo 79, del Código de Reglamentos Federales).

En concreto, una práctica es desleal si provoca o es probable que provoque daños o perjuicios importantes que no se pueden evitar razonablemente y no están compensados por ventajas para los consumidores o la competencia.

Una práctica es engañosa para los consumidores si es probable que induzca a error respecto a un aspecto importante a los consumidores que estén actuando de forma razonable dadas las circunstancias. Un aspecto es importante si es probable que haya afectado al comportamiento o la decisión del consumidor con respecto a un bien o un servicio. Aparte de estos principios generales, el Departamento de Transporte interpreta, en particular, el artículo 41712 en el sentido de que prohíbe a los transportistas y a los agentes de venta de billetes: 1) infringir las condiciones de sus directrices en materia de privacidad; 2) incumplir las normas aprobadas por el Departamento de Transporte en las que se declaren como desleales o engañosas prácticas concretas en materia de privacidad; 3) vulnerar la Ley de protección de la privacidad infantil en internet o la normativa de la Comisión Federal de Comercio de desarrollo de dicha Ley; 4) o incumplir, siendo participante en el Marco de Privacidad de Datos UE-EE. UU., los principios del Marco de Privacidad de Datos UE-EE. UU. ([1]).

Como ya se ha indicado, según el Derecho federal, el Departamento de Transporte tiene competencia exclusiva para regular las prácticas en materia de privacidad de las aerolíneas y tiene competencia compartida con la Comisión Federal de Comercio con respecto a las prácticas en materia de privacidad de los agentes de venta de billetes en la comercialización de este tipo de transporte.

Por ello, cuando el transportista o el vendedor de servicios de transporte aéreo se compromete públicamente a cumplir los principios del Marco de Privacidad de Datos UE-EE. UU., el Departamento de Transporte puede utilizar las competencias que le otorga el 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 a cumplir los principios del Marco de Privacidad de Datos UE-EE. UU., su incumplimiento por parte del transportista o del agente de venta de billetes constituye una vulneración del artículo 41712.

B. Prácticas de garantía del cumplimiento

La Oficina de Protección de los Consumidores del Sector de la Aviación (Office of Aviation Consumer Protection) ([2]), adscrita al Departamento de Transporte, investiga y enjuicia los asuntos derivados del título 49, artículo 41712, del Código de Estados Unidos. Garantiza la prohibición legal de las prácticas desleales y engañosas contemplada en el artículo 41712 principalmente a través de la negociación y la elaboración de órdenes de cese de actividad y de resoluciones que determinen el importe de la sanción pecuniaria. La Oficina tiene conocimiento de las posibles infracciones principalmente por las reclamaciones que recibe de particulares, agencias de viajes, aerolíneas y organismos públicos estadounidenses y extranjeros. Los consumidores pueden utilizar el sitio web correspondiente del Departamento de Transporte para presentar reclamaciones en materia de privacidad contra las aerolíneas y los agentes de venta de billetes ([3]).

En caso de no lograrse un convenio transaccional razonable y adecuado, la Oficina tiene competencia para incoar un proceso de ejecución, con audiencia probatoria ante un juez de lo contencioso-administrativo del Departamento de Transporte. El juez de lo contencioso-administrativo tiene potestad para dictar órdenes de cese de actividad e imponer sanciones pecuniarias. Las vulneraciones del artículo 41712 pueden conllevar que se dicten órdenes de cese de actividad y se impongan sanciones pecuniarias de hasta 37 377 USD por cada vulneración del artículo 41712.

El Departamento de Transporte no tiene competencia para conceder indemnizaciones por daños y perjuicios ni para establecer reparaciones monetarias para el reclamante. No obstante, tiene competencia para homologar los convenios transaccionales que resulten de las investigaciones llevadas a cabo por la Oficina de Protección de los Consumidores del Sector de la Aviación que beneficien directamente a los consumidores (por ejemplo, dinero en efectivo o vales) por importe equivalente a las sanciones pecuniarias que, de otro modo, se tendrían que pagar al Ejecutivo estadounidense. Esta posibilidad se ha materializado alguna vez en el pasado y podría también suceder en el contexto de los principios del Marco de Privacidad de Datos UE-EE. UU. cuando las circunstancias lo justifiquen. Si una aerolínea vulnera repetidamente el artículo 41712, ello puede poner en duda la veracidad del compromiso de la aerolínea, lo que en supuestos graves puede comportar que se resuelva que la aerolínea no reúne los requisitos para seguir funcionando como tal, y, por consiguiente, se decrete la pérdida de su correspondiente licencia.

Hasta la fecha, el Departamento de Transporte ha recibido pocas reclamaciones por posibles vulneraciones de la privacidad por parte de agentes de venta de billetes o aerolíneas. Cuando surjan, serán investigadas de conformidad con los principios antes descritos.

C. Garantías jurídicas del Departamento de Transporte que benefician a los consumidores de la UE

En virtud del artículo 41712, la prohibición de las prácticas desleales o engañosas en el transporte aéreo o en la comercialización de este tipo de transporte se aplica a los transportistas aéreos y agentes de venta de billetes estadounidenses y extranjeros. El Departamento de Transporte toma con frecuencia medidas contra las aerolíneas estadounidenses y extranjeras en relación con prácticas que afectan tanto a los consumidores estadounidenses como a los extranjeros si las prácticas de la aerolínea tienen lugar en el transcurso del transporte con destino a los EE. UU. o procedente de los EE. UU. El Departamento de Transporte utiliza y continuará utilizando todas las medidas de reparación 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.

([2]) Anteriormente denominada Oficina de Procesos y Ejecución Forzosa en Materia de Aviación (Office of Aviation Enforcement and Proceedings).

([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

También vela por el cumplimiento, respecto de las aerolíneas, de otras leyes específicas cuyas garantías se extienden a los consumidores no estadounidenses, como la Ley de protección de la privacidad infantil en internet. Esta Ley exige, por ejemplo, que los operadores de sitios web y de servicios en línea dirigidos a menores o de sitios web para todos los públicos que recojan a sabiendas información personal de menores de trece años lo notifiquen a los padres y obtengan consentimiento parental verificable. Los sitios web radicados en los EE. UU. y los servicios prestados en dicho país que estén sujetos a la Ley de protección de la privacidad infantil en internet y recojan información personal de menores extranjeros deben hacerlo de conformidad con dicha Ley. Los sitios web radicados en el extranjero y los servicios prestados en el extranjero deben también hacerlo de conformidad con la Ley de protección de la privacidad infantil en internet si se dirigen a menores estadounidenses o si recogen a sabiendas información personal de menores estadounidenses. En la medida en que las aerolíneas estadounidenses o extranjeras que operen en los EE. UU. vulneren la Ley de protección de la privacidad infantil en internet, el Departamento de Transporte tiene competencia para tomar medidas de garantía forzosa del cumplimiento.

II. **Garantía del cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU.**

Si una aerolínea o un agente de venta de billetes decide participar en el Marco de Privacidad de Datos UE-EE. UU. y el Departamento de Transporte recibe una reclamación por el supuesto incumplimiento del Marco por parte de dicha aerolínea o agente de venta de billetes, el Departamento de Transporte puede tomar las medidas necesarias para hacer cumplir el Marco.

A. Priorización de la investigación de las posibles vulneraciones

La Oficina de Protección de los Consumidores del Sector de la Aviación, adscrita al Departamento de Transporte, investiga todas y cada una de las reclamaciones por posibles vulneraciones de los principios del Marco de Privacidad de Datos UE-EE. UU. (incluidas las recibidas de las autoridades de protección de datos de la UE) y toma medidas coercitivas cuando se demuestra que ha habido una vulneración.

Asimismo, la Oficina coopera con la Comisión Federal de Comercio y el Departamento de Comercio y da prioridad a los supuestos de incumplimiento de los compromisos en materia de privacidad asumidos por las entidades participantes en el Marco de Privacidad de Datos UE-EE. UU.

Tras la recepción de la reclamación por vulneración de los principios del Marco de Privacidad de Datos UE-EE. UU., la Oficina de Protección de los Consumidores del Sector de la Aviación puede tomar una serie de medidas como parte de su investigación. Por ejemplo, puede analizar las directrices en materia privacidad del agente de venta de billetes o de la aerolínea, obtener más información del agente de venta de billetes, de la aerolínea o de terceros, realizar consultas con el reclamante y valorar si existe un patrón de vulneraciones o un número considerable de consumidores afectados. Además, puede comprobar si el asunto guarda relación con cuestiones que sean competencia del Departamento de Comercio o de la Comisión Federal de Comercio, valorar la utilidad que tendría realizar medidas de educación de los consumidores o de las empresas, y, si procede, incoar un proceso de ejecución forzosa.

Cuando el Departamento de Transporte descubre posibles vulneraciones de los principios del Marco de Privacidad de Datos UE-EE. UU. por parte de agentes de venta de billetes, se coordina con la Comisión Federal de Comercio. También informa a la Comisión Federal de Comercio y al Departamento de Comercio sobre los resultados de las medidas de garantía del cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU.

B. Tratamiento de las declaraciones falsas o engañosas en cuanto a su participación en el Marco

El Departamento de Transporte está resuelto a investigar las vulneraciones de los principios del Marco de Privacidad de Datos UE-EE. UU., en particular las declaraciones falsas o engañosas en cuanto a la participación en el Marco. Da prioridad a las reclamaciones remitidas por el Departamento de Comercio relacionadas con entidades que considere que declaren engañosamente su participación en el Marco de Privacidad de Datos UE-EE. UU. o que utilicen la marca de certificación del Marco de Privacidad de Datos UE-EE. UU. sin autorización.

Asimismo, cabe señalar que, si en las directrices en materia de privacidad de la entidad se declara que esta promete cumplir los principios del Marco de Privacidad de Datos UE-EE. UU., el mero hecho de no autocertificarse o revalidar su certificación ante el Departamento de Comercio no dispensa, *per se*, a la entidad de la obligación, controlada por el Departamento de Transporte, de cumplir los principios.

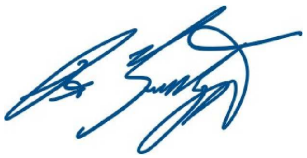
C. Seguimiento y publicidad de las resoluciones de ejecución forzosa por vulneración de los principios del Marco de Privacidad de Datos UE-EE. UU.

La Oficina de Protección de los Consumidores del Sector de la Aviación, adscrita al Departamento de Transporte, también se compromete a supervisar las resoluciones de ejecución forzosa necesarias para garantizar el cumplimiento de los principios del Marco de Privacidad de Datos UE-EE. UU. Concretamente, si la Oficina dicta una resolución de cese de futuras infracciones de los principios del Marco de Privacidad de Datos UE-EE. UU. y del artículo 41712 contra la aerolínea o el agente de venta de billetes infractor, también se encarga de supervisar el cumplimiento de la entidad de dicha resolución. De igual modo, la Oficina garantiza la publicación de las resoluciones que se deriven de los casos relacionados con los principios del Marco de Privacidad de Datos UE-EE. UU. en su sitio web.

Esperamos poder seguir colaborando con nuestros socios federales y las partes interesadas de la UE en cualquier cuestión relacionada con el Marco de Privacidad de Datos UE-EE. UU.

Espero que esta información le sea útil. Si desea preguntarme algo o necesita más información, no dude en dirigirse a mí.

Atentamente,



Pete Buttigieg

ANEXO VI

Departamento de Justicia de los Estados Unidos

División de lo Penal

Oficina del Fiscal General Adjunto Washington, D.C. 20530

23 de junio de 2023

Sra. D.ª Ana Gallego Torres
Directora general de Justicia y Consumidores
Commission européenne / Europese Commissie
Rue Montoyer / Montoyerstraat 59
1049 Bruxelles/Brussel
BÉLGICA

Estimada directora general Gallego Torres:

Por medio de la presente se ofrece una breve visión general de las principales herramientas de investigación utilizadas para la obtención de datos comerciales y otra información escrita de las sociedades de capital estadounidenses a efectos penales o en aras del interés público (civil y regulatorio), incluidas las limitaciones de acceso correspondientes ([1]). Todas las figuras jurídicas descritas en esta carta son no discriminatorias ya que se utilizan para obtener información de sociedades de capital estadounidenses, incluidas las sociedades que se autocertifiquen a efectos del Marco de Privacidad de Datos UE-EE. UU., independientemente de la nacionalidad o el lugar de residencia del interesado. Además, las sociedades de capital que sean objeto de una de estas figuras jurídicas en los EE. UU. pueden impugnarla judicialmente como se explica a continuación ([2]).

Especial atención con respecto a la recogida de datos por parte de los poderes públicos merece la cuarta enmienda de la Constitución de los EE. UU. que contempla que «[n]o se violará el derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias, contra allanamientos e incautaciones fuera de lo razonable, y no se expedirá ningún mandamiento judicial para el efecto, si no es en virtud de causa probable, respaldada en juramento o promesa, y con la descripción en detalle del lugar que habrá de ser allanado y de las personas o efectos que serán objeto de detención o incautación». Como declaró la Corte Suprema de Estados Unidos en el asunto Berger c. State of New York (volumen 388, páginas 41 y 53, del Repertorio Jurisprudencial de los EE. UU., de 1967), el propósito principal de esta enmienda, reconocido en innumerables resoluciones de dicha Corte, es garantizar la privacidad y la seguridad de los particulares frente a injerencias arbitrarias por parte de los funcionarios públicos (en referencia al asunto Camara c. Mun. Court of San Francisco; volumen 387, páginas 523 y 528, del Repertorio Jurisprudencial de los EE. UU., de 1967). En las investigaciones penales nacionales, la cuarta enmienda exige, por lo general, que los agentes policiales obtengan una orden judicial antes de realizar registro alguno (véase el asunto Katz c. United States; volumen 389, páginas 347 y 357, del

([1]) En esta visión general no se describen las herramientas de investigación del ámbito de la seguridad nacional utilizadas por las autoridades policiales en investigaciones sobre terrorismo y otras investigaciones relacionadas con la seguridad nacional, como los requerimientos de seguridad nacional (national security letters), con los que se puede obtener cierta información que obre en fichas de información crediticia, documentos económicos y financieros y registros de transacciones electrónicas y de usuarios digitales (título 12, artículo 3414, título 15, artículo 1681 duovicies y artículo 1681 tervicies, título 18, artículo 2709, y título 50, artículo 3162, del Código de Estados Unidos), ni las utilizadas para la vigilancia electrónica, las órdenes de registro, los documentos empresariales y otro tipo de información en virtud de la Ley de vigilancia de inteligencia exterior (título 50, artículo 1801 y siguientes, del Código de Estados Unidos).

([2]) La presente carta se refiere a las competencias policiales y regulatorias federales. Las vulneraciones del Derecho de los Estados federados son investigadas por las autoridades policiales de los Estados federados y juzgadas por los órganos jurisdiccionales de estos. Las autoridades policiales de los Estados federados deben utilizar las órdenes y los requerimientos contemplados en su Derecho estatal, en esencia, tal como se describe en este documento, con la salvedad de que la figura jurídica del Estado federado en cuestión puede estar sujeta a garantías adicionales que establezca la constitución o la legislación estatal y que superen a las de la Constitución de los EE. UU. Las garantías que establezca el Derecho de los Estados federados deben ser al menos iguales a las de la Constitución de los EE. UU., en particular, aunque no exclusivamente, a las de la cuarta enmienda.

Repertorio Jurisprudencial de los EE. UU., de 1967). Las normas que rigen tales órdenes, como los requisitos de causa probable y especificidad, se aplican a las órdenes de registro físico e incautación, así como a las órdenes que se dictan en virtud de la Ley de comunicaciones almacenadas en relación con el contenido almacenado de las comunicaciones electrónicas, como se expone a continuación. Cuando no sea obligatorio dictar una orden judicial, la actividad de los poderes públicos seguirá estando sujeta a la prueba de verosimilitud contemplada en la cuarta enmienda. Por consiguiente, la propia Constitución garantiza que los poderes públicos estadounidenses no cuenten con atribuciones ilimitadas o arbitrarias para obtener información privada ([3]).

Competencias policiales penales:

Los fiscales federales, que son funcionarios del Departamento de Justicia, y los agentes de investigación federales, incluidos los agentes del Buró Federal de Investigaciones (en lo sucesivo, «FBI», por sus siglas en inglés), que es una autoridad policial del Departamento de Justicia, pueden exigir a las sociedades de capital estadounidenses la presentación de documentos y otra información escrita en el marco de investigaciones penales por medio de varias figuras jurídicas vinculantes, como los requerimientos de los jurados de acusación, los requerimientos administrativos y las órdenes de registro, y pueden interceptar otras comunicaciones gracias a las competencias penales federales en materia de interceptación de comunicaciones y de registro de comunicaciones salientes.

Requerimientos para comparecer ante un jurado de acusación o en juicio: Los requerimientos penales coadyuvan a las investigaciones policiales. Un requerimiento de un jurado de acusación es una intimación oficial que expide el jurado de acusación (generalmente a instancias del fiscal federal) en el marco de una investigación, con jurado de acusación, de una determinada posible vulneración del Derecho penal. El jurado de acusación es una sección instructora del órgano jurisdiccional para la que se nombra un juez penal o un juez de paz. Por medio de dicho requerimiento se puede exigir el testimonio de una persona en el proceso o que esta presente o aporte de otro modo documentos empresariales, información almacenada electrónicamente u otros elementos tangibles. La información debe ser pertinente para la investigación y el requerimiento no puede ser irrazonable por ser excesivo, opresivo u oneroso. El destinatario puede oponerse al requerimiento basándose en estos motivos. Véase el artículo 17 del Código Procesal Penal Federal. En determinadas circunstancias, pueden utilizarse requerimientos para presentar documentos en juicio, por haberse abierto el juicio a petición del jurado de acusación.

Requerimientos administrativos: Los requerimientos administrativos se pueden dictar en las investigaciones civiles y en las penales. En el ámbito penal, son varias las leyes federales que autorizan el uso de los requerimientos administrativos para que se presenten o aporten de otro modo documentos empresariales, información almacenada electrónicamente u otros elementos tangibles en las investigaciones relacionadas con el fraude sanitario, el maltrato infantil, la protección de los servicios secretos y las sustancias controladas, así como las investigaciones del inspector general relacionadas con organismos públicos. Si el Ejecutivo intenta exigir judicialmente la ejecución forzosa de un requerimiento administrativo, el destinatario del requerimiento administrativo puede, al igual que el destinatario de un requerimiento de un jurado de acusación, oponer lo irrazonable del requerimiento por ser este excesivo, opresivo u oneroso.

Órdenes judiciales para el registro de comunicaciones salientes y entrantes: Según las disposiciones relativas al registro de comunicaciones salientes y entrantes, las autoridades policiales pueden solicitar una resolución judicial para conseguir, en tiempo real, información básica sobre el marcado, el enrutamiento, el direccionamiento y la señalización de un número de teléfono o de una dirección de correo electrónico tras haber comprobado que la información en cuestión es pertinente para una investigación penal en curso. Véase el título 18, artículos 3121 a 3127, del Código de Estados Unidos. El uso o instalación de un dispositivo de este tipo sin la debida autorización es un delito federal.

Ley de privacidad de las comunicaciones electrónicas: Existen otras reglas por las que se rige el acceso de los poderes públicos a la información de los usuarios digitales, los datos de tráfico y el contenido almacenado de las comunicaciones que obran en poder de las empresas de servicios de internet, las compañías telefónicas y otras empresas externas de servicios, de conformidad con el título II de la Ley de privacidad de las comunicaciones electrónicas, a saber, las de la Ley de comunicaciones almacenadas (título 18, artículos 2701 a 2712, del Código de Estados Unidos). La Ley de comunicaciones almacenadas establece un sistema legal de derechos de privacidad, que limitan el acceso de las autoridades policiales a los datos de los clientes y abonados de las empresas de servicios de internet, más garantista que el del ordenamiento constitucional. Esta Ley también confiere una mayor protección de la privacidad cuanto mayor sea el nivel

([3]) Los órganos jurisdiccionales estadounidenses aplican regularmente los principios de la cuarta enmienda sobre la protección de los intereses en materia de privacidad y seguridad que se han comentado anteriormente a los nuevos tipos de instrumentos de investigación policial que se desarrollan gracias a la evolución de la tecnología. Por ejemplo, en 2018 la Corte Suprema dictaminó que la obtención por parte de los poderes públicos, en el marco de una investigación policial, del historial de ubicaciones de un teléfono móvil que obre en poder de la correspondiente empresa de telefonía móvil durante un período de tiempo prolongado constituye un «registro», por lo que, en virtud de la cuarta enmienda, es necesaria una orden judicial (volumen 138, página 2206, del Repertorio de la Corte Suprema, de 2018).

de injerencia que represente la recogida de los datos. Las autoridades policiales deben solicitar un requerimiento para obtener información del registro de abonados, las direcciones IP, los sellos de tiempo correspondientes y la información de la facturación. Para la mayoría de la demás información almacenada no sustantiva, como los encabezados de los correos electrónicos sin el asunto, las autoridades policiales deben aducir al juez hechos concretos que demuestren que la información que se pretende recabar es pertinente y sustancial para una investigación penal en curso. Para obtener el contenido almacenado de las comunicaciones electrónicas, las autoridades policiales penales deben, por lo general, solicitar una orden judicial que se fundamente en la existencia de una causa probable para considerar que la cuenta en cuestión alberga pruebas de un delito. La Ley de comunicaciones almacenadas contempla también penas y supuestos en que se puede exigir responsabilidad civil ([4]).

Órdenes judiciales de vigilancia contempladas en la Ley federal de interceptación de comunicaciones: Por otra parte, las autoridades policiales pueden interceptar en tiempo real comunicaciones por cable, orales o electrónicas a efectos de investigaciones penales con arreglo a la Ley federal de interceptación de comunicaciones. Véase el título 18, artículos 2510 a 2523, del Código de Estados Unidos. Para realizar la interceptación es necesaria una resolución judicial en la que el juez considere, entre otros aspectos, que existe una causa probable para considerar que la escucha o la interceptación electrónica demostrará que se ha cometido un delito federal o permitirá conocer el paradero de un fugitivo de la justicia. La Ley contempla penas y supuestos de exigibilidad de responsabilidad civil por la vulneración de las disposiciones sobre la interceptación de las comunicaciones.

Orden de registro (artículo 41 del Código Procesal Penal Federal): Las autoridades policiales pueden registrar físicamente bienes inmuebles en los EE. UU. cuando así se autorice judicialmente. Las autoridades policiales deben demostrar al juez que existe una causa probable de que se ha cometido un delito o se va a cometer un delito y que es probable que los elementos relacionados con el delito se encuentren en el lugar especificado en la orden. Esta figura se utiliza generalmente cuando es necesario que la policía registre físicamente un inmueble debido al peligro de destrucción de las pruebas si se traslada un requerimiento u otro tipo de orden equivalente a la sociedad de capital. La persona objeto de un registro o cuyo patrimonio sea objeto de registro puede impugnar las pruebas obtenidas o derivadas de un registro ilícito si dichas pruebas se aportan en su contra durante el proceso penal. Véase el asunto Mapp c. Ohio; volumen 367, página 643, del Repertorio Jurisprudencial de los EE. UU., de 1961. Cuando se exija al titular de los datos que comunique los datos en virtud de una orden judicial, la parte obligada puede impugnar la orden si esta resulta excesivamente onerosa. Véase el asunto In re Application of United States, volumen 610, segunda serie del Repertorio Jurisprudencial Federal, páginas 1148 a 1157 (Corte de Apelaciones del Tercer Circuito, 1979), donde se sostiene que el respeto de las debidas garantías procesales exige resolver la cuestión de la onerosidad antes de obligar a la compañía telefónica a prestar ayuda para ejecutar la orden de registro; véase asimismo el asunto In re Application of United States, volumen 616, segunda serie del Repertorio Jurisprudencial Federal, página 1122 (Corte de Apelaciones del Noveno Circuito, 1980), donde se llega a la misma conclusión basándose en la potestad de control judicial.

Directrices y directivas del Departamento de Justicia: Además de estas limitaciones constitucionales, legales y judiciales sobre el acceso de los poderes públicos a los datos, el secretario de Justicia ha aprobado directrices por las que se fijan límites adicionales para el acceso de las autoridades policiales a los datos; se establecen también garantías de la privacidad y las libertades civiles. Por ejemplo, en la Directrices del secretario de Justicia, de septiembre de 2008, sobre las operaciones nacionales del FBI (en lo sucesivo, «Directrices sobre el FBI»), que se pueden consultar en http://www.justice.gov/archive/opa/docs/guidelines.pdf, se establecen límites al uso de medios de investigación para obtener información relacionada con investigaciones de delitos federales. Estas Directrices exigen al FBI que use métodos de investigación lo menos invasivos posible, teniendo en cuenta el efecto en la privacidad y en las libertades civiles y el posible daño a la reputación de la institución. Además, señalan que es axiomático que el FBI debe llevar a cabo las investigaciones y demás actuaciones de una manera lícita y razonable que respete la libertad y la privacidad y evite injerencias innecesarias en las vidas de los ciudadanos que acatan las normas. Véanse las Directrices sobre el FBI, página 5. El FBI ha implantado estas Directrices a través de la Guía de Investigaciones y Operaciones Nacionales del FBI, que se puede consultar en inglés en https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29; es un manual exhaustivo que recoge pormenorizadamente los límites al 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. Figuran reglas y directrices sobre las limitaciones a las actividades de investigación de los fiscales federales en el Manual de Justicia, se puede consultar en inglés en http://www.justice.gov/usam/united-states-attorneys-manual.

Competencias civiles y regulatorias (interés público):

([4]) Además, el artículo 2705, letra b), de la Ley de comunicaciones almacenadas faculta a los poderes públicos para solicitar órdenes judiciales, siempre que demuestren la necesidad de protección de la investigación, por las que se prohíba a la empresa de servicios de comunicaciones correspondiente notificar voluntariamente a sus usuarios el empleo de la figura jurídica contemplada en la Ley de comunicaciones almacenadas. En octubre de 2017, el secretario de Justicia adjunto, Rod Rosenstein, publicó una circular dirigida a los funcionarios y cargos del Departamento de Justicia con instrucciones para garantizar que las solicitudes de tales medidas cautelares se ajusten a los hechos y cuestiones específicos de la investigación; en ella se establece que el plazo máximo por el que se puede intentar retrasar la notificación es de un año con carácter general. En mayo de 2022, la secretaria de Justicia adjunta, Lisa Mónaco, publicó unas directrices complementarias sobre este tema, por las que, entre otros aspectos, se establecían requisitos internos que deben cumplirse para que el Departamento de Justicia pueda aprobar las solicitudes de prórroga de estas medidas cautelares por encima del período inicial de un año y se exigía el cese de tales medidas al término de la investigación.

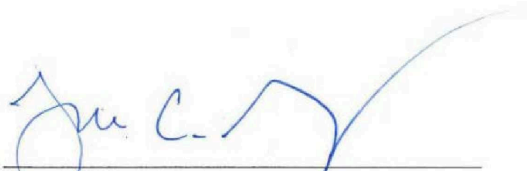
Existen también límites importantes al acceso civil o regulatorio (esto es, por motivos de interés público) a los datos que obran en poder de las sociedades de capital estadounidenses. Los organismos con competencias civiles y regulatorias pueden enviar requerimientos a las sociedades de capital para que estas presenten documentos empresariales, información almacenada electrónicamente u otros elementos tangibles. La competencia de estos organismos para enviar requerimientos administrativos o civiles está limitada no solo por las leyes por las que aquellos son creados, sino también por la revisión judicial independiente de los requerimientos que se realiza cuando se exige su cumplimiento por la vía de la ejecución forzosa. Véase, por ejemplo, el artículo 45 del Código Procesal Civil Federal (Federal Rules of Civil Procedure). Estos organismos solo pueden solicitar el acceso a los datos pertinentes para las cuestiones comprendidas en su ámbito regulatorio. Además, el destinatario de un requerimiento administrativo puede impugnar judicialmente la ejecución forzosa del mismo mediante la aportación de pruebas de que la actuación del organismo no se ajusta al principio de verosimilitud descrito anteriormente.

Existen otros fundamentos con los que las sociedades de capital pueden oponerse a las solicitudes de datos de los organismos administrativos, que dependen del sector al que pertenecen y el tipo de datos que obran en su poder. Por ejemplo, las entidades financieras pueden oponerse a los requerimientos administrativos de cierto tipo de información alegando que constituyen una vulneración de la Ley del secreto bancario y su normativa de desarrollo (título 31, artículo 5318, del Código de Estados Unidos; título 31, capítulo X, del Código de Reglamentos Federales). Otras empresas pueden ampararse en la Ley sobre fichas de información crediticia justas (título 15, artículo 1681 ter, del Código de Estados Unidos) o numerosas leyes específicas de su sector. El uso indebido de estos requerimientos por parte de un organismo puede comportar la responsabilidad del mismo o la responsabilidad personal de los funcionarios del organismo. Véase, por ejemplo, la Ley del derecho a la privacidad financiera (título 12, artículos 3401 a 3423, del Código de Estados Unidos). Los órganos jurisdiccionales de los EE. UU. son, por consiguiente, los guardianes del empleo correcto de los requerimientos regulatorios y realizan un control independiente de la actuación de los organismos federales.

Por último, toda competencia legal que tengan las autoridades administrativas para realizar una incautación física de los documentos de una sociedad de capital estadounidense durante un registro administrativo debe cumplir los requisitos que impone la cuarta enmienda. Véase el asunto See c. City of Seattle; volumen 387, página 541, del Repertorio Jurisprudencial de los EE. UU., de 1967.

Conclusión:

Todas las actuaciones policiales y regulatorias realizadas en los EE. UU. deben ajustarse a la normativa aplicable, en particular la Constitución de los EE. UU., la legislación y los reglamentos. Tales actuaciones deben cumplir también las directrices aplicables, incluidas las directrices del secretario de Justicia que rijan las actuaciones policiales federales. El marco jurídico antes descrito limita la competencia de las autoridades regulatorias y policiales estadounidenses para obtener información de sociedades de capital estadounidenses, independientemente de que la información se refiera a ciudadanos estadounidenses o a ciudadanos de países extranjeros, y dispone el control judicial de las solicitudes de datos efectuadas por los poderes públicos en ejercicio de estas competencias.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ANEXO VII

OFICINA DEL DIRECTOR DE INTELIGENCIA NACIONAL OFICINA DEL ASESOR GENERAL

WASHINGTON, DC 20511

9 de diciembre de 2022

Leslie B. Kiernan,
Asesora general
Departamento de
Comercio de los EE. UU., 1401 Constitution
Ave., NW Washington, DC 20230

Estimada señora Kiernan:

El 7 de octubre de 2022, el presidente Biden aprobó el Decreto Presidencial n.º 14086, titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos», que redobla el conjunto de garantías rigurosas en materia de privacidad y libertades civiles que son de aplicación a las actividades de inteligencia de señales estadounidenses. Entre dichas garantías se cuentan: la exigencia de que las actividades de inteligencia de señales tengan fines legítimos específicos; la prohibición explícita de que tales actividades se realicen con fines específicos prohibidos; el establecimiento de procedimientos novedosos para asegurar que las actividades de inteligencia de señales coadyuven a lograr fines legítimos y no contribuyan a la consecución de fines prohibidos; la exigencia de que tales actividades se lleven a cabo únicamente tras determinar, en una valoración razonable de todos los factores pertinentes, que son necesarias para avanzar en una prioridad de inteligencia validada y solo de manera proporcionada a la prioridad de inteligencia validada para la que hayan sido autorizadas; ordenar a los servicios de la Comunidad de Inteligencia que actualicen sus directrices y procedimientos a fin de incorporar las garantías en materia de inteligencia de señales que establece el Decreto Presidencial. Más importante aún, el Decreto Presidencial también crea un órgano independiente y vinculante que permite a los particulares de los «Estados cualificados», designados con arreglo a el Decreto Presidencial, solicitar reparación si consideran que han sido objeto de actividades ilícitas de inteligencia de señales estadounidenses, en particular actividades que vulneren las garantías establecidas en el Decreto Presidencial.

La aprobación del Decreto Presidencial n.º 14086 por parte del presidente Biden marcó la culminación de más de un año de negociaciones minuciosas entre los representantes de la Comisión Europea y de los Estados Unidos («EE. UU.») y sientan las bases para que los EE. UU. tomen medidas para cumplir sus compromisos en el Marco de Privacidad de Datos UE-EE. UU. En consonancia con el espíritu de cooperación que hizo posible el Marco, entiendo que usted ha recibido dos series de preguntas de la Comisión Europea sobre la manera en que la Comunidad de Inteligencia dará cumplimiento al Decreto Presidencial. Quisiera tratar estas preguntas por medio de la presente.

Artículo 702 de la Ley de vigilancia de inteligencia exterior, de 1978

La primera serie de preguntas se refiere al artículo 702 de la Ley de vigilancia de inteligencia exterior, que autoriza la recogida de información de inteligencia exterior respecto de personas no estadounidenses que se considere que es razonable que se encuentren fuera de los EE. UU., con la ayuda obligada de las empresas de servicios de comunicación electrónica. En concreto, las preguntas se refieren a la interrelación entre dicha disposición y el Decreto Presidencial n.º 14086 y las demás garantías que se aplican a las actividades realizadas en virtud del referido artículo 702.

Para empezar, podemos confirmar que la Comunidad de Inteligencia debe aplicar las garantías establecidas en el Decreto Presidencial n.º 14086 a las actividades realizadas en virtud del referido artículo 702.

También son de aplicación muchas otras garantías al uso de la facultad contemplada en el referido artículo 702 por parte de los poderes públicos. Por ejemplo, todas las certificaciones que se presenten a efectos del referido artículo 702 deben estar firmadas tanto por el secretario de Justicia como por el director de Inteligencia Nacional, y el Ejecutivo debe presentar, para su aprobación, todas estas certificaciones al Tribunal de Vigilancia de Inteligencia Exterior (Foreign Intelligence Surveillance Court), que está formado por magistrados independientes y vitalicios que ejercen su cargo por períodos de siete años no prorrogables. En estas certificaciones se especifican las categorías de información de inteligencia exterior que se pretende recoger, que deben ajustarse a la definición legal de información de inteligencia exterior, respecto de personas no estadounidenses que se considere que es razonable que se encuentren fuera de los EE. UU. Algunas de estas certificaciones han tenido por objeto información sobre terrorismo internacional y otros temas, como la obtención de información sobre armas de destrucción masiva. Las certificaciones anuales deben presentarse, para su aprobación, al Tribunal de Vigilancia de Inteligencia Exterior en un expediente que incluya las certificaciones del secretario de Justicia y del director de Inteligencia Nacional, las declaraciones juradas de determinados jefes de servicios de inteligencia, así como los procedimientos de selección de objetivos, de minimización y de consulta seguidos, que son vinculantes para el Ejecutivo. El procedimiento de selección de objetivos supone, entre otras cosas, que la Comunidad de Inteligencia debe concluir razonablemente, atendiendo a todas las circunstancias, que es probable que dirigiéndose contra el objetivo de la solicitud se pueda recoger la información de inteligencia exterior mencionada en la certificación presentada con arreglo al referido artículo 702.

Por otra parte, al recoger información en virtud del artículo 702 de la Ley de vigilancia de inteligencia exterior, la Comunidad de Inteligencia debe: justificar por escrito la conclusión, en el momento en que se seleccione el objetivo, de que se espera que el objetivo tenga, reciba o probablemente comunique la información de inteligencia exterior mencionada en la certificación presentada con arreglo al referido artículo 702; confirmar que el procedimiento de selección de objetivos se ajusta a la norma contemplada en el referido artículo 702; y dejar de recoger la información si deja de cumplirse dicha norma. Véase el escrito del Ejecutivo de los EE. UU. al Tribunal de Vigilancia de Inteligencia Exterior, titulado «Resumen de 2015 de exigencias destacadas del artículo 702» (2015 Summary of Notable Section 702 Requirements), pp. 2 y 3 (15 de julio de 2015).

Exigir a la Comunidad de Inteligencia que consigne por escrito su conclusión de que la selección del objetivo de la certificación a efectos del referido artículo 702 cumple las normas aplicables, y confirmar periódicamente la validez de esa conclusión, y facilita la supervisión por parte del Tribunal de Vigilancia de Inteligencia Exterior de la actividad de recogida de información que realiza la Comunidad de Inteligencia. Los funcionarios del Departamento de Justicia encargados de la supervisión en materia de inteligencia, que realizan esta función de forma independiente respecto de las operaciones de inteligencia exterior, revisan con periodicidad bimestral la conclusión y justificación de las certificaciones aprobadas. El servicio del Departamento de Justicia que desempeña esta función está obligado, en virtud de una norma que estableció el Tribunal de Vigilancia de Inteligencia Exterior hace tiempo, a informar a dicho Tribunal de cualquier incumplimiento de los procedimientos aplicables. Esta obligación de información, junto con las reuniones periódicas entre el Tribunal de Vigilancia de Inteligencia Exterior y dicho servicio del Departamento de Justicia en relación con la supervisión de las certificaciones presentadas con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior, permite al Tribunal de Vigilancia de Inteligencia Exterior velar por el cumplimiento de dicho artículo y los procedimientos conexos y, en general, garantizar la legalidad de las actuaciones del Ejecutivo. En particular, el Tribunal de Vigilancia de Inteligencia Exterior puede hacer esto de varias maneras, en particular dictando resoluciones vinculantes por las que invalide la recogida de datos por parte del Ejecutivo respecto de un objetivo o por las que se modifique o retrase la recogida de los datos en virtud del referido artículo 702. El Tribunal de Vigilancia de Inteligencia Exterior también puede exigir al Ejecutivo que presente informes o resúmenes complementarios sobre su cumplimiento del procedimiento de selección de objetivos o de otros procedimientos, o exigir cambios específicos en dichos procedimientos.

Recogida masiva de datos de inteligencia de señales

La segunda serie de preguntas se refiere a la recogida masiva de datos de inteligencia de señales, que se define en el Decreto Presidencial n.º 14086 como la recogida autorizada de grandes cantidades de datos de inteligencia de señales que, por consideraciones técnicas u operativas, se adquieren sin emplear criterios de discriminación (por ejemplo, sin utilizar identificadores o criterios de selección específicos).

Con respecto a estas preguntas, observamos en primer lugar que ni la Ley de vigilancia de inteligencia exterior ni los requerimientos de seguridad nacional permiten la recogida masiva de datos. Con respecto a la Ley de vigilancia de inteligencia exterior:

— En los títulos I y III de dicha Ley, sobre la autorización, respectivamente, de la vigilancia electrónica y de los registros físicos, se exige una resolución judicial para realizar estas actuaciones (salvo en supuestos restringidos, como las situaciones de emergencia) y que siempre se demuestre que existe una causa probable para pensar que el objetivo es una potencia extranjera o un agente de una potencia extranjera. Véase el título 50, artículos 1805 a 1824, del Código de Estados Unidos.

— La Ley de libertad de los Estados Unidos, de 2015, modificó el título IV de la Ley de vigilancia de inteligencia exterior, por el que se podían emplear dispositivos de registro de comunicaciones salientes y entrantes si se contaba con una resolución judicial (excepto en situaciones de emergencia), para exigir al Ejecutivo que fundamentase sus solicitudes en un criterio de selección específico. Véase el título 50, artículo 1842, letra c), apartado 3, del Código de Estados Unidos.

— En virtud del título V de la Ley de vigilancia de inteligencia exterior, por el que el Buró Federal de Investigaciones (en lo sucesivo, «FBI», por sus siglas en inglés) puede incautarse de ciertos tipos de documentos empresariales, es necesario que a la solicitud siga una resolución judicial que especifique que concurren circunstancias específicas y demostrables que llevan a pensar que la persona a quien pertenecen los documentos es una potencia extranjera o un agente de una potencia extranjera. Véase el título 50, artículo 1862, letra b), apartado 2, punto B), del Código de Estados Unidos ([1]).

— Por último, el artículo 702 de la Ley de vigilancia de inteligencia exterior permite seleccionar como objetivos de la adquisición de información de inteligencia exterior a personas de las que se tengan motivos fundados para pensar que se encuentran fuera de los EE. UU. Véase el título 50, artículo 1881 *bis*, letra a), del Código de Estados Unidos. Por lo tanto y como ha señalado la Junta de Supervisión de la Privacidad y las Libertades Civiles (Privacy and Civil Liberties Oversight Board), la recogida de datos por parte del Ejecutivo en virtud del artículo 702 de la Ley de vigilancia de inteligencia exterior consiste enteramente en la selección de personas físicas como objetivos y la adquisición de las comunicaciones relacionadas con ellas; el Ejecutivo debe tener motivos para pensar que de estas personas podrá obtener ciertos tipos de inteligencia extranjera, es decir, esta figura no puede servir para recoger comunicaciones de forma masiva. Junta de Supervisión de la Privacidad y las Libertades Civiles, Informe sobre el programa de vigilancia derivado de la aplicación del artículo 702 de la Ley de vigilancia de inteligencia exterior (Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act), de 2 de julio de 2014, página 103 ([2]).

Con respecto a los requerimientos de seguridad nacional, la Ley de libertad de los Estados Unidos, de 2015, impone que en dichos requerimientos se emplee un criterio de selección específico. Véase el título 12, artículo 3414, letra a), apartado 2, el título 15, artículo 1681 *duovicies* y artículo 1681 *tervicies*, letra a), y el título 18, artículo 2709, letra b), del Código de Estados Unidos.

Por otro lado, el Decreto Presidencial n.º 14086 dispone que se debe favorecer la recogida selectiva de información y que, cuando la Comunidad de Inteligencia realice una recogida masiva de información, tal recogida de datos de inteligencia de señales solo debe autorizarse si se demuestra que la información necesaria para avanzar en la prioridad de inteligencia validada no se puede conseguir razonablemente mediante una recogida selectiva de información [artículo 2, letra c), inciso ii), punto A), del Decreto Presidencial n.º 14086].

A mayor abundamiento, el Decreto Presidencial n.º 14086 establece garantías adicionales en los supuestos en que la Comunidad de Inteligencia demuestra que la recogida masiva de información se ajusta a la normativa aplicable. En concreto, el Decreto Presidencial exige a la Comunidad de Inteligencia que, al realizar la recogida masiva de información, aplique métodos razonables y medidas técnicas para limitar los datos que se recogen únicamente a lo necesario para avanzar en la prioridad de inteligencia validada, de modo que se minimice la recogida de información no pertinente (*ibidem*). El Decreto Presidencial también dispone que las actividades de inteligencia de señales, entre las que se incluyen la consulta de la inteligencia de señales obtenida con la recogida masiva de información, debe realizarse tras determinar, en una valoración razonable de todos los factores pertinentes, que son necesarias para avanzar en la prioridad de inteligencia validada [*ibidem*, artículo 2, letra a), inciso ii), punto A)]. El Decreto Presidencial desarrolla este principio al establecer que la Comunidad de Inteligencia solo puede consultar la inteligencia de señales no minimizada obtenida con la recogida masiva de información para lograr alguna de las seis finalidades admitidas, y que tales consultas deben realizarse con arreglo a directrices y procedimientos que tengan debidamente en cuenta el efecto de las consultas en la privacidad y las libertades civiles de todas las personas, independientemente de su nacionalidad o de su lugar de residencia [*ibidem*, artículo 2, letra c), inciso iii), punto D)]. Por último, el Decreto Presidencial regula la manipulación, la seguridad y el control del acceso respecto de los datos recogidos [*ibidem*, artículo 2, letra c), inciso iii), puntos A) y B)].

* * * * *

Esperamos que estas aclaraciones le sean de utilidad. No dude en ponerse en contacto con nosotros si tiene más preguntas sobre la forma en que la Comunidad de Inteligencia de los EE. UU. tiene previsto dar cumplimiento a el Decreto Presidencial n.º 14086.

([1]) Desde 2001 hasta 2020, el FBI podía en virtud del título V de la FISA pedir autorización al Tribunal de Vigilancia de Inteligencia Exterior para incautarse de elementos tangibles pertinentes para determinadas investigaciones autorizadas. Véase el artículo 215 de la Ley de Libertad de EE. UU., de 2001 (Ley pública n.º 107-56; Repertorio de leyes del Congreso, volumen 115, página 272). Este precepto, que ya no está en vigor, otorgaba antes al Ejecutivo la competencia para recoger de forma masiva metadatos telefónicos. Sin embargo, incluso antes de que el precepto dejara de estar en vigor, la Ley de libertad de los Estados Unidos ya lo había modificado de modo que el Ejecutivo tuviese que fundamentar sus solicitudes en un criterio de selección específico. Véase el artículo 103 de la Ley de Libertad de los EE. UU., de 2015 (Ley pública n.º 114-23; Repertorio de leyes del Congreso, volumen 129, página 268).

([2]) En virtud de los artículos 703 y 704, que autorizan a la Comunidad de Inteligencia a seleccionar como objetivos a personas estadounidenses en el extranjero, se exige contar con una resolución judicial (excepto en situaciones de emergencia) y que siempre se demuestre que existe una causa probable para pensar que el objetivo es una potencia extranjera, un agente de una potencia extranjera o un funcionario o empleado de una potencia extranjera (título 50, artículos 1881 *ter* y 1881 *quater*, del Código de Estados Unidos).

Sincerely,

Christopher C. FONZONE
Asesor general

ANEXO VIII

Lista de abreviaciones

En la presente Decisión de Ejecución figuran las abreviaciones siguientes:

AEA	Asociación Estadounidense de Arbitraje
Reglamento sobre el Tribunal de Recurso	Reglamento sobre el Tribunal de Recurso en Materia de Protección de Datos
CIA	Agencia Central de Inteligencia
TJUE	Tribunal de Justicia de la Unión Europea
Decisión	Decisión de Ejecución de la Comisión relativa a la adecuación del nivel de protección de los datos personales en el Marco de Privacidad de Datos UE-EE. UU. con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo
Departamento de Comercio	Departamento de Comercio de los Estados Unidos
Departamento de Justicia	Departamento de Justicia de los Estados Unidos
Departamento de Transporte	Departamento de Transporte de los Estados Unidos
APD	Autoridades de protección de datos
EEE	Espacio Económico Europeo
Decreto Presidencial n.º 12333	Decreto «Actividades de inteligencia de los Estados Unidos»
Decreto Presidencial n.º 14086	Decreto Presidencial de 7 de octubre de 2022, titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos»
Marco	Marco de Privacidad de Datos UE-EE. UU.
FBI	Buró Federal de Investigaciones
Reglamento (UE) 2016/679	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

Los principios en materia de privacidad	Principios del Marco de Privacidad de Datos UE-EE. UU.
EE. UU.	Estados Unidos de América
UE	Unión Europea