COMISIÓN
EUROPEA

Bruselas, 9.10.2024
COM(2024) 451 final

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

sobre la primera revisión periódica del funcionamiento de la decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE. UU.

1. PRIMERA REVISIÓN PERIÓDICA: ANTECEDENTES, PREPARACIÓN Y PROCESO

En su Decisión de 10 de julio de 2023 (la «decisión de adecuación»), la Comisión consideró que el Marco de Privacidad de Datos UE-EE. UU. ofrece un nivel de protección adecuado de los datos personales transferidos desde la Unión Europea a entidades establecidas en los Estados Unidos de América[1]. La decisión de adecuación exige a la Comisión que lleve a cabo revisiones periódicas, la primera de las cuales debe tener lugar un año después de la fecha de notificación de la decisión de adecuación a los Estados miembros. El presente informe concluye esta primera revisión.

Tal como exige el considerando 211 de la decisión de adecuación, esta primera revisión, que se ha realizado después del primer año de funcionamiento del nuevo Marco, se centró en verificar si todos los elementos previstos en el Marco se han implantado y si funcionan eficazmente. La revisión abarcó todos los aspectos del funcionamiento del Marco, especialmente dado los cambios jurídicos que han tenido lugar desde la adopción de la decisión de adecuación.

Para preparar la revisión, la Comisión recabó información de partes interesadas pertinentes, en particular de organizaciones no gubernamentales (ONG) con experiencia en derechos digitales y privacidad[2], entidades certificadas con arreglo al Marco de Privacidad de Datos, a través de sus organismos profesionales[3], así como de las autoridades estadounidenses que participan en la aplicación del marco. Además, la Comisión también ha recabado observaciones la sociedad en general a través de una convocatoria de datos específica en el portal «Díganos lo que piensa»[4].

Los días 18 y 19 de julio de 2024 se celebró una reunión de revisión en Washington D. C. Fue inaugurada por el comisario de Justicia y Consumidores de la UE, Didier Reynders, y la secretaria de Comercio estadounidense, Gina Raimondo[5].

---

[1] 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.

[2] La Comisión envió un cuestionario a nueve ONG (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center y Center for Democracy and Technology), centrado en las novedades pertinente del marco jurídico estadounidense, los mecanismos de supervisión y garantía del cumplimiento y el funcionamiento de las vías de impugnación. Los servicios de la Comisión y los representantes del CEPD también se reunieron en línea con estas ONG el 9 de julio de 2024.

[3] La Comisión envió un cuestionario a nueve asociaciones comerciales (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association y Engine), centrado en la experiencia de las empresas certificadas con arreglo al Marco de Privacidad de Datos, en particular el proceso de certificación, las medidas adoptadas para cumplir los principios del Marco de Privacidad de Datos, los mecanismos para tramitar las solicitudes y reclamaciones de particulares, etc.

[4] Las observaciones recibidas están disponibles en el enlace siguiente: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-Marco-de-Privacidad-de-Datos-UE-EE-UU-informe-de-la-Comision-sobre-el-funcionamiento-del-Marco_es.

[5] La reunión de revisión se organizó por temas y cada punto específico del orden del día se inició con una breve presentación a cargo de la autoridad estadounidense, el representante de la UE o la entidad pertinentes, seguida de una sesión detallada de preguntas y respuestas. Los «aspectos comerciales» del Marco (es decir, la aplicación y el control del cumplimiento de los requisitos aplicables a las empresas certificadas con arreglo al Marco de

Por lo que se refiere a la UE, la revisión fue realizada por representantes de la Dirección General de Justicia y Consumidores de la Comisión Europea, junto con cinco representantes designados por el Comité Europeo de Protección de Datos (CEPD), procedentes de diferentes autoridades nacionales de protección de datos (APD) y el Supervisor Europeo de Protección de Datos[6]. En representación de los Estados Unidos, participaron representantes del Departamento de Comercio (Department of Commerce), del Departamento de Estado (Department of State), de la Comisión Federal de Comercio (Federal Trade Commission, FTC), del Departamento de Transporte (Department of Transportation), de la Oficina del Director de Inteligencia Nacional (Office of the Director of National Intelligence, ODNI), del Departamento de Justicia (Department of Justice), de la Oficina del Inspector General de los Servicios de Inteligencia (Inspector General for the Intelligence Community), así como miembros de la Junta de Supervisión de la Privacidad y las Libertades Civiles (Privacy and Civil Liberties Oversight Board, PCLOB). Además, representantes de organizaciones que ofrecen servicios independientes de resolución de controversias y de la Asociación Estadounidense de Arbitraje facilitaron información durante las sesiones de revisión pertinentes. Asimismo, la revisión se elaboró sobre la base de presentaciones a cargo de entidades certificadas con arreglo al Marco de Privacidad de Datos sobre la manera en que las empresas cumplen con los requisitos del Marco.

Las constataciones de la Comisión también se basaron en material de dominio público, como resoluciones judiciales, normas de desarrollo y procedimientos de las autoridades estadounidenses pertinentes, informes y estudios elaborados por organizaciones no gubernamentales, informes de transparencia publicados por empresas certificadas con arreglo al Marco de Privacidad de Datos, informes anuales de organismos de supervisión independientes, así como informes de los medios de comunicación.

2. CONSTATACIONES

2.1. Aspectos comerciales

2.1.1. El proceso de certificación

A fin de poder recibir los datos personales transferidos desde la UE con arreglo al Marco de Privacidad de Datos, las empresas estadounidenses deben certificar ante el Departamento de Comercio su cumplimiento de las exigencias específicas en materia de protección de datos (los «principios del Marco de Privacidad de Datos») y revalidar cada año la certificación. La certificación exige que las empresas se sometan a las competencias de investigación y ejecución forzosa de la Comisión Federal de Comercio o del Departamento de Transporte, declaren públicamente su compromiso de cumplir los principios del Marco de Privacidad de Datos, publiquen sus directrices en materia de privacidad y poner en práctica estos requisitos íntegramente[7]. Antes de finalizar una certificación, el Departamento de Comercio verifica si las empresas cumplen todos los requisitos para la certificación[8].

Privacidad de Datos) se trataron el primer día, mientras que las cuestiones relativas al acceso de los poderes públicos a los datos personales se debatieron el segundo día.

[6] Los representantes de la Comisión y del CEPD se reunieron el 12 de junio y el 10 de julio de 2024 para preparar la revisión, debatir las aportaciones recibidas y determinar qué aspectos requieren una recopilación de información y aclaraciones adicionales.

[7] Sección I, punto 2, del anexo I de la decisión de adecuación.

[8] Anexo III de la decisión de adecuación.

En la reunión de revisión, el Departamento de Comercio explicó que, en este primer año del Marco de Privacidad de Datos, la atención se ha centrado en poner en marcha el proceso de certificación, en particular en el desarrollo de herramientas informáticas específicas, la actualización de los procedimientos, la colaboración con las empresas y la realización de otras actividades de divulgación y concienciación. En la fecha de la reunión de revisión, más de 2 800 empresas se habían certificado con arreglo al Marco de Privacidad de Datos. Esto implica que, en su primer año de funcionamiento, más empresas se han certificado con arreglo al Marco de Privacidad de Datos que con arreglo al marco anterior, el Escudo de la privacidad[9]. Según la información proporcionada por el Departamento de Comercio, el 70 % de los participantes son pymes y un gran número de empresas participantes (47 %) pertenecen al sector de las tecnologías de la información y de las comunicaciones (TIC). Además, el 60 % de las empresas están certificadas exclusivamente para datos no relacionados con recursos humanos, el 2,5 % exclusivamente para datos de recursos humanos y el 37,5 % para ambos tipos de datos.

El Departamento de Comercio ha adoptado los procedimientos necesarios para tramitar las solicitudes de las empresas. Las empresas deben presentar sus solicitudes de certificación en el sitio web del Departamento de Comercio sobre el Marco de Privacidad de Datos (https://www.dataprivacyframework.gov/). Contiene información sobre cómo adherirse al Marco de Privacidad de Datos[10] y sobre las obligaciones que asumen las empresas en dicho Marco[11]. Un equipo específico del Departamento de Comercio, bajo la responsabilidad de un director específico para el Marco de Privacidad de Datos, se encarga de todos los aspectos relacionados con la gestión y la administración del Marco, incluidos el proceso de certificación y el control del cumplimiento. Cada solicitud se asigna a un empleado específico que sigue siendo responsable de la empresa correspondiente a lo largo de todo el proceso de certificación.

Para certificarse con arreglo al Marco, las empresas presentan su solicitud, incluido un proyecto de directrices en materia privacidad. El Departamento de Comercio comprueba si cumple los requisitos pertinentes del Marco de Privacidad de Datos. Si las entidades desean certificar distintos entes dentro de un grupo de empresas (por ejemplo, diferentes filiales), el Departamento de Comercio pide y revisa unas directrices globales en materia de privacidad que indiquen claramente todos los entes a las que se aplican o directrices separadas para cada uno. Asimismo, el Departamento de Comercio verifica con el órgano independiente de impugnación[12] indicado en la solicitud si las entidades están dadas de alta realmente ante él. En el caso de las empresas que seleccionan el panel de las autoridades de protección de datos (por ejemplo, porque tratan datos de recursos humanos), el Departamento de Comercio comprueba si las empresas han pagado las tasas exigidas para hacer uso del panel. En caso necesario, el Departamento de Comercio también verifica si el solicitante está sujeto a la competencia de la Comisión Federal de Comercio o del Departamento de Transporte (y, por tanto, puede adherirse al Marco de Privacidad de Datos).

Si se cumplen todas las condiciones, el Departamento de Comercio informa a la entidad de que puede publicar sus directrices en materia de privacidad haciendo referencia al Marco de Privacidad de Datos en su sitio web. Una vez que se publican las directrices en materia de

[9] En el período equivalente, 2 400 empresas se habían certificado con arreglo al Escudo de la privacidad.
[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).
[11] https://www.dataprivacyframework.gov/key-requirements.
[12] Órganos de resolución de controversias del sector privado que investigan y resuelven rápidamente las reclamaciones y controversias sin coste alguno para el interesado.

privacidad, el Departamento de Comercio confirma la certificación e incluye la empresa en la lista del Marco de Privacidad de Datos en su sitio web. Puede invocarse el Marco de Privacidad de Datos para recibir datos personales de la UE a partir de la fecha en que el Departamento de Comercio inscriba a la entidad en dicha lista[13].

Como se explicó en la reunión de revisión, los controles realizados hasta la fecha por el Departamento de Comercio han dado lugar a la denegación de 33 solicitudes por no cumplir los requisitos del Marco de Privacidad de Datos. En general, el Departamento de Comercio colabora con la empresa para subsanar cualquier deficiencia. Si el Departamento de Comercio detecta deficiencias, informa a la empresa de que debe subsanarlas y de que la falta de respuesta dentro de un plazo determinado o cualquier otro incumplimiento de la obligación de completar su autocertificación de conformidad con los procedimientos del Departamento tendrá como consecuencia que se entienda desistida su solicitud. Si la certificación inicial no se completa o modifica en un plazo de doce meses, el Departamento de Comercio la considera desistida.

El plazo para la revalidación anual de la certificación se especifica en la lista del Marco de Privacidad de Datos para cada empresa. Para recordar a las empresas la necesidad de solicitar una revalidación de la certificación, el Departamento de Comercio ha creado un sistema con recordatorios de que la certificación está a punto de vencer. Las entidades reciben un recordatorio un mes antes, dos semanas antes y un día antes de la fecha de vencimiento. Aquellas que dejen vencer su certificación se eliminan de la lista del Marco de Privacidad de Datos. Como se describe en el anexo III de la decisión de adecuación, el Departamento de Comercio dispone de una sección específica en su sitio web en la que se indican las entidades estadounidenses que ya no son participantes activos, así como las respectivas razones (por ejemplo, vencimiento o baja voluntaria) por las que se han eliminado de la lista (la «lista de inactivos») las empresas en cuestión. Cuando se eliminan entidades de la lista del Marco de Privacidad de Datos por haber dejado vencer su certificación, el Departamento de Comercio se pone en contacto con ellas para confirmar si desean darse de baja o si tienen la intención de revalidar su certificación, y, en este último caso, verificar que, durante el tiempo en que estuvo vencida su certificación, han aplicado los principios del Marco a los datos personales recibidos en el Marco de Privacidad de Datos y aclarar qué medidas adoptarán para resolver las cuestiones pendientes que hayan retrasado la revalidación de su certificación. Si las empresas notifican al Departamento de Comercio que desean darse de baja en el Marco, el Departamento les exige que confirmen si devolverán o suprimirán los datos recibidos en el Marco de Privacidad de Datos; los conservarán y seguirán aplicando los principios del Marco a dichos datos (lo cual debe confirmarse anualmente); o los conservarán y establecerán otras medidas de protección (como las cláusulas contractuales tipo adoptadas por la Comisión Europea).

Las observaciones recibidas de los organismos profesionales y las empresas indican que las empresas certificadas con arreglo al Marco de Privacidad de Datos han adoptado una serie de medidas para garantizar el cumplimiento de los principios del Marco. Por ejemplo, para cumplir el *principio de impugnación, ejecución forzosa y responsabilidad*, las entidades han llevado a cabo controles internos mediante una autoevaluación o una verificación externa del cumplimiento. Los dos órganos independientes de impugnación del sector privado que participaron en la reunión de revisión explicaron que también ofrecen una verificación externa del cumplimiento mediante la revisión de las directrices en materia de privacidad y uno de ellos explicó que también ofrece auditorías y comprobaciones aleatorias, centradas, por ejemplo, en

[13] Sección I, punto 3, del anexo I de la decisión de adecuación.

los principios de *acceso*, *opción* y *responsabilidad proactiva por las transferencias ulteriores*. Además, las empresas certificadas han desarrollado programas de cumplimiento interno y mecanismos de supervisión, han formado a sus empleados, han implantado mecanismos para que los particulares puedan ejercer sus derechos, han llevado a cabo evaluaciones de impacto sobre la privacidad y han revisado los contratos existentes.

2.1.2. Control del cumplimiento, declaraciones falsas de participación y ejecución forzosa

Con arreglo al Marco de Privacidad de Datos, el Departamento de Comercio es responsable de controlar el cumplimiento de los principios del Marco mediante el uso de diferentes herramientas, como verificaciones de oficio (por iniciativa propia), inspecciones sin aviso *ad hoc* y cuestionarios sobre cumplimiento. Esto incluye la detección y corrección de declaraciones falsas de participación en el Marco, por ejemplo, a través de búsquedas en internet[14].

Para controlar el cumplimiento de los principios por las empresas participantes, el Departamento de Comercio se ha basado principalmente en búsquedas *ad hoc* en la web y en comprobaciones en medios de comunicación (o en medios sociales) durante el último año. El Departamento de Comercio informó de que no había detectado problemas de cumplimiento de los principios del Marco de Privacidad de Datos en este primer año y no había remitido ninguna empresa a la Comisión Federal de Comercio ni al Departamento de Transporte para que emprendieran medidas de ejecución forzosa. Asimismo, ha creado un punto de contacto específico para facilitar la cooperación con las APD y recibir reclamaciones de particulares y remisiones de otras autoridades (por ejemplo, las APD o la Comisión Federal de Comercio). No obstante, en el último año no se han recibido remisiones ni reclamaciones. Mientras que este primer año de funcionamiento del Marco de Privacidad de Datos se centró en la creación del Marco y el proceso de certificación, en la reunión de revisión, el Departamento de Comercio explicó que tiene previsto llevar a cabo comprobaciones del cumplimiento con medios automatizados para llevarlos a cabo de manera más sistemática y actualmente está desarrollando las herramientas informáticas necesarias para ello.

La Comisión reconoce que, durante este primer año, el Departamento de Comercio debía centrar sus esfuerzos en la creación del Marco y el proceso de certificación. En el futuro, es importante que el Departamento de Comercio intensifique sus esfuerzos para controlar y comprobar el cumplimiento de los principios en materia de privacidad, lo cual es necesario para garantizar el mantenimiento de un nivel elevado de cumplimiento del Marco y detectar casos que requieran nuevas medidas de ejecución forzosa, incluidas las posibles declaraciones falsas de participación de las empresas. A este respecto, la Comisión acoge con satisfacción el hecho de que el Departamento de Comercio haya confirmado su intención de desarrollar y utilizar herramientas (automatizadas) para detectar de manera más eficaz y sistemática los problemas de cumplimiento y las declaraciones falsas, y considera que esto debería formar parte de un esfuerzo más amplio para hacer un mayor uso de las diferentes herramientas a su disposición (por ejemplo, inspecciones sin aviso, cuestionarios de control del cumplimiento,

[14] Véase el anexo III de la decisión de adecuación. Pueden surgir declaraciones falsas, por ejemplo, cuando una empresa declara que participa en el Marco de Privacidad de Datos y nunca ha iniciado el proceso de certificación o lo ha iniciado, pero no lo ha finalizado o ha dejado vencer su certificación.

solicitudes de información, etc.), en particular para verificar el cumplimiento de los requisitos específicos del Marco de Privacidad de Datos[15].

Las entidades participantes están sujetas a la competencia de la Comisión Federal de Comercio y del Departamento de Transporte. Durante la reunión de revisión, el Departamento de Transporte confirmó que ha establecido todos los procesos necesarios para adoptar las medidas de ejecución forzosa adecuadas. Asimismo, explicó que muy pocas empresas sujetas a su competencia se han adherido al Marco de Privacidad de Datos (a saber, algunos agentes de venta de billetes, pero ninguna compañía aérea). La Comisión Federal de Comercio confirmó que, en cada una de sus investigaciones en materia de privacidad, controla sistemáticamente si se han producido vulneraciones de los principios del Marco de Privacidad de Datos. Hasta la fecha, la Comisión Federal de Comercio no ha recibido ninguna remisión de otras autoridades. Ha recibido algunas reclamaciones en las que se menciona el Marco de Privacidad de Datos, aunque dos de ellas se referían a empresas incluidas en la «lista de inactivos», dos se referían a empresas que no participaban en el Marco y una no se refería a datos personales transferidos desde la UE. En el momento de la elaboración del presente informe, la Comisión Federal de Comercio no había adoptado decisiones para hacer cumplir el Marco de Privacidad de Datos, aunque confirmó que varias empresas certificadas con arreglo al Marco están siendo investigadas actualmente.

La Comisión acoge con satisfacción el hecho de que la Comisión Federal de Comercio controle sistemáticamente si se han producido vulneraciones de los principios del Marco de Privacidad de Datos en todas sus investigaciones en materia de privacidad. Dado que la eficacia permanente del Marco de Privacidad de Datos depende de su cumplimiento riguroso, se espera que la Comisión Federal de Comercio siga ejerciendo sus competencias de investigación en virtud del Marco, en particular llevando a cabo de forma proactiva acciones de barrido centradas en el cumplimiento de los requisitos específicos del Marco de Privacidad de Datos o en determinados sectores.

2.1.3. Tramitación de reclamaciones

El Marco de Privacidad de Datos ofrece a los particulares de la UE diversas vías de recurso en caso de incumplimiento de los principios del Marco de Privacidad de Datos por parte de las entidades certificadas[16]. Esto incluye buscar una resolución poniéndose en contacto directamente con la entidad participante en cuestión, que debe dar una respuesta al particular afectado en un plazo de cuarenta y cinco días. Los particulares también pueden presentar una reclamación ante un órgano independiente de impugnación designado por una entidad para investigar y resolver reclamaciones. En función de las circunstancias, podría tratarse de un organismo de resolución alternativa de controversias o de una APD[17]. Por último, en caso de que ninguna de las demás vías de recurso disponibles haya resuelto de manera satisfactoria la reclamación del interesado, los particulares pueden solicitar la incoación de un proceso arbitral

[15] Por ejemplo, en relación con las transferencias ulteriores, haciendo uso de la posibilidad contemplada en el principio 3, letra b), del Marco de Privacidad de Datos de solicitar un resumen o una copia representativa de las cláusulas en materia de privacidad pertinentes de los contratos para las transferencias ulteriores.

[16] Véase la sección 2.4 de la decisión de adecuación.

[17] Las entidades participantes 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.

vinculante al Panel del Marco de Privacidad de Datos UE-EE. UU. como instancia de último recurso.

2.1.3.1. Tramitación de reclamaciones por parte de las empresas

Las respuestas de los organismos profesionales y las empresas a los cuestionarios enviados por la Comisión indican que las empresas certificadas con arreglo al Marco de Privacidad de Datos han recibido muy pocas, aquellas que las han recibido, reclamaciones de particulares relativas al incumplimiento de los principios del Marco. Al mismo tiempo, las empresas han establecido diferentes mecanismos y herramientas para que los particulares puedan ejercer sus derechos y presentar reclamaciones, en particular a través de formularios en línea, por correo electrónico y por teléfono.

2.1.3.2. *Órganos independientes de impugnación*

Las observaciones recibidas durante la reunión de revisión y la información proporcionada por los organismos profesionales indican que ha habido muy pocas reclamaciones ante los órganos independientes de impugnación. Entre los órganos independientes de impugnación seleccionados por las empresas figuran BBB National Programs, JAMS, TRUSTe y VeraSafe. El Marco de Privacidad de Datos exige que los órganos independientes de impugnación publiquen un informe anual con estadísticas agregadas sobre el uso de sus servicios de resolución de controversias. En el momento de la adopción del presente informe, todos los órganos independientes de impugnación afectados habían publicado sus informes anuales[18].

Además, en la reunión de revisión, BBB y VeraSafe realizaron presentaciones detalladas sobre sus actividades del último año. Informaron de un aumento del número de empresas participantes que eligieron sus servicios en comparación con marcos anteriores y mencionaron que habían recibido algunas reclamaciones, aunque la gran mayoría no reunían los requisitos para ser admitidas a trámite. Por ejemplo, BBB recibió 87 reclamaciones de particulares de la UE y solo dos de ellas pudieron ser admitidas a trámite. Aunque BBB explicó que las reclamaciones se tramitan en una media de cinco días hábiles, esas dos reclamaciones acabaron archivándose debido a la falta de respuesta de los particulares. VeraSafe recibió veintiséis reclamaciones, de las cuales seis pudieron ser admitidas a trámite. Dos de ellas estaban relacionadas con solicitudes de acceso y supresión y se resolvieron, mientras que dos siguen pendientes de resolución, y dos se retiraron o fueron archivadas debido a la falta de respuesta

[18] ANA: https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs: https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR-AAA: https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights Association: https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS: https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services: https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution: https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
Verasafe: https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

del particular. Ambos órganos independientes de impugnación explicaron que tratan de responder a las reclamaciones en la lengua del particular.

Las empresas participantes que tratan datos de recursos humanos transferidos desde la UE deben seleccionar a las APD de la UE como sus órganos independientes de impugnación en relación con esos datos, mientras que las empresas participantes pueden seleccionar voluntariamente a las APD de la UE como sus órganos independientes de impugnación en relación con otros tipos de datos personales transferidos en el Marco de Privacidad de Datos. De hecho, más de la mitad de las empresas certificadas con arreglo al Marco de Privacidad de Datos en el momento de la revisión optaron por esta solución[19], lo que se acoge con satisfacción. Desde que se adoptó la decisión de adecuación, el CEPD ha adoptado el Reglamento interno del «panel informal de APD de ámbito europeo». El panel es competente para aprobar dictámenes vinculantes para las entidades estadounidenses en relación con reclamaciones no resueltas de particulares referidas al tratamiento de datos personales transferidos desde la UE en el Marco de Privacidad de Datos. De conformidad con su Reglamento interno, el panel está formado por una APD que actúa como APD principal y otras APD coverificadoras designadas[20]. Publica dictámenes vinculantes en un plazo de sesenta días a partir de la recepción de la correspondiente reclamación relacionada con el Marco de Privacidad de Datos. El CEPD también ha publicado un modelo de formulario de reclamación para presentar reclamaciones ante las APD[21], así como «Preguntas frecuentes para particulares europeos»[22] y empresas[23] sobre el Marco de Privacidad de Datos. El panel no había recibido ninguna reclamación en el momento de la revisión.

2.1.3.3. El mecanismo de arbitraje vinculante

El Centro Internacional de Resolución de Controversias (International Centre for Dispute Resolution, ICDR), que es la división internacional de la Asociación Estadounidense de Arbitraje (American Arbitration Association, AAA), fue seleccionado por el Departamento de Comercio para gestionar el mecanismo de arbitraje vinculante. Tras la adopción de la decisión de adecuación, el Departamento de Comercio, junto con la Comisión, seleccionó a once árbitros con experiencia en materia de privacidad y procedentes de diversos ámbitos, como el arbitraje, el poder judicial, el mundo universitario y la sociedad civil[24]. Además, se ha adoptado el Reglamento de arbitraje[25] para el Panel del Marco de Privacidad de Datos, así como un código de conducta para los árbitros[26], que están disponibles en el sitio web del Centro

[19] Poco después de la fecha de la reunión de revisión, en el sitio web sobre el Marco de Privacidad de Datos se indicó que 1 511 de los 2 892 participantes contaban con una Autoridad de Protección de Datos de la UE como su órgano de impugnación.
[20] El 17 de abril de 2024, el CEPD adoptó el reglamento interno del «panel informal de APD de la UE» de conformidad con el Marco de Privacidad de Datos UE-EE. UU. Puede consultarse en el enlace siguiente: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.
[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_es.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_es.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_es.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/ICDR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.

Internacional de Resolución de Controversias. En el momento de la revisión, ningún particular de la UE había activado aún el mecanismo de arbitraje.

2.1.4. Orientación, cooperación y concienciación

Desde la entrada en vigor del Marco de Privacidad de Datos, el Departamento de Comercio ha llevado a cabo diversas actividades de concienciación organizando presentaciones itinerantes, seminarios web y conferencias; poniéndose en contacto con los organismos profesionales e interactuando directamente con más de 3 000 empresas para ofrecer información sobre el Marco de Privacidad de Datos. También ha publicado orientaciones, en particular en forma de respuestas a preguntas frecuentes dirigidas a particulares, así como a empresas de la UE y de los Estados Unidos[27]. A su vez, el CEPD ha elaborado formularios de reclamación y un documento de respuestas a preguntas frecuentes dirigidas a particulares y empresas. Del mismo modo, cuando adoptó su decisión de adecuación, la Comisión publicó un documento de respuestas a preguntas frecuentes y una ficha informativa sobre el Marco de Protección de Datos[28].

Al mismo tiempo, de la reunión de revisión se desprende que es necesario seguir trabajando para concienciar a los particulares y proporcionar orientación a las empresas. Las aportaciones recibidas de las empresas y de los órganos independientes de impugnación, así como el número muy reducido de reclamaciones, sugieren que es posible que los particulares no siempre sean conscientes de sus derechos o del mecanismo para ejercerlos. Durante la reunión de revisión, el Departamento de Comercio manifestó su interés en colaborar con las APD de la UE para aumentar la concienciación sobre el Marco entre los particulares de la UE. La Comisión fomenta estas iniciativas y también está tomando medidas para informar mejor a las personas, en particular facilitando información adicional sobre el Marco de Privacidad de Datos en su sitio web, por ejemplo, incorporando enlaces y referencias a los documentos de orientación pertinentes adoptados por el CEPD, el Departamento de Comercio y otras autoridades estadounidenses.

En lo que respecta a las orientaciones sobre los principios del Marco de Privacidad de Datos, los representantes del CEPD acordaron, durante la reunión de revisión, cooperar en los próximos meses para proporcionar aclaraciones adicionales sobre el concepto de «datos de recursos humanos» en el Marco de Privacidad de Datos y las obligaciones específicas que se aplican al tratamiento de dichos datos. Se estudiaron diferentes elementos que deberían incluirse en dichas orientaciones. Por ejemplo, estas orientaciones podrían abordar determinados supuestos prácticos en los que los datos de los asalariados serían tratados en el Marco de Privacidad de Datos (por ejemplo, por una empresa que ofrezca servicios de nube) y explicar qué obligaciones del Marco serían pertinentes para tales supuestos. Asimismo, podría sugerir a las empresas que reciban datos de particulares asalariados de la UE (pero no los utilicen necesariamente en el contexto de una relación laboral) que elijan el panel de las APD como su órgano independiente de impugnación. Esto garantizaría que dichos particulares pudieran dirigirse a una autoridad «cercana a su domicilio» y, en su caso, que esté más familiarizada con la normativa nacional aplicable a los datos de recursos humanos.

Además, un aspecto específico para el que parece que sería útil disponer de más orientaciones (también sobre la base de las aportaciones recibidas de los organismos profesionales) se refiere

[27] Véase, por ejemplo, https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_es.

a los requisitos del Marco de Privacidad de Datos para las transferencias ulteriores. Por otra parte, el Departamento de Comercio indicó que sería conveniente estudiar si algunos sectores podrían beneficiarse de orientaciones adicionales sobre la aplicación de los principios del Marco a sus actividades, por ejemplo, en el ámbito de la investigación sanitaria y los servicios financieros.

La Comisión acoge con satisfacción la disposición de ambas partes a elaborar orientaciones y espera que los trabajos sobre los temas mencionados comiencen en breve.

De manera más general, se han creado varios mecanismos para garantizar los intercambios y la cooperación entre las autoridades estadounidenses y las APD, en particular mediante la designación de puntos de contacto específicos en la Comisión Federal de Comercio y el Departamento de Comercio para tramitar las consultas de las APD y las reclamaciones remitidas por estas.

2.1.5. Cambios pertinentes en el sistema jurídico estadounidense

Desde la adopción de la decisión de adecuación, han tenido lugar varios cambios en el marco jurídico estadounidense en el ámbito de la privacidad. Estos cambios son de tipo legislativo, regulatorio y jurisprudencial. En general, estos cambios indican una mayor convergencia de los enfoques de la UE y de los Estados Unidos ante determinadas dificultades en materia de protección de la privacidad, en particular mediante el uso de conceptos jurídicos similares. Algunos de estos cambios están en curso y deberán ser objeto de un seguimiento ulterior.

A nivel federal, el presidente dictó varios Decretos Presidenciales pertinentes para el uso de datos personales. En particular, el Decreto Presidencial n.º 14117, de 28 de febrero de 2024[29], prohíbe o limita las transacciones relativas a determinadas categorías de datos personales sensibles (por ejemplo, datos sanitarios, identificadores biométricos y datos genómicos humanos) con entidades de algunos «países que suscitan preocupación»[30]. El decreto adoptado encarga al secretario de Justicia (*Attorney General*) que proponga normativa, aún por emitir en el momento de la adopción del presente informe, para especificar en mayor medida su aplicación. Además, el Decreto Presidencial n.º 14110, de 30 de octubre de 2023, relativo a la inteligencia artificial[31], se centra en el desarrollo de una inteligencia artificial segura y fiable. Exige que varias agencias federales elaboren normas y directrices de seguridad relacionadas con la IA, en particular sobre los riesgos específicos de la IA para la privacidad y sobre técnicas de protección de la privacidad.

En cuanto a la labor legislativa, si bien en los últimos años se han presentado en el Congreso proyectos de ley federal de protección de la privacidad, veinte Estados del país ya han promulgado leyes exhaustivas en materia de privacidad a julio de 2024, ocho de las cuales ya han comenzado a aplicarse: California, Colorado, Oregón, Virginia, Connecticut, Utah, Texas y Florida. Además, diecisiete Estados del país han adoptado legislación que aborda el tratamiento automatizado (o, al menos, algunas de sus formas) y, en general, permite pedir

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Entre ellos figuran, según lo propuesto por el secretario de Justicia en un aviso anticipado de reglamentación propuesta emitido el 3 de mayo de 2024, China, Cuba, Hong Kong y Macao, Irán, Corea del Norte y Venezuela. Véase https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

quedar excluido de determinados tipos de toma de decisiones basados en la «elaboración de perfiles»[32].

En cuanto a la evolución de la jurisprudencia, varios representantes de la sociedad civil han señalado la reciente sentencia del Tribunal Supremo en el asunto Loper Bright Enterprises/Raimondo (de 28 de junio de 2024). Esta sentencia invalida la jurisprudencia anterior sobre la doctrina *Chevron*, según la cual los órganos jurisdiccionales aplican el principio de deferencia a la interpretación razonable de la legislación por parte de una agencia reguladora en caso de ambigüedad de una ley aplicada por dicha agencia. En particular, algunas ONG han expresado su preocupación por el impacto de esta sentencia del Tribunal Supremo sobre la competencia normativa de la Comisión Federal de Comercio en el ámbito de la privacidad, reconociendo al mismo tiempo que es posible que el impacto sobre sus competencias de ejecución sea nulo o limitado. En la reunión de revisión, la Comisión Federal de Comercio informó de que todavía es pronto para conocer las implicaciones exactas de esta sentencia. Al mismo tiempo, explicó que la elaboración de normas de la Comisión Federal de Comercio se lleva a cabo en virtud de una competencia otorgada por la Ley de la Comisión Federal de Comercio diferente de las de otras agencias administrativas y para la que la doctrina *Chevron* era menos pertinente. Por tanto, la reciente sentencia puede tener un impacto limitado en este ámbito.

Además, la Comisión Federal de Comercio informó sobre la evolución reciente de su enfoque en materia de tratamiento automatizado de datos e inteligencia artificial. Esto incluye la adopción de una declaración conjunta con otros organismos de garantía del cumplimiento contra la discriminación y los sesgos en los sistemas automatizados[33], así como varias medidas de ejecución, en las que la Comisión Federal de Comercio se centra, entre otras cosas, en la transparencia, la equidad del tratamiento automatizado de datos y la posibilidad de los particulares de impugnar los resultados. El caso más destacado a este respecto es la decisión de la Comisión Federal de Comercio contra *Rite Aid* en marzo de 2024, que impuso una prohibición de cinco años del uso de la tecnología de reconocimiento facial con fines de seguridad por parte de dicha empresa[34]. En particular, la Comisión Federal de Comercio

[32] Aunque existen diferencias en lo que se entiende por «elaboración de perfiles» en los distintos Estados, la elaboración de perfiles se define generalmente como toda forma de tratamiento automatizado de datos personales para evaluar, analizar o predecir aspectos personales relativos a la situación económica, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la ubicación o los movimientos de una persona física identificada o identificable. Los consumidores suelen ser quienes pueden pedir quedar excluidos de la elaboración de perfiles. Los siguientes Estados han adoptado legislación en materia de elaboración de perfiles: Colorado (Estatutos Revisados Anotados de Colorado, artículo 6-1-1306), Connecticut (Estatutos Generales Anotados de Connecticut, artículo 42-518), Delaware (Código Anotado de Delaware, título 6, artículo 12D-104), Florida (Estatutos Anotados de Florida, artículo 501.705), Indiana (Código Anotado de Indiana, artículo 24-15-3-1), Kentucky (Estatutos Revisados Anotados de Kentucky, artículo 367.3615), Maryland (Ley de privacidad de datos en línea de Maryland de 2024, promulgada el 9 de mayo de 2024), Minnesota (Estatutos Anotados de Minnesota, artículo 325O.07), Montana (Código Anotado de Montana, artículo 30-14-2808), Nebraska (Estatutos Revisados Anotados de Nebraska, artículo 87-1107), Nuevo Hampshire (Estatutos Revisados Anotados de New Hampshire, artículo 507-H:4), Nueva Jersey (Estatutos Anotados de New Jersey, artículo 56:8-166.8), Oregón (Estatutos Revisados Anotados de Oregón, artículo 646A.574), Rhode Island (Ley de transparencia de datos y protección de la privacidad de Rhode Island, promulgada el 29 de junio de 2024), Tennessee (Código Anotado de Tennessee, artículo 47-18-3304), Texas (Código de Negocios y Comercio Anotado de Texas, artículo 541.051) y Virginia (Código Anotado de Virginia, artículo 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

constató que *Rite Aid* no había adoptado medidas razonables para evitar resultados erróneos e informar a los consumidores de la tecnología utilizada. De manera más general, en la reunión de revisión, la Comisión Federal de Comercio abordó sus prioridades actuales y, en particular, los ámbitos que considera merecedores de un enfoque más proactivo de garantía del cumplimiento en el futuro. Esto incluye la protección de datos sensibles (por ejemplo, datos sanitarios, biométricos y de geolocalización)[35], la protección de niños[36] y menores en línea y la seguridad de los datos[37].

La Comisión continuará siguiendo de cerca estos y otros avances en los Estados Unidos, en particular cualquier nueva medida encaminada a una ley federal integral en materia de privacidad y el posible impacto de la reciente jurisprudencia del Tribunal Supremo en el papel de la Comisión Federal de Comercio en el ámbito de la privacidad.

La Comisión acoge con satisfacción la información facilitada por la Comisión Federal de Comercio sobre sus recientes medidas de ejecución y las prioridades actuales, que se corresponden en gran medida con las tendencias y prioridades en materia de aplicación de la protección de datos en Europa. La Comisión Federal de Comercio también participa activamente en la red que reúne a los países que se benefician de una decisión de adecuación de la UE, que la Comisión puso en marcha en marzo de 2024[38]. Esta mayor convergencia debe fomentar y facilitar una cooperación más estrecha entre las autoridades responsables de proteger la privacidad a ambos lados del Atlántico, en particular en cuestiones pertinentes para el funcionamiento del Marco de Privacidad de Datos.

2.2. Aspectos relacionados con el acceso y el uso de los datos personales transferidos en el Marco de Privacidad de Datos UE-EE. UU. por parte de los poderes públicos estadounidenses

La decisión de adecuación contiene una evaluación detallada de las normas que rigen la recogida y el uso de los datos personales transferidos desde la UE a empresas certificadas con arreglo al Marco de Privacidad de Datos por parte de los poderes públicos estadounidenses, en particular con fines penales y de seguridad nacional. Desde la adopción de la decisión de adecuación, confirmada por las autoridades estadounidenses durante la reunión de revisión, no se han producido cambios pertinentes con respecto al marco jurídico aplicable al acceso a los

[35] Véase, por ejemplo, la reciente Orden de la Comisión Federal de Comercio contra X-Mode por la venta y el intercambio de información sensible de localización (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) y contra Monument en relación con la divulgación de datos sanitarios sensibles a terceros con fines de comercialización (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Por ejemplo, la Comisión Federal de Comercio ha anunciado recientemente una investigación que ha dado lugar a una demanda contra TikTok y su empresa matriz, Bytedance, por haber cometido una supuesta infracción de la legislación en materia de privacidad de los menores. Se alega que ambas empresas incumplieron el requisito de notificar y obtener el consentimiento parental antes de recoger y utilizar información personal de menores de trece años (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Véase el resumen de las recientes medidas de ejecución en el informe *The Federal Trade Commission 2023 Privacy and Data Security Update* [«Actualización sobre la privacidad y la seguridad de los datos de 2023 de la Comisión Federal de Comercio», documento en inglés]: https://ec.europa.eu/commission/presscorner/detail/es/mex_24_1307.

[38] Véase https://ec.europa.eu/commission/presscorner/detail/es/mex_24_1307. A raíz de la reunión de marzo de 2024, se decidió celebrar una serie de sesiones temáticas. La primera tuvo lugar en julio de 2024 y se centró en el desarrollo de herramientas que puedan ayudar a las pequeñas y medianas empresas a cumplir la legislación en materia de privacidad.

datos con fines policiales o regulatorios en el primer año del Marco de Privacidad de Datos. Por este motivo, las conclusiones que figuran a continuación solo se refieren a la evolución en el ámbito de la seguridad nacional.

Las conclusiones alcanzadas en la decisión de adecuación sobre el acceso a los datos por parte de los servicios de inteligencia se basan en el análisis de las condiciones y limitaciones que se aplican a las operaciones de inteligencia de señales en virtud de diversos fundamentos jurídicos pertinentes, en particular el artículo 702 de la Ley de vigilancia de inteligencia exterior (Foreign Intelligence Surveillance Act, FISA) y el Decreto Presidencial n.º 12333[39], complementado y reforzado por el Decreto Presidencial n.º 14086, relativo al refuerzo de las garantías en las actividades de inteligencia de señales de los Estados Unidos, adoptado por el presidente de los Estados Unidos el 7 de octubre de 2022. Las garantías establecidas en el Decreto Presidencial n.º 14086 se aplican a todas las actividades de inteligencia de señales estadounidenses, con independencia del fundamento jurídico en que se basen dichas actividades y del lugar en el que se lleven a cabo, y protegen los datos de particulares no estadounidenses (incluidos los europeos)[40]. El Decreto Presidencial n.º 14086 también estableció una nueva vía de recurso con la que los particulares de la UE pueden exigir el cumplimiento de estas garantías vinculantes.

En las secciones siguientes se describen las medidas adoptadas por las autoridades estadounidenses desde la adopción de la decisión de adecuación para cumplir el Decreto Presidencial n.º 14086, así como la evolución pertinente en relación con el marco jurídico antes mencionado.

2.2.1. Evolución pertinente con respecto al marco jurídico estadounidense

2.2.1.1. Aplicación del Decreto Presidencial n.º 14086 por parte de los servicios de inteligencia

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. Son vinculantes para todos los servicios de inteligencia y se han puesto en práctica mediante políticas y procedimientos adoptados por cada servicio.

Como parte de la primera revisión, las autoridades estadounidenses confirmaron que no se han producido cambios en el Decreto Presidencial n.º 14086 desde su adopción. Además, se aclaró que el presidente de los Estados Unidos no ha hecho uso de la facultad prevista en el artículo 2, letra b), inciso i), subletra B), y en el artículo 2, letra b), inciso ii), subletra C), del Decreto Presidencial n.º 14086 para actualizar la lista de fines legítimos que pueden perseguirse con la recogida de inteligencia de señales ni la lista de fines para los que pueden utilizarse los datos recogidos de forma masiva[41]. Para determinar prioridades de inteligencia más específicas para

[39] Otras medidas que pueden adoptarse en virtud de la Ley de vigilancia de inteligencia exterior con respecto a los datos transferidos desde la UE son la vigilancia electrónica individualizada (artículo 105 de la Ley de vigilancia de inteligencia exterior), los registros físicos (artículo 302 de la Ley de vigilancia de inteligencia exterior), el uso de dispositivos de registro de comunicaciones salientes y entrantes (artículo 402 de la Ley de vigilancia de inteligencia exterior) y la recogida de documentos comerciales de determinadas empresas (transportistas comunes, establecimientos de alojamiento, establecimientos de alquiler de vehículos o instalaciones de almacenamiento físico, artículo 501 de la Ley de vigilancia de inteligencia exterior). Estas distintas bases jurídicas se analizan detalladamente en la decisión de adecuación (considerandos 142 a 152).

[40] Para obtener más información, véase la sección 3.2.1.2 de la decisión de adecuación.

[41] Entre estos objetivos o fines legítimos figuran la protección contra los asesinatos, sabotajes y espionajes u otras actividades de inteligencia llevadas a cabo por personas, organizaciones o administraciones públicas extranjeras,

las que pueda recogerse realmente inteligencia de señales, el Decreto Presidencial n.º 14086 estableció un procedimiento específico. En particular, debe consultarse al responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional para evaluar, por cada prioridad, 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[42]. La responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional confirmó durante la reunión de revisión que revisó las prioridades propuestas por el director de Inteligencia Nacional en el Marco de Prioridades Nacionales de Inteligencia de 2023, llegó a la conclusión de que cumplían los requisitos anteriores y compartió su conclusión con el director de Inteligencia Nacional, que, a su vez, presentó las prioridades al presidente para su validación. La responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional también impartió formación sobre los requisitos del Decreto Presidencial n.º 14086 a partes de la Comunidad de Inteligencia que participan en el establecimiento de prioridades de inteligencia.

Además, las autoridades estadounidenses han adoptado en el último año nuevas medidas prácticas para aplicar el Decreto Presidencial n.º 14086 en sus operaciones cotidianas. En particular, los servicios de inteligencia han adoptado nuevas políticas y directrices internas sobre la aplicación del Decreto Presidencial, por ejemplo, procesos internos (a través de requisitos internos de autorización, controles de acceso documentados, de modo que solo las personas que hayan recibido la formación adecuada y cumplan los requisitos de misión necesarios tengan acceso a la información, etc.) para garantizar el cumplimiento de sus requisitos de necesidad y proporcionalidad en el contexto de la recogida selectiva y masiva[43]. Además, se ha impartido formación sobre el Decreto Presidencial n.º 14086 al personal de diferentes servicios de inteligencia [por ejemplo, la Agencia Nacional de Seguridad (NSA), la Agencia Central de Inteligencia (CIA) y el Buró Federal de Investigaciones (FBI)], incluidas sesiones de formación anuales y *ad hoc* organizadas por el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y formación obligatoria para todo el personal nuevo que se incorpore a la Oficina del Director de Inteligencia Nacional.

La Comisión acoge con satisfacción las diversas medidas adoptadas para aplicar y garantizar el cumplimiento del Decreto Presidencial n.º 14086. A medida que se adquiera más experiencia con la aplicación práctica de las garantías del Decreto Presidencial, la Comisión agradecería la oportunidad de debatir ejemplos concretos de cómo se aplica el Decreto Presidencial en la práctica (respetando al mismo tiempo las cuestiones de confidencialidad pertinentes) en futuras revisiones.

2.2.1.2. Reautorización del artículo 702 de la Ley de vigilancia de inteligencia exterior

El artículo 702 de la Ley de vigilancia de inteligencia exterior autoriza la adquisición de información de inteligencia exterior respecto de personas no estadounidenses que se considere que es razonable que se encuentren fuera de los Estados Unidos. La adquisición de dicha

en nombre de estas o con su apoyo; 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.

[42] Artículo 2, letra b), inciso iii), del Decreto Presidencial n.º 14086.

[43] Véase https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, publicado el 3 de julio de 2023.

información se realiza sobre la base de certificaciones anuales presentadas al Tribunal de Vigilancia de Inteligencia Exterior (Foreign Intelligence Surveillance Court) y aprobadas por este. Estas certificaciones especifican las categorías de información de inteligencia exterior que deben adquirirse. El 21 de julio de 2023, la Oficina del Director de Inteligencia Nacional anunció que existen tres certificaciones aprobadas en virtud del artículo 702 de la Ley de vigilancia de inteligencia exterior, que abarcan las siguientes categorías de inteligencia exterior: 1) administraciones públicas extranjeras y entidades vinculadas, 2) lucha contra el terrorismo y 3) lucha contra la proliferación[44]. Las certificaciones también deben incluir procedimientos de selección de objetivos y minimización aprobados por el Tribunal de Vigilancia de Inteligencia Exterior[45]. En particular, la selección de objetivos se lleva a cabo solicitando a las empresas estadounidenses que cumplan la definición de «empresa de servicios de comunicación electrónica» de la Ley de vigilancia de inteligencia exterior que divulguen datos de comunicaciones electrónicas enviadas a o desde «selectores», que indican una cuenta de comunicación específica, por ejemplo, un número de teléfono o una dirección de correo electrónico. El Gobierno de los Estados Unidos ha publicado una serie de materiales sobre el artículo 702 de la Ley de vigilancia de inteligencia exterior para informar al público sobre el funcionamiento de los programas de vigilancia, los requisitos aplicables y la protección de la privacidad, así como sobre el papel del Tribunal de Vigilancia de Inteligencia Exterior[46].

Debido a una cláusula de extinción, el artículo 702 de la Ley de vigilancia de inteligencia exterior debía expirar a finales de 2023, a menos que el Congreso lo reautorizara. Tras una reautorización temporal sin cambios, el Congreso aprobó la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos (Reforming Intelligence and Securing America Act) el 19 de abril de 2024, por la que se reautorizaba el artículo 702 de la Ley de vigilancia de inteligencia exterior por un período de dos años y se introducían varios cambios. A grandes rasgos, pueden dividirse en dos categorías: 1) cambios en el alcance de las actividades de vigilancia permitidas en virtud del artículo 702 de la Ley de vigilancia de inteligencia exterior y 2) cambios institucionales y de procedimiento.

Cambios en el alcance de las actividades de vigilancia permitidas en virtud del artículo 702 de la Ley de vigilancia de inteligencia exterior

Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos ha introducido tres cambios principales en el alcance de las actividades de vigilancia que pueden llevarse a cabo en virtud del artículo 702 de la Ley de vigilancia de inteligencia exterior.

En primer lugar, la recogida de comunicaciones «sobre» un selector ha quedado prohibida definitivamente[47]. Esto se refiere a la recogida de comunicaciones que no son «a» o «desde» un selector del artículo 702 (por ejemplo, una dirección de correo electrónico), sino que contienen una referencia a dicho selector (por ejemplo, comunicaciones por correo electrónico que no se envían a o desde la dirección de correo electrónico seleccionada, pero que la incluyen en el texto o cuerpo del correo electrónico). Si bien dicha recogida ya se había excluido a raíz

[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.

[45] Dichos procedimientos limitan la recogida de datos con respecto a un fin específico de inteligencia exterior, restringen el acceso a las bases de datos en las que se almacena la información obtenida con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior (incluso mediante controles de acceso) e imponen límites al uso, la conservación y la difusión de dicha información.

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

[47] Artículo 22 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos.

de una modificación de la Ley de vigilancia de inteligencia exterior en 2018, dicha ley seguía previendo la posibilidad de reanudar la recogida de comunicaciones «sobre» selectores en el futuro, tras un procedimiento de autorización específico que implicaba al Tribunal de Vigilancia de Inteligencia Exterior y al Congreso. La última modificación introducida por la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos ha eliminado esta posibilidad.

En segundo lugar, se ha ampliado la definición de «información de inteligencia exterior» para incluir información relativa a la lucha contra los estupefacientes[48]. Durante la reunión de revisión, las autoridades estadounidenses explicaron que esto se introdujo a la luz de la actual crisis de fentanilo y de la creciente amenaza para la seguridad nacional que suponen los traficantes y fabricantes internacionales de estupefacientes. En este contexto, se confirmó que este concepto responde a varios de los objetivos legítimos indicados en el Decreto Presidencial n.º 14086, a saber, comprender o valorar las capacidades, intenciones o actividades de organizaciones extranjeras que suponen una amenaza actual o potencial para la seguridad nacional de los Estados Unidos o de sus aliados; comprender o valorar las amenazas transnacionales que afectan a la seguridad mundial, incluidos los riesgos para la salud pública; y proteger contra las amenazas delictivas transnacionales[49].

En tercer lugar, la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos amplió la definición de «empresa de servicios de comunicación electrónica», ampliando así el número de empresas que pueden verse obligadas a proporcionar información de conformidad con el artículo 702 de la Ley de vigilancia de inteligencia exterior[50]. La definición incluye ahora otras empresas de servicios que tienen «acceso a equipos que se utilizan o pueden utilizarse para transmitir o almacenar comunicaciones por cable o electrónicas», excluyendo explícitamente los establecimientos de alojamiento, las viviendas, las instalaciones comunitarias y los establecimientos de restauración. En una carta dirigida al Congreso, el Departamento de Justicia se refirió a esta modificación como un cambio técnico destinado a cubrir un número «extremadamente reducido» de empresas tecnológicas que, según las recientes resoluciones del Tribunal de Vigilancia de Inteligencia Exterior y del Tribunal de Apelación de Inteligencia Exterior (Foreign Intelligence Surveillance Court of Review, FISCR), no estaban incluidas en la definición anterior de «empresa de servicios de comunicación electrónica»[51]. En ese mismo escrito, el Departamento de Justicia se comprometió a reducir el alcance aplicando esta definición exclusivamente al tipo de empresa de servicios controvertido en el litigio que dio lugar a la resolución del Tribunal de Vigilancia de Inteligencia Exterior. Por consiguiente, las empresas afectadas se mencionan en un anexo clasificado para el Congreso. Varias ONG, incluidas las que formularon observaciones como parte de la revisión, expresaron su preocupación por esta ampliación, alegando que podría abarcar a muchas empresas estadounidenses (ya que muchas de ellas prestan algún tipo de servicio y tienen acceso a equipos de comunicaciones). A la luz de estas preocupaciones, se ha propuesto una nueva modificación con el apoyo de la Comunidad de Inteligencia en un

[48] Artículo 23 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos.
[49] Artículo 2, letra b), inciso ii), subletra A), puntos 2, 3 y 10, del Decreto Presidencial n.º 14086.
[50] Artículo 25 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos.
[51] https://www.justice.gov/opa/media/1348621/dl?inline. Véase la resolución del Tribunal de Vigilancia de Inteligencia Exterior de 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) y la sentencia del Tribunal de Vigilancia de Inteligencia Exterior que confirma dicha resolución (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

proyecto de Ley de autorización de actividades de inteligencia para el ejercicio de 2025, que se encuentra actualmente en el Congreso. Este cambio, si lo aprueba el Congreso, garantizaría que las empresas adicionales incluidas en la definición de «empresa de servicios de comunicación electrónica» solo se limitarían a las mencionadas en las citadas resoluciones del Tribunal de Vigilancia de Inteligencia Exterior. El proyecto de ley también prevé que cada directiva dirigida a una de estas empresas tendría que notificarse al Tribunal de Vigilancia de Inteligencia Exterior, a fin de que este pueda comprobar si la empresa entra efectivamente en el ámbito de aplicación. En su carta al Congreso, el Departamento de Justicia se comprometió a informar al Congreso cada seis meses sobre toda aplicación de la definición actualizada, a fin de que el Congreso pueda ejercer una supervisión adecuada en lo que respecta a la aplicación estricta de la definición.

Es importante señalar que, en la reunión de revisión, las autoridades estadounidenses y la Junta de Supervisión de la Privacidad y las Libertades Civiles confirmaron que todas las garantías del Decreto Presidencial n.º 14086 siguen aplicándose plenamente a todas las recogidas y usos de datos con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior, incluso después de estas modificaciones. Así pues, si bien la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos amplía en cierta medida el número de empresas que pueden recibir un requerimiento, no limita el ejercicio de los derechos. No obstante, será importante hacer un seguimiento de la evolución (legislativa y en materia de notificación) y recibir información sobre la aplicación de estas nuevas normas en la práctica. Esto incluye, por ejemplo, el impacto de la ampliación de las definiciones de «inteligencia exterior» y «empresas de servicios de comunicación electrónica» en el número de objetivos seleccionados con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior (según lo comunicado anualmente por la Oficina del Director de Inteligencia Nacional, véase la sección sobre transparencia). El futuro informe de seguimiento del reciente informe de la Junta de Supervisión de la Privacidad y las Libertades Civiles sobre el artículo 702 de la Ley de vigilancia de inteligencia exterior (véase más adelante) debe ser especialmente informativo a este respecto.

Cambios institucionales y de procedimiento

En cuanto a los cambios institucionales y de procedimiento, la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos codificó varios procedimientos que ya se seguían en la práctica e introdujo nuevas garantías. Si bien algunos de ellos solo afectan a los ciudadanos estadounidenses, varios cambios aumentan la protección tanto para los ciudadanos estadounidenses como para los no estadounidenses cuyos datos pueden recogerse con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior[52] y, por tanto, son pertinentes para el funcionamiento del Marco de Privacidad de Datos.

[52] Además, Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos introdujo algunos cambios con respecto a la vigilancia electrónica individualizada tradicional contemplada en el artículo 105 de la Ley de vigilancia de inteligencia exterior (sobre la base de una orden dictada por el Tribunal de Vigilancia de Inteligencia Exterior si se cumple el criterio de la causa probable). Las solicitudes de los servicios de inteligencia al secretario de Justicia de que se dicte una orden para llevar a cabo una vigilancia electrónica individualizada deben ahora incorporar una declaración jurada en la que se justifiquen por qué se cumplen las condiciones del artículo 105 de la Ley de vigilancia de inteligencia exterior [artículo 6, letra a), de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos]. La posible duración de la vigilancia electrónica con respecto

En primer lugar, se estableció una serie de requisitos adicionales de rendición de cuentas, supervisión e información. En particular, el personal del Buró Federal de Investigaciones debe recibir ahora una formación anual sobre las normas aplicables a la consulta de información obtenida con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior[53]. El Buró Federal de Investigaciones también está obligado a informar al Congreso sobre sus actividades de consulta (por ejemplo, el número de consultas realizadas utilizando «tecnologías de trabajo por lotes», es decir, empleando varios términos de búsqueda como parte de una única consulta) y sobre las medidas de rendición de cuentas adoptadas para garantizar el cumplimiento de las obligaciones legales para realizar consultas (artículos 11 y 12 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos). Asimismo, se encarga al inspector general del Departamento de Justicia que elabore un informe sobre el cumplimiento de las obligaciones legales para realizar consultas por parte del Buró Federal de Investigaciones (artículo 9 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos). De manera más general, con el fin de aumentar la transparencia de los procesos sustanciados por el Tribunal de Vigilancia de Inteligencia Exterior, la Oficina del Director de Inteligencia Nacional y el secretario de Justicia están ahora obligados a completar el examen de desclasificación de las resoluciones del Tribunal de Vigilancia de Inteligencia Exterior en un plazo de 180 días (artículo 7 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos). Además, las transcripciones de todas las audiencias celebradas ante el Tribunal de Vigilancia de Inteligencia Exterior y el Tribunal de Apelación de Inteligencia Exterior (Foreign Intelligence Court of Review, FISCR, ante el que pueden recurrirse las resoluciones del Tribunal de Vigilancia de Inteligencia Exterior) deben conservarse y transmitirse al Congreso (artículo 8 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos).

En segundo lugar, Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos introdujo nuevas limitaciones relativas al uso por parte del Buró Federal de Investigaciones de los datos recogidos en el marco del artículo 702 de la Ley de vigilancia de inteligencia exterior. El artículo 2, letra d), de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos establece que una consulta con «tecnología de lotes» solo puede realizarse previa autorización de un fiscal del Buró Federal de Investigaciones, a menos que existan circunstancias apremiantes. Además, el Buró Federal de Investigaciones ahora tiene prohibido consultar automáticamente la información no minimizada obtenida con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior y, en su lugar, debe garantizar que los analistas tengan que seleccionar expresamente la búsqueda en dicha información. La Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos también ha prohibido al Buró Federal de Investigaciones realizar consultas destinadas exclusivamente a encontrar y extraer pruebas de una actividad delictiva (a menos que exista una convicción razonable de que podrían ayudar a mitigar o eliminar una amenaza para la vida o lesiones corporales graves o cuando sea necesario para cumplir las obligaciones de divulgación en litigios)[54]. Asimismo, el Buró Federal de Investigaciones tiene prohibido introducir datos no

a potencias extranjeras o agentes de potencias extranjeras se ha ampliado de 120 días a un año [artículo 6, letra g), de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos].

[53] Artículo 2, letra d), de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos.

[54] Artículo 3, letra a), de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos.

minimizados en repositorios analíticos, a menos que la persona en cuestión sea pertinente para una investigación de seguridad nacional en curso[55].

En tercer lugar, se han modificado determinadas disposiciones relativas al estatuto y a la función de los *amici curiae* ante el Tribunal de Vigilancia de Inteligencia Exterior[56]. Los *amici* son designados como expertos para asistir al Tribunal (y al Tribunal de Apelación de Inteligencia Exterior) en cuestiones relacionadas con la privacidad y las libertades civiles o para ayudar a aclarar cuestiones tecnológicas a la hora de tramitar una solicitud específica del Gobierno. Si bien la Ley de vigilancia de inteligencia exterior exigía anteriormente que los *amici* tuvieran conocimientos especializados en materia de privacidad y libertades civiles, recogida de inteligencia, tecnologías de la comunicación u otros ámbitos pertinentes, ahora exige, en principio, conocimientos especializados en materia de privacidad, libertades civiles y recogida de inteligencia. El Tribunal ya tenía la posibilidad de designar un *amicus* en cualquier caso que considerara oportuno y estaba obligado a hacerlo en caso de una interpretación nueva o significativa del Derecho. A raíz de la reautorización, el Tribunal de Vigilancia de Inteligencia Exterior ahora también está obligado a designar un *amicus* cada vez que se le pida que apruebe certificaciones con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior y los procedimientos correspondientes (por ejemplo, los procedimientos de selección de objetivos), a menos que considere que ello no sería adecuado o podría dar lugar a retrasos indebidos[57]. Además, en lugar de designar solo uno, el Tribunal de Justicia ahora puede decidir nombrar a uno o varios *amici*. Asimismo, se aclara que la información que deben facilitar los *amici* debe «limitarse a abordar las cuestiones específicas determinadas por el tribunal», aunque los ámbitos sobre los que los *amici* pueden formular observaciones siguen siendo amplios (es decir, argumentos jurídicos e información relacionados con la protección de la privacidad y las libertades civiles de los ciudadanos estadounidenses, la recogida de inteligencia, tecnologías de la comunicación o cualquier otro ámbito pertinente).

Por último, el artículo 18 de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos establece una «Comisión de Reforma de la Ley de vigilancia de inteligencia exterior», compuesta, entre otros, por miembros del Congreso, el presidente de la Junta de Supervisión de la Privacidad y las Libertades Civiles, el director adjunto principal de Inteligencia Nacional, el secretario de Justicia adjunto y otros miembros nombrados por el Congreso[58], para que recomiende reformas adicionales de la Ley de vigilancia de inteligencia exterior.

La Comisión seguirá de cerca la evolución de la situación con respecto al artículo 702 de la Ley de vigilancia de inteligencia exterior, en particular en el contexto de las actividades de supervisión de la Junta de Supervisión de la Privacidad y las Libertades Civiles (véase más adelante), el trabajo de la Comisión de Reforma y la próxima revisión de la Ley de vigilancia de inteligencia exterior al cabo de dos años.

2.2.1.3. Actividades de vigilancia en la práctica: cifras y tendencias

[55] Artículo 3, letra b), de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos. Cuando sea necesario debido a circunstancias apremiantes, el director del Buró Federal de Investigaciones puede decidir hacer una excepción a esta disposición, lo cual debe notificarse al Congreso.

[56] En aras de la claridad, estas modificaciones no afectan al estatuto ni a la función de los abogados especiales ante el Tribunal de Recurso en Materia de Protección de Datos, tal como confirmaron los Estados Unidos en la reunión de revisión.

[57] Artículo 5, letra b), de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos.

[58] El artículo 18 exige específicamente la representación de fuera del Congreso.

El informe anual de transparencia estadística de la Oficina del Director de Inteligencia Nacional en relación con el uso por parte de la Comunidad de Inteligencia de las autoridades nacionales de vigilancia de la seguridad en el año natural 2023 (publicado en abril de 2024)[59] muestra que el número de objetivos con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior aumentó de 245 073 en el año natural 2022 a 268 590 en el año natural 2023. El informe explica que las fluctuaciones en el número de objetivos pueden estar relacionadas con diversas razones, como cambios en las prioridades operativas, acontecimientos mundiales, capacidades técnicas, conducta de los objetivos y cambios en el sector de las telecomunicaciones. El informe también indica que ninguna persona no estadounidense (frente a una en 2021 y cero en 2022) fue seleccionada como objetivo con arreglo al artículo 402 de la Ley de vigilancia de inteligencia exterior (dispositivos de registro de comunicaciones salientes y entrantes), mientras que se emitieron seis órdenes (frente a once en 2021 y 2022), para seis objetivos (frente a trece en 2021 y once en 2022), con arreglo al artículo 501 de la Ley de vigilancia de inteligencia exterior (acceso a documentos comerciales de transportistas comunes, establecimientos de alquiler de vehículos o instalaciones de almacenamiento físico), que abarcaban 5 412 identificadores únicos (frente a 23 157 en 2021 y 55 431 en 2022) utilizados para comunicar la información recogida en virtud de dichas órdenes.

El informe anual del Departamento de Justicia sobre la Ley de vigilancia de inteligencia exterior al Congreso indica que, durante el año natural 2023, se presentaron al Tribunal de Vigilancia de Inteligencia Exterior 327 solicitudes para llevar a cabo actividades de vigilancia electrónica o registros físicos con fines de inteligencia exterior con arreglo a los artículos 105 y 302 de la Ley de vigilancia de inteligencia exterior, respectivamente[60]. El número total de personas seleccionadas como objetivos osciló entre 500 y 999. Por lo que se refiere a los requerimientos de seguridad nacional (*national security letters*), el informe indica que se emitieron 10 115 solicitudes (excluidas las solicitudes de información de abonados únicamente) de información sobre ciudadanos no estadounidenses, para obtener información sobre 3 033 ciudadanos no estadounidenses distintos[61].

Varias empresas certificadas con arreglo al Marco de Privacidad de Datos (por ejemplo, Google y Meta) hacen uso de la posibilidad prevista en la legislación estadounidense de publicar informes de transparencia que indiquen el número de solicitudes en virtud de la Ley de vigilancia de inteligencia exterior y de requerimientos de seguridad nacional que hayan recibido durante un período de notificación determinado. En el momento de la elaboración del presente informe, aún no se disponía de estadísticas sobre las solicitudes en virtud de la Ley de vigilancia de inteligencia exterior posteriores a julio de 2023. Google, por ejemplo, informó que había recibido entre 500 y 999 requerimientos de seguridad nacional, que afectaban a entre 2 000 y 2 499 cuentas, entre julio y diciembre de 2023[62]. Meta informó de que había recibido entre 0 y 499 requerimientos de seguridad nacional, que afectaban a entre 500 y 999 cuentas,

[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Estas cifras se han mantenido estables a grandes rasgos en relación con el año de notificación anterior (2022). En comparación, en 2022, hubo 317 solicitudes finales ante el Tribunal de Vigilancia de Inteligencia Exterior para llevar a cabo actividades de vigilancia electrónica o registros físicos con fines de inteligencia exterior. El número total de personas objeto de órdenes de vigilancia electrónica se situó entre 0 y 499. El Buró Federal de Investigaciones presentó 9 103 requerimientos de seguridad nacional para obtener información sobre ciudadanos no estadounidenses en 2022 (excluidas las solicitudes de información de abonados únicamente). Fuente: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.
[62] https://transparencyreport.google.com/user-data/us-national-security.

en el mismo período de notificación[63]. Las cifras se han mantenido bastante estables en los últimos años. A fin de aumentar aún más la transparencia, algunas empresas (por ejemplo, Google) publican de forma proactiva los requerimientos de seguridad nacional que han recibido una vez levantadas las restricciones de no divulgación[64].

2.2.1.4. Otros aspectos

En el marco de la preparación de la revisión, varias ONG han planteado preguntas sobre nuevas formas de obtención de datos por parte de los servicios de inteligencia estadounidenses mediante la compra de datos a entidades comerciales, en particular a intermediarios de datos. Explicaron que, si bien los datos recogidos sobre esta base deben tratarse de conformidad con otros requisitos, por ejemplo, con arreglo al Decreto Presidencial n.º 12333[65], dicha adquisición tiene lugar fuera del marco de la Ley de vigilancia de inteligencia exterior y del Decreto Presidencial n.º 14086.

A este respecto, cabe recordar que cualquier tipo de intercambio voluntario de datos con terceros está sujeto a varias condiciones detalladas del Marco de Privacidad de Datos. En primer lugar, la entidad certificada no puede compartir datos con terceros (que no actúen como agentes o encargados del tratamiento) sin notificarlo ni ofrecer el derecho de opción a las personas afectadas[66]. En segundo lugar, de conformidad con el *principio de responsabilidad proactiva por las transferencias ulteriores*, dichas transferencias solo pueden realizarse 1) para fines limitados y especificados, 2) sobre la base de un contrato entre la entidad participante y el tercero y 3) solo si dicho contrato exige al tercero que confiera el mismo nivel de protección que el garantizado por los principios en materia de privacidad[67].

Además, como también se debatió durante la reunión de revisión, la Comisión Federal de Comercio ha adoptado medidas de ejecución contra los intermediarios de datos que venden datos sensibles de los consumidores. Por ejemplo, en un asunto contra *X-Mode* y su sucesor *Outlogic*, la Comisión Federal de Comercio adoptó una orden el 9 de enero de 2024 por la que se prohibía a la empresa vender datos de geolocalización a terceros y se exigía la supresión de los datos que había utilizado y compartido ilícitamente. La investigación de la Comisión Federal de Comercio constató, entre otras cosas, que la empresa no había informado plenamente a las personas del uso y la venta de sus datos de geolocalización, no había adoptado medidas que permitieran a las personas acogerse a la exclusión voluntaria del seguimiento, había permitido el uso de los datos con fines potencialmente discriminatorios y no había limitado el uso de dicha información por parte de terceros[68]. La Comisión espera que la Comisión Federal de Comercio adopte el mismo enfoque si las empresas certificadas con arreglo al Marco de Privacidad de Datos compartieran datos infringiendo las disposiciones mencionadas.

Por último, cabe mencionar que, en mayo de 2024, la Oficina del Director de Inteligencia Nacional publicó el Marco político de la Comunidad de Inteligencia para la información

[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] Véase, por ejemplo, el artículo 2.4 del Decreto Presidencial n.º 12333 sobre las técnicas de recogida.
[66] Véase el considerando 40 de la decisión de adecuación.
[67] Véase el considerando 38 de la decisión de adecuación.
[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

comercialmente disponible[69]. Este Marco establece una serie de principios y requisitos que los servicios de inteligencia deben seguir, en particular con el fin de minimizar los riesgos para la privacidad y las libertades civiles, al adquirir y utilizar información en el contexto de una transacción comercial.

2.2.2. Supervisión independiente

Las actividades de los servicios de inteligencia estadounidenses están sujetas a la supervisión de diferentes organismos, incluidos los responsables de la protección de la privacidad y de las libertades civiles, los inspectores generales, el Congreso y la Junta de Supervisión de la Privacidad y de las Libertades Civiles. En particular, 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. 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[70]. 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.

El asesor general de la Oficina del Inspector General de la Comunidad de Inteligencia (Office of the Intelligence Community Inspector General, ICIG) de la Oficina del Director de Inteligencia Nacional, 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, participó en la reunión de revisión. Confirmó que la Oficina del Inspector General de la Comunidad de Inteligencia controla sistemáticamente el cumplimiento del Decreto Presidencial n.º 14086 como parte de sus actividades de supervisión. También hizo referencia a las recientes actividades de supervisión de otros inspectores generales de la Comunidad de Inteligencia, tal como se detalla en los informes periódicos. Por ejemplo, en su informe semestral al Congreso correspondiente a los meses de abril a septiembre de 2023[71], el inspector general de la Agencia Nacional de Seguridad informó sobre una evaluación de un marco de control interno de dicha Agencia para las decisiones de selección de objetivos y las solicitudes. Se concluyó que este marco funcionaba correctamente para garantizar el cumplimiento de las leyes, directivas y políticas que protegen las libertades civiles

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Los servicios de inteligencia están obligados a cumplir el Marco desde agosto de 2024.

[70] Cada servicio de inteligencia cuenta con un inspector general que goza de independencia por mandato legal y se encarga de llevar a cabo auditorías e investigaciones sobre las actividades llevadas a cabo por el servicio correspondiente con fines de seguridad nacional. Pueden consultar todo el material pertinente (también el clasificado), previo requerimiento si es preciso, y pueden tomar declaración. 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. Aunque sus recomendaciones no son vinculantes, sus informes, especialmente los relativos a las actuaciones a raíz de recomendaciones (o a su ausencia), generalmente se publican y se transmiten asimismo al Congreso. Véase a este respecto la nota a pie de página n.º 136 de la decisión de adecuación sobre el papel del inspector general.

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

y la privacidad. El mismo informe también menciona una investigación que reveló el uso indebido de una herramienta de inteligencia de señales con fines no autorizados por parte de un trabajador de la Agencia Nacional de Seguridad.

En virtud del Decreto Presidencial n.º 14086, la Junta de Supervisión de la Privacidad y las Libertades Civiles[72] tiene encomendadas funciones de supervisión específicas[73]. El presidente de la Junta de Supervisión de la Privacidad y las Libertades Civiles y sus tres miembros participaron en la reunión de revisión e informaron de que la Junta proporcionó asesoramiento a los servicios de inteligencia sobre sus proyectos de directrices y procedimientos para la aplicación del Decreto Presidencial n.º 14086 en abril de 2023 y fue consultada sobre el nombramiento de los jueces y abogados especiales del Tribunal de Recurso en Materia de Protección de Datos (Data Protection Review Court, DPRC). La Junta también puso en marcha un proyecto de supervisión para 1) revisar la aplicación de las políticas y procedimientos actualizados adoptados por los servicios de inteligencia para garantizar que sean coherentes con el Decreto Presidencial y 2) llevar a cabo una revisión anual del funcionamiento de la nueva vía de recurso (véase más adelante)[74]. Los miembros de la Junta de Supervisión de la Privacidad y las Libertades Civiles confirmaron que esta tiene previsto llevar a cabo ambas revisiones en un futuro próximo. Con respecto a la reparación, explicaron que, a falta de reclamaciones, la revisión de la Junta de Supervisión de la Privacidad y las Libertades Civiles se centrará en las políticas y procedimientos aplicados para establecer la vía de recurso.

En cuanto a otras actividades de supervisión, la Junta de Supervisión de la Privacidad y las Libertades Civiles publicó un informe sobre el artículo 702 de la Ley de vigilancia de inteligencia exterior el 28 de septiembre de 2023[75]. Este informe es un seguimiento de un informe anterior de 2014 y contiene información fáctica y jurídica actualizada sobre el funcionamiento de los programas de vigilancia con arreglo al artículo 702 de la Ley de vigilancia de inteligencia exterior. El informe también contiene recomendaciones sobre el cumplimiento por parte de los servicios de inteligencia de los requisitos aplicables y sugerencias al Congreso para seguir reforzando varios aspectos del artículo 702 de la Ley de vigilancia de inteligencia exterior en el marco de su reautorización (en particular mediante la codificación de los objetivos legítimos de las actividades de vigilancia mencionadas en el Decreto Presidencial n.º 14086)[76]. Durante la reunión de revisión, la Junta de Supervisión de la Privacidad y las Libertades Civiles informó de que espera recibir en breve respuestas de los

[72] La Junta de Supervisión de la Privacidad y las Libertades Civiles es un organismo independiente que 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. Puede acceder a toda la información pertinente (incluida la clasificada), realizar interrogatorios y tomar declaración. Puede formular recomendaciones a las autoridades policiales y de inteligencia e informa periódicamente al Congreso y al presidente. Sus informes se ponen a disposición del público en la mayor medida posible.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

[76] La Comisión observa que algunas de estas recomendaciones se han incorporado como parte de la Ley de reforma de actividades de inteligencia y seguridad de los Estados Unidos, como la recomendación relativa a la recogida de comunicaciones sobre selectores o la recomendación relativa al refuerzo del papel de los expertos del Tribunal de Vigilancia de Inteligencia Exterior (*amici*).

servicios de inteligencia sobre la aplicación de sus recomendaciones, que se tendrán en cuenta en el futuro informe de seguimiento. Otros proyectos de supervisión en curso son uno sobre la lucha contra el terrorismo interior y su incidencia en la privacidad y las libertades civiles y la recogida de datos de código abierto o comercialmente disponibles por el Buró Federal de Investigaciones[77].

Por último, las ONG consultadas en el marco de la revisión expresaron su preocupación por el hecho de que el mandato de varios miembros de la Junta de Supervisión de la Privacidad y las Libertades Civiles vencerá en un futuro próximo, lo que podría dejar a la Junta sin *quorum*. En particular, el mandato de la presidenta ha expirado y el período durante el cual puede actuar en calidad de interina finaliza en enero de 2025, mientras que otro puesto está vacante y un tercero también quedará vacante en enero del próximo año. Durante la reunión de revisión, los miembros explicaron que no esperan que la Junta de Supervisión de la Privacidad y las Libertades Civiles llegue a estar sin *quorum*, pues ya se ha presentado una candidatura para el puesto actualmente vacante (y está a la espera de confirmación por el Senado)[78]. También subrayaron que, incluso si la Junta perdiera su *quorum*, esto no afectaría a su capacidad para seguir llevando a cabo proyectos de supervisión. No obstante, dado el importante papel de la Junta de Supervisión de la Privacidad y las Libertades Civiles en la revisión de la aplicación del Decreto Presidencial n.º 14086, la Comisión seguirá de cerca la situación de las vacantes y los nombramientos o designaciones futuros.

2.2.3. Reparación

El Decreto Presidencial n.º 14086, complementado con un Reglamento del secretario de Justicia, estableció una nueva vía de recurso para tramitar y resolver las reclamaciones admisibles de particulares relativas a actividades de inteligencia de señales estadounidenses[79]. 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) con respecto a los datos personales transferidos a los Estados Unidos que afecten negativamente a sus intereses en materia de privacidad y libertades civiles. Los particulares pueden presentar una reclamación ante una APD de un Estado miembro de la UE, que canaliza la reclamación, a través de la Secretaría del CEPD, al órgano correspondiente. La vía consta de dos niveles; la investigación inicial de las reclamaciones la lleva a cabo el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y los particulares tienen la posibilidad de recurrir la decisión de la Oficina del Director de Inteligencia Nacional ante un Tribunal de Recurso en Materia de Protección de Datos independiente. Una vez que el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional o el Tribunal de Recurso en Materia de Protección de Datos finalizan el examen, se informa a los particulares, 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 o el Tribunal de Recurso en Materia de Protección de Datos exigieron una reparación adecuada. Las decisiones del responsable de la protección de las libertades civiles de la Oficina del Director de

[77] https://www.pclob.gov/OversightProjects.
[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Considerandos 176 a 194 de la decisión de adecuación.

Inteligencia Nacional y del Tribunal de Recurso en Materia de Protección de Datos son vinculantes para los servicios de inteligencia.

Desde la adopción de la decisión de adecuación, se han tomado nuevas medidas para que la vía de recurso sea plenamente operativa.

Por lo que se refiere a la creación del Tribunal de Recurso en Materia de Protección de Datos, el 14 de noviembre de 2023 se nombraron ocho jueces del Tribunal [es decir, dos jueces más que el número mínimo exigido en virtud del Decreto Presidencial n.º 14086, complementado por los reglamentos del secretario de Justicia en el título 28, artículo 201.3, letra a), del Código de Reglamentos Federales][80]. Fueron nombrados sobre la base de los criterios recogidos en el Decreto Presidencial n.º 14086 y de conformidad con el proceso establecido en él, incluso previa consulta, entre otros, a la Junta de Supervisión de la Privacidad y de las Libertades Civiles[81]. Entre ellos figuran antiguos jueces de tribunales federales de distrito y del Tribunal de Apelación, un antiguo secretario de Justicia de los Estados Unidos y un antiguo miembro de la Junta de Supervisión de la Privacidad y de las Libertades Civiles. Tal como exige el Decreto Presidencial, al menos la mitad de los jueces tienen experiencia judicial previa. Además, en abril de 2024, se nombraron dos abogados especiales, profesionales del Derecho con experiencia tanto en privacidad como en seguridad nacional, para que representen los intereses de los particulares ante el Tribunal de Recurso en Materia de Protección de Datos. En la reunión de revisión se confirmó que todos los jueces y abogados especiales han recibido la habilitación de seguridad más alta y, por tanto, pueden acceder a materiales clasificados en el desempeño de sus funciones para el Tribunal de Recurso en Materia de Protección de Datos. Este Tribunal también había publicado una serie de preguntas frecuentes, que proporcionaban más información sobre su papel, su independencia y su funcionamiento[82].

En cuanto a la tramitación de las reclamaciones, el 6 de diciembre de 2022, la Oficina del Director de Inteligencia Nacional adoptó la Directiva de los Servicios de Inteligencia n.º 126, que regula de manera detallada (fijando plazos, creando un repositorio electrónico seguro y canales de comunicación, exigiendo al responsable de la protección de las libertades civiles y a la Comunidad de Inteligencia que cooperen con la Junta de Supervisión de la Privacidad y las Libertades Civiles en el marco de la revisión anual de la vía de recurso, etc.) diferentes aspectos del proceso de investigación y resolución de reclamaciones[83]. Esta Directiva es aplicable a toda la Comunidad de Inteligencia de los Estados Unidos y se ha complementado con los procedimientos internos adoptados por los distintos servicios de inteligencia para su cooperación con el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional en el marco de la tramitación de reclamaciones (por ejemplo, el desarrollo de un repositorio seguro para compartir reclamaciones y documentos de respuesta; y comunicaciones seguras entre los organismos pertinentes). En los próximos meses, el Tribunal de Recurso en Materia de Protección de Datos también adoptará normas más detalladas sobre la tramitación de reclamaciones y otros aspectos de procedimiento.

En la Unión Europea y los Estados Unidos se adoptaron varias medidas adicionales para informar a la sociedad, así como para facilitar la presentación y tramitación de reclamaciones.

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Artículo 3, letra d), subletra A), del Decreto Presidencial n.º 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.

Entre ellas se cuenta la adopción por parte del CEPD de una nota informativa sobre la nueva vía de procesal[84], un modelo de formulario de reclamación (que lo traducirán y publicarán todas las APD en sus lenguas nacionales)[85] y normas de procedimiento que rigen la cooperación entre las autoridades de control nacionales y la Secretaría del CEPD[86]. Del mismo modo, la Oficina del Director de Inteligencia Nacional publicó un documento de respuestas a preguntas frecuentes y una ficha informativa sobre la nueva vía procesal y participó en actividades de concienciación pública[87].

Además, durante el último año, el CEPD y las autoridades estadounidenses pertinentes han colaborado estrechamente en varios aspectos operativos. En particular, como se confirmó durante la reunión de revisión, establecieron un canal de comunicación cifrado para transmitir las reclamaciones de las autoridades nacionales de la UE a la Secretaría del CEPD, de la Secretaría del CEPD al responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional, así como a la Oficina de Privacidad y Libertades Civiles (Office of Privacy and Civil Liberties, OPCL) del Departamento de Justicia, y entre el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional y otras autoridades de los Estados Unidos (por ejemplo, el Tribunal de Recurso en Materia de Protección de Datos). Además, el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional explicó que se han establecido otros procedimientos internos para su cooperación con los distintos servicios de inteligencia en lo que respecta a la tramitación de reclamaciones.

Por último, la Oficina de Privacidad y Libertades Civiles, que presta apoyo administrativo al Tribunal de Recurso en Materia de Protección de Datos, también informó de que dicho Tribunal opera con cargo a su propia línea presupuestaria específica y dispone del equipo necesario para llevar a cabo sus tareas, como ordenadores y ordenadores portátiles seguros, teléfonos, etc. Además, tal como exige el Decreto Presidencial n.º 14086, el Departamento de Comercio ha adoptado las medidas necesarias, en particular mediante la creación de un canal de comunicación cifrado con el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional, para llevar un registro de todas las reclamaciones admisibles recibidas. El Departamento de Comercio se pondrá periódicamente en contacto con el responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional para saber si se ha desclasificado la información relativa a una reclamación individual. En caso afirmativo, el Departamento de Comercio lo notificará al interesado, a fin de permitirle acceder a dicha información.

En el momento de la reunión de revisión, las autoridades de control de la UE no habían recibido ninguna reclamación, por lo que aún no se había activado la nueva vía procesal.

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_es.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_es.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_es.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf y https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

3. CONCLUSIÓN

Sobre la base de la información recopilada durante esta primera revisión, la Comisión concluye que las autoridades estadounidenses han establecido las estructuras y procedimientos necesarios para garantizar el funcionamiento eficaz del Marco de Privacidad de Datos. En este contexto, la Comisión valora enormemente la excelente cooperación con las autoridades estadounidenses para llevar a cabo la revisión.

Aunque esta primera revisión se centró lógicamente en verificar si se han implantado todos los elementos constitutivos del marco, la experiencia con la aplicación práctica de las garantías aplicables tanto al tratamiento de datos por las empresas certificadas como al acceso a los datos por las autoridades públicas es necesariamente limitada tras solo un año de funcionamiento. Por consiguiente, la Comisión seguirá de cerca las novedades pertinentes en los próximos meses y años, prestando especial atención a 1) los próximos informes de la Junta de Supervisión de la Privacidad y las Libertades Civiles sobre la aplicación del Decreto Presidencial n.º 14086 y el funcionamiento de la vía procesal relacionada con la inteligencia de señales, en particular el Tribunal de Recurso en Materia de Protección de Datos; 2) las posibles modificaciones futuras del artículo 702 de la Ley de vigilancia de inteligencia exterior; y 3) el nombramiento y la designación de miembros de la Junta de Supervisión de la Privacidad y las Libertades Civiles para cubrir las próximas vacantes.

Además, a fin de garantizar un funcionamiento continuo y eficaz, la Comisión considera importante que:

- como se anunció en la reunión de revisión, el Departamento de Comercio utilice mejor las diferentes herramientas previstas en el Marco de Privacidad de Datos para controlar el cumplimiento de los principios en materia de privacidad por parte de las empresas y detectar las declaraciones falsas de participación;
- la Comisión Federal de Comercio siga desarrollando su enfoque proactivo para la investigación y la garantía del cumplimiento de los principios del Marco de Privacidad de Datos por parte de las empresas certificadas; y
- el Departamento de Comercio, la Comisión Federal de Comercio y las autoridades de protección de datos de la UE elaboren instrumentos de orientación comunes sobre los requisitos clave de los principios del Marco de Privacidad de Datos, por ejemplo, sobre los datos de recursos humanos y las transferencias ulteriores.

A la luz de este resultado de la revisión y tal como se prevé en el considerando 211 de la decisión de adecuación, la Comisión considera adecuado llevar a cabo la próxima revisión periódica al cabo de tres años. Esto debería permitir adquirir más experiencia en la aplicación práctica del Marco de Privacidad de Datos y tener en cuenta los próximos cambios antes mencionados. Por tanto, de conformidad con el artículo 3, apartado 4, de la decisión de adecuación, la Comisión consultará al CEPD y al Comité establecido en virtud del artículo 93, apartado 1, del Reglamento general de protección de datos sobre la periodicidad de las próximas revisiones.