Dictamen del Comité (art. 70.1.s)

Dictamen 5/2023 sobre el proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación de la protección de los datos personales de acuerdo con el marco de privacidad de datos UE-EE. UU.

Adoptado el 28 de febrero de 2023

Resumen

El 13 de diciembre de 2022, la Comisión Europea publicó un proyecto de Decisión de adecuación (en lo sucesivo «proyecto de Decisión») que incluye anexos que constituyen un nuevo marco para los intercambios transatlánticos de datos personales, el marco de privacidad de datos UE-EE. UU. (en lo sucesivo, «MPD»), que tiene por objeto sustituir al Escudo de la privacidad UE-EE. UU., invalidado por el Tribunal de Justicia de la Unión Europea (en lo sucesivo, «TJUE») el 16 de julio de 2020 en el asunto Schrems II. El componente fundamental del MPD son los principios del marco de privacidad de datos UE-EE. UU., en particular los principios complementarios (denominados conjuntamente «los principios del MPD»).

Conforme al artículo 70, apartado 1, letra s), del Reglamento (UE) 2016/679[1] del Parlamento Europeo y del Consejo (en lo sucesivo, «el RGPD»), la Comisión solicitó el dictamen del Comité Europeo de Protección de Datos (en lo sucesivo, «el CEPD») sobre el proyecto de Decisión.

El CEPD evaluó la adecuación del nivel de protección concedido por EE. UU. sobre la base del examen del proyecto de Decisión. Analizó, asimismo, los aspectos comerciales y el acceso a los datos personales transferidos por los poderes públicos desde la UE a EE. UU., así como la utilización de estos datos.

El CEPD tuvo en cuenta el marco jurídico de protección de datos de la UE aplicable según lo establecido en el RGPD, así como los derechos fundamentales a la vida privada y a la protección de datos consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 8 del Convenio Europeo de Derechos Humanos. Asimismo, contempló el derecho a la tutela judicial efectiva y a un juez imparcial establecido en el artículo 47 de la Carta, así como la jurisprudencia relacionada con diversos derechos fundamentales.

Además, el CEPD ha considerado los requisitos del documento relativo a las referencias sobre adecuación adoptado por el CEPD[2].

El principal objetivo del CEPD es emitir un dictamen para la Comisión sobre la adecuación del nivel de protección conferido a los particulares cuyos datos personales se trasfieren a EE. UU. Es importante reconocer que el CEPD no espera que el marco de protección de datos de los EE. UU. refleje punto por punto la legislación europea en materia de protección de datos.

Sin embargo, el CEPD recuerda que, para considerar que existe un nivel de protección adecuado, el artículo 45 del RGPD y la jurisprudencia del TJUE exigen que la legislación del tercer país ofrezca a los interesados un nivel de protección equivalente, en lo esencial, al garantizado en la UE.

1.1. Aspectos generales relativos a la protección de datos

El MPD establece que el cumplimiento de sus principios por parte de las entidades adheridas al MPD se puede limitar en algunos casos (por ejemplo, en la medida necesaria para cumplir un mandato judicial o para cumplir un objetivo de interés público). Con vistas a determinar mejor la repercusión de

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DO L 119 de 4.5.2016, p. 1).

[2] Grupo de Trabajo del Artículo 29, Documento relativo a las referencias sobre adecuación, WP 254 rev. 01, 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018, refrendado por el CEPD el 25 de mayo de 2018 (en lo sucesivo, «documento relativo a las referencias sobre adecuación»).

estas exenciones relativas al nivel de protección de los interesados, el CEPD recomienda a la Comisión que incluya en el proyecto de Decisión una aclaración sobre el ámbito de aplicación de las exenciones, también sobre las garantías aplicables en virtud de la legislación de los Estados Unidos.

El CEPD señala que la estructura de los anexos y su numeración dificulta la localización de la información y su consulta. Esto contribuye a una presentación general compleja del nuevo marco, que compila, en sus anexos, documentos de valor jurídico diferente y puede dificultar la correcta comprensión de los principios del MPD por parte de los interesados, las entidades adheridas al MPD y las autoridades de protección de datos en la UE. El CEPD también recalca que la terminología debería utilizarse de forma coherente a lo largo de todo el MPD. Asimismo, se echa en falta la definición de algunos términos esenciales[3].

El CEPD acoge favorablemente las actualizaciones de los principios del MPD[4], que constituirán el marco jurídico vinculante para las entidades adheridas al MPD, pero observa que, a pesar del número de cambios y explicaciones adicionales introducidos en los considerandos del proyecto de Decisión, los principios del MPD que las entidades adheridas al MPD deben respetar siguen siendo esencialmente idénticos a los que se aplicaban en virtud del Escudo de la privacidad [en los que se basaron las revisiones conjuntas anuales del Grupo de Trabajo del artículo 29 (en lo sucesivo, «GT29») y el CEPD]. Los principios del MPD son también, en gran medida, los mismos que se recogen en el proyecto del Escudo de la privacidad en los que el GT29 basó su dictamen de 2016[5]. Por lo que se refiere a los principios del MPD que siguen siendo esencialmente idénticos, el CEPD no considera necesario repetir todos los comentarios ya realizados por el GT29. El CEPD ha decidido centrarse en aspectos específicos que considera que son aún más pertinentes hoy en día, habida cuenta de la evolución del entorno jurídico y tecnológico.

Por ejemplo, el CEPD observa que persisten algunos de los motivos de preocupación planteados previamente por el GT29 y el propio CEPD en relación con los principios del Escudo de la privacidad. En particular, las cuestiones relacionadas con los derechos de los interesados (como algunas excepciones al derecho de acceso y el momento y las modalidades de ejercicio del derecho de oposición), la ausencia de definiciones clave, la falta de claridad en relación con la aplicación de los principios del MPD a los encargados del tratamiento, y la amplia exención para la información públicamente disponible[6].

Asimismo, el CEPD desearía reiterar que el nivel de protección de los particulares cuyos datos se transfieren no debe verse menoscabado por transferencias ulteriores del destinatario inicial de los datos transferidos[7]. Una vez más, el CEPD invita a la Comisión a que aclare que las garantías impuestas por el destinatario inicial al importador en el tercer país deben ser efectivas a la luz de la legislación del tercer país, antes de que se produzca una transferencia ulterior en el contexto del MPD.

Merecen especial atención los rápidos avances experimentados en el ámbito de las decisiones automatizadas y la elaboración de perfiles, que cada vez se realizan más a través de tecnología de

[3] Como ocurre con los términos «agente» y «encargado del tratamiento». Además, el concepto de «datos de recursos humanos (RR. HH.)» aún debe debatirse con las autoridades estadounidenses.

[4] Por ejemplo, la aclaración de que los datos codificados son datos personales.

[5] Grupo de Trabajo del artículo 29, Dictamen 01/2016 sobre el proyecto de Decisión sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., adoptado el 13 de abril de 2016 (en lo sucesivo, «Dictamen 01/2016 del GT29»).

[6] Escudo de la privacidad UE-EE. UU. - Tercera revisión conjunta anual, informe del CEPD adoptado el 12 de noviembre de 2019, apartado 11.

[7] Documento relativo a las referencias sobre adecuación con arreglo al RGPD, 3.A.9.

inteligencia artificial (en lo sucesivo, «IA»). El CEPD acoge con satisfacción las referencias de la Comisión a garantías específicas proporcionadas por la legislación estadounidense pertinente en distintos ámbitos[8]. Sin embargo, el nivel de protección de los particulares parece variar de acuerdo con las normas sectoriales específicas, cuando estas existen, que se aplican a la situación de que se trate. El CEPD mantiene que, para proporcionar garantías suficientes, se necesitan normas específicas relativas a las decisiones automatizadas, en concreto el derecho del particular de conocer la lógica subyacente, para impugnar la decisión y obtener intervención humana cuando la decisión le afecte significativamente.

El CEPD recuerda la importancia de la supervisión y el control de la aplicación del MPD, y considera crucial la comprobación del cumplimiento en relación con los requisitos más sustantivos. El CEPD someterá estos aspectos a una estrecha vigilancia, incluso en el contexto de las revisiones periódicas. El CEPD toma nota de los compromisos renovados contenidos en las cartas de la Comisión Federal de Comercio (en lo sucesivo, «FTC», por sus siglas en inglés)[9] y el Departamento de Transporte (en lo sucesivo, «DOT», por sus siglas en inglés)[10] por lo que respecta al control de la aplicación, por ejemplo, para priorizar la investigación de supuestas infracciones del MPD.

El CEPD observa que se ofrecen siete vías de recurso a los interesados de la UE, en caso de que sus datos se traten infringiendo el MPD. Estos mecanismos de recurso son los mismos que figuran en el antiguo Escudo de la privacidad, que habían sido objeto de observaciones por parte del GT29[11]. El CEPD someterá a estrecha vigilancia la eficacia de estos mecanismos de recurso, también en el contexto de las revisiones periódicas.

1.2. Acceso a datos personales transferidos desde la Unión Europea y utilización de estos por parte de los poderes públicos estadounidenses

En el proyecto de Decisión, la Comisión Europea concluye que toda vulneración del interés público, en particular a efectos de control de la aplicación del Derecho penal y de seguridad nacional, por los poderes públicos estadounidenses de los derechos fundamentales de los particulares cuyos datos personales sean transferidos desde la Unión Europea a Estados Unidos en virtud del marco de privacidad de datos UE-EE. UU. se limitará a lo estrictamente necesario para alcanzar el objetivo legítimo perseguido, y que existe una tutela judicial efectiva contra tales vulneraciones[12].

La Comisión Europea basa su conclusión en una evaluación exhaustiva del *Executive Order* (decreto) 14086, que amplía las garantías para las actividades de inteligencia de señales de los EE. UU. (en lo sucesivo «EO 14086»). El EO 14086 fue adoptado por el Presidente de los Estados Unidos el 7 de octubre de 2022 tras las negociaciones de la Comisión Europea con el Gobierno de los Estados Unidos a raíz de la invalidación de la Decisión de adecuación previa, denominada Escudo de la privacidad, por parte del TJUE.

El CEPD acogería con satisfacción que, no solo la entrada en vigor, sino también la adopción de la Decisión, se condicionen a, entre otras cosas, la adopción de unas políticas y procedimientos actualizados para la aplicación del EO 14086 por parte de todas las agencias de inteligencia estadounidenses. El CEPD recomienda a la Comisión que evalúe estas políticas y procedimientos actualizados y comparta su evaluación con el CEPD.

[8] Proyecto de Decisión, considerando 35.
[9] Proyecto de Decisión, anexo IV.
[10] Proyecto de Decisión, anexo V.
[11] Véase en concreto el Dictamen 01/2016 del GT29, apartado 2.2.6, letra a).
[12] Proyecto de Decisión, considerando 195.

Por lo que respecta al acceso de las autoridades públicas a los datos personales transferidos a EE. UU., el CEPD ha centrado su análisis en la evaluación del nuevo EO 14086, ya que, en la práctica, está destinado a abordar y subsanar las deficiencias detectadas por el TJUE en la sentencia Schrems II, en la que declaró inválida la anterior Decisión de adecuación.

El CEPD reconoce que el marco jurídico estadounidense relativo a las actividades de inteligencia de señales se ha modificado mediante la adopción del EO 14086 y considera que las garantías adicionales incluidas en este decreto constituyen una mejora importante. El EO 14086 introduce los conceptos de necesidad y proporcionalidad en el marco jurídico estadounidense relativo a la inteligencia de señales, y prevé un nuevo mecanismo de recurso para los ciudadanos de la Unión en caso de que la UE adquiriera la designación de organización regional de integración económica elegible. El CEPD considera que el nuevo mecanismo de recurso se ha mejorado significativamente con respecto al anterior mecanismo del Defensor del Pueblo previsto en el Escudo de la privacidad. Al contrario que el marco jurídico anterior, que no creaba derechos para los ciudadanos de la Unión, como observó específicamente el TJUE, el nuevo EO 14086 sí crea dichos derechos, y prevé más garantías para la independencia del Tribunal de Revisión de la Protección de Datos y competencias más efectivas para subsanar las infracciones.

Al comparar las garantías adicionales recogidas en el EO 14086 con las que el CEPD ha calificado como las garantías esenciales europeas, como norma elaborada sobre la base de la jurisprudencia del TJUE y el Tribunal Europeo de Derechos Humanos (en lo sucesivo, «TEDH»), el CEPD sigue detectando en su evaluación una serie de puntos que requieren aclaración adicional, atención o cuidado. Estos puntos reflejan que, si bien el CEPD basó su dictamen en la sentencia Schrems II, el ámbito de su evaluación incluye necesariamente consideraciones que trascienden las constataciones específicas de dicha sentencia.

El CEPD observa que aún es preciso esclarecer algunas cuestiones, en particular, las relacionadas con la «recopilación en bloque temporal» y con la conservación y divulgación ulteriores de los datos recogidos (en bloque) en el marco jurídico estadounidense.

Dado que la prueba de equivalencia sustancial no es una prueba de identidad, y dado que las garantías previstas en el nuevo marco jurídico relativo a la inteligencia de señales se han reforzado, el principal punto de atención y preocupación del CEPD se centra en una evaluación de las garantías en su totalidad, siguiendo un enfoque holístico que cubra las garantías para el ciclo de tratamiento completo, desde la recogida de los datos hasta su divulgación, y que incluya los elementos de supervisión y recurso.

A este respecto, el CEPD subraya las siguientes constataciones:

Si bien el CEPD reconoce que el EO 14086 introduce los conceptos de necesidad y proporcionalidad en el marco jurídico relativo a la inteligencia de señales, subraya la necesidad de someter los efectos prácticos de estas modificaciones a una vigilancia estrecha, en particular, la revisión de las políticas y los procedimientos internos que aplican las garantías del EO a nivel de agencia.

El CEPD también acoge con satisfacción el hecho de que el EO 14086 contenga una lista de finalidades específicas en virtud de las que puede o no tener lugar la recogida, observando que los objetivos se pueden actualizar con objetivos adicionales —no necesariamente públicos— a la luz de nuevos imperativos de seguridad nacional.

Como deficiencia del marco actual, el CEPD ha detectado, en particular, que el marco jurídico estadounidense carece del requisito de autorización previa por parte de una autoridad independiente

al permitir la recopilación de datos en bloque en virtud del EO 12333, tal y como exige la mayor parte de la jurisprudencia reciente del TEDH, así como tampoco establece una revisión *ex post* independiente sistemática de un órgano jurisdiccional o un organismo independiente equivalente. Con respecto a la autorización previa independiente de vigilancia en virtud del artículo 702 de la *Foreign Intelligence Surveillance Act* (Ley de Vigilancia de Inteligencia Exterior; en lo sucesivo, «FISA»), el CEPD lamenta que el Tribunal de la FISA (en lo sucesivo, «FISC») no revise el cumplimiento del EO 14086 a la hora de certificar el programa que autoriza la segmentación de personas no estadounidenses, aunque las autoridades de inteligencia que llevan a cabo el programa estén vinculadas a él. En opinión del CEPD, las garantías adicionales contenidas en este EO deberían, no obstante, ser tenidas en cuenta, también por el FISC. El CEPD recuerda que los informes del Consejo de Supervisión de la Privacidad y de las Libertades Civiles (en lo sucesivo, «PCLOB») resultarían particularmente útiles para evaluar el modo en que se ejecutarán las garantías del EO 14086 y cómo se aplicarán cuando los datos se recojan en virtud del artículo 702 de la FISA y el EO 12333.

Por lo que respecta al mecanismo de recurso, el CEPD reconoce una mejora significativa en relación con las competencias del Tribunal de Revisión de la Protección de Datos (en lo sucesivo, «DPRC») y la ampliación de su independencia en comparación con el mecanismo del Defensor del Pueblo. El CEPD también reconoce las garantías adicionales previstas en el nuevo mecanismo de recurso, como la función de los letrados especiales, que incluye la defensa en relación con el interés del reclamante, así como la revisión del mecanismo de recurso por parte del PCLOB. Aunque tiene en cuenta el carácter de la seguridad nacional y las garantías previstas en el EO 14086, el CEPD alberga dudas sobre la aplicación general de la respuesta tipo del DPRC al notificar al reclamante que no se detectaron infracciones cubiertas o bien que se emitió una decisión que requiere una reparación adecuada, así como sobre la imposibilidad de recurso. Habida cuenta de la importancia del mecanismo de recurso, el CEPD insta a la Comisión a que supervise de forma más estrecha el funcionamiento práctico de dicho mecanismo.

El CEPD espera que la Comisión dé seguimiento a su compromiso de suspender, derogar o modificar la Decisión de adecuación por motivos de urgencia, en particular si el poder ejecutivo de los EE. UU. decidiera restringir las garantías establecidas en el EO[13].

En general, el CEPD observa con satisfacción las mejoras sustanciales que el EO ofrece en comparación con el marco jurídico anterior, en particular por lo que respecta a la introducción de los principios de necesidad y proporcionalidad y al mecanismo de recurso individual para los interesados de la UE. Habida cuenta de las preocupaciones expresadas y de las aclaraciones solicitadas, el CEPD señala la necesidad de abordar estas preocupaciones y de que la Comisión proporcione las aclaraciones solicitadas para consolidar las bases del proyecto de Decisión y garantizar una supervisión estrecha de la aplicación concreta de este nuevo marco jurídico, en particular de las garantías que este brinda, en las futuras revisiones conjuntas.

[13] Proyecto de Decisión, considerando 212.

Índice

El Comité Europeo de Protección de Datos

El Comité Europeo de Protección de Datos ha adoptado la declaración siguiente:

Visto el artículo 70, apartado 1, letra s), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, «el RGPD»)[1],

Visto el Acuerdo EEE, y en particular su anexo XI y su protocolo 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[2],

Vistos los artículos 12 y 22 de su Reglamento interno,

HA APROBADO EL SIGUIENTE DICTAMEN

1 INTRODUCCIÓN

1.1 Marco de protección de datos de los Estados Unidos

1. Los Estados Unidos («EE. UU.») y la Unión Europea («UE») tienen distintos planteamientos en materia de protección de la privacidad y protección de los datos. Si bien la protección de la privacidad y la protección de los datos en la UE son derechos fundamentales consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, en los EE. UU. la protección de datos se aborda por lo general desde una perspectiva de protección de los consumidores. En consecuencia, los enfoques normativos son distintos en los EE. UU. y en la UE[3].

2. A diferencia del enfoque integral de la UE adoptado por el RGPD, en los EE. UU. no existe ninguna ley general integral en materia de protección de datos a nivel federal. La protección de la privacidad en los EE. UU. se lleva a cabo principalmente mediante la adopción de un enfoque sectorial y estatal. Por ejemplo, algunos sectores específicos están amparados por leyes concretas, como las siguientes:

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE) (DO L 119 de 4.5.2016, p. 1).
[2] Las referencias a los «Estados miembros» en el presente dictamen deben entenderse como referencias a los «Estados miembros del EEE».
[3] Véase también el proyecto de Decisión de Ejecución de la Comisión Europea con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativa al nivel adecuado de protección de los datos personales en virtud del marco de privacidad de datos UE-EE. UU., publicado el 13 de diciembre de 2022 (en lo sucesivo, el «proyecto de Decisión»), anexo I, sección I.

- *Health Insurance Portability and Accountability Act* (HIPAA, Ley de Transferibilidad y Responsabilidad del Seguro Sanitario)[4]
- *Children's Online Privacy Protection Act* (COPPA, Ley de Protección de la Privacidad Infantil en Internet)[5]
- *Gramm-Leach-Bliley Act* (GLBA, Ley Gramm-Leach-Bliley)[6]

3. En el ámbito del acceso del Gobierno a los datos personales transferidos desde la UE a los EE. UU., se aplica una serie de bases jurídicas, limitaciones y garantías distintas. Los procesos legales para acceder a la información a efectos de aplicación de la legislación se derivan tanto de la Constitución estadounidense directamente (la Enmienda IV), como de las normas estatutarias y procedimentales, o de las directrices y políticas del Departamento de Justicia a escala federal o estatal. El acceso a la información a efectos de seguridad nacional está regulado por varios instrumentos jurídicos y, en particular, por la *Foreign Intelligence Surveillance Act* (FISA, Ley de Vigilancia de Inteligencia Exterior), el *Executive Order* 12333, el *Executive Order* 14086 de reciente adopción y el Reglamento de la Fiscalía General (en lo sucesivo, «Reglamento FG»)[7] por el que se establece un Tribunal de Revisión de la Protección de Datos (en lo sucesivo, «DPRC»).

4. El 13 de diciembre de 2022, la Comisión emitió su proyecto de Decisión de Ejecución de la Comisión con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativa a la adecuación de la protección de los datos personales en virtud del marco de privacidad de datos UE-EE. UU. (en lo sucesivo, «el proyecto de Decisión»), que contiene en su anexo al marco de privacidad de datos UE-EE. UU. (en lo sucesivo, «el MPD»). Por las razones explicadas anteriormente, el proyecto de Decisión no se basa en un marco jurídico federal específico e integral, sino en el MPD.

[4] La *Health Insurance Portability and Accountability Act* (HIPAA) de 1996 es una ley federal estadounidense. En ella se establecen normas de rango nacional para proteger la información sanitaria delicada de los pacientes. El objetivo de la HIPAA es proteger de forma adecuada la información sanitaria de los particulares, permitiendo al mismo tiempo que la información sanitaria fluya para la prestación y promoción de una atención sanitaria de alta calidad. La HIPAA regula la utilización y la comunicación de la información sanitaria por parte de las entidades sujetas a la Regla de privacidad. Asimismo, contiene normas relativas a los derechos de los particulares a entender y controlar la forma en que se utiliza su información sanitaria.
https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] El principal objetivo de la COPPA es dotar a los progenitores del control de la información personal que los operadores de páginas web y de servicios en línea dirigidos a menores (incluidas aplicaciones móviles y dispositivos del IdC, como juguetes inteligentes) o de páginas para el público en general recogen sobre sus hijos menores de trece años. La COPPA exige a estos operadores que notifiquen a los progenitores y obtengan un consentimiento parental verificable. Esto se aplica asimismo a los datos de los menores extranjeros si las páginas web o los servicios se operan en los EE. UU. y están sujetos a la COPPA. Al mismo tiempo, la normativa también se aplica a las páginas web y los servicios radicados en el extranjero si estos están dirigidos a menores en los EE. UU. Véase: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions y proyecto de Decisión, anexo IV, p. 3.

[6] Uno de los objetivos de la *Gramm-Leach-Bliley Act* es proteger la privacidad de los consumidores en el sector financiero. La GLBA exige a las entidades financieras que expliquen a sus clientes sus prácticas de intercambio de información y que creen garantías para proteger la información de los clientes (por ejemplo, para las empresas reguladas por la FTC en virtud de su Regla de salvaguardias). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[7] Decreto de la Fiscalía General n.º 5517-2022, por el que se modifica la normativa del Departamento de Justicia de los EE. UU. conforme a lo autorizado y ordenado por el EO 14086.

5. El MPD funciona del siguiente modo: El Departamento de Comercio de los EE. UU. («el Departamento») publica los principios del marco de privacidad de datos UE-EE. UU. (denominados conjuntamente «los principios») y el anexo I de los principios («anexo I»), en su calidad de autoridad competente para estimular, fomentar y desarrollar el comercio internacional (USC, título 15, artículo 1512)[8].

6. El desarrollo de los «principios» (en lo sucesivo, «los principios del MPD») se llevó a cabo previa consulta con la Comisión Europea (en lo sucesivo, «la Comisión»), la industria y otras partes interesadas con vistas a alcanzar el objetivo de facilitar los intercambios y el comercio entre la UE y los EE. UU.[9], al tiempo que se garantiza que los interesados cuenten con un nivel de protección sustancialmente equivalente al garantizado en la UE.

7. Los principios del MPD se describen como un «componente esencial» del MPD. Por un lado, proporcionan un «mecanismo listo para usar» para las transferencias de datos de la UE a los EE. UU. Por otro lado, los datos personales transferidos de la UE a los EE. UU. se salvaguardan y protegen conforme al Derecho de la Unión.

8. El MPD solo es aplicable a las entidades estadounidenses que se hayan autocertificado de conformidad con los requisitos del marco (en lo sucesivo, «entidades adheridas al MPD»). De momento, esto solo es posible si se hallan bajo la jurisdicción de la Comisión Federal de Comercio (en lo sucesivo, «FTC») o del Departamento de Transporte (en lo sucesivo, «DoT»). En el futuro, otros órganos estatutarios, con competencia para supervisar la aplicación de los principios del MPD, podrían añadirse en un posterior anexo.

9. Los principios del MPD explican que las condiciones del marco son de cumplimiento exigible por parte de i) la FTC en virtud del artículo 5 de la *Federal Trade Commission Act* (Ley FTC, Ley de la Comisión Federal de Comercio) que prohíbe los actos desleales o fraudulentos relacionados con el comercio[10], ii) el DoT en virtud del USC, título 49, artículo 41712, que prohíbe a un transportista o a un agente de venta de billetes recurrir a prácticas desleales o fraudulentas en relación con el transporte aéreo para la venta o el transporte aéreo, o iii) en virtud de otras disposiciones legales o reglamentarias que prohíban dichos actos.

10. En los principios del MPD se señala que ni el RGPD se ve afectado en su aplicación, ni dichos principios limitan las obligaciones existentes en materia de privacidad, aplicadas de otro modo en virtud del Derecho de los Estados Unidos.

1.2 Alcance de la evaluación del CEPD

11. El proyecto de Decisión refleja la evaluación del MPD realizada por la Comisión, que es el resultado de las conversaciones con el Gobierno de los Estados Unidos. Conforme al artículo 70, apartado 1, letra s), del RGPD, se espera que el CEPD facilite un dictamen sobre las constataciones de la Comisión en relación con la adecuación del nivel de protección en un tercer país y, si es necesario, procure hacer propuestas para abordar cualquier problema.

12. El CEPD acoge con satisfacción las actualizaciones realizadas en los principios del MPD[11], que constituirán el marco jurídico vinculante para las entidades adheridas al MPD. Sin embargo, el CEPD

[8] Proyecto de Decisión, anexo I, sección I.
[9] *Ibidem*.
[10] USC, título 15, artículo 45 (a).
[11] Por ejemplo, la aclaración de que los datos codificados son datos personales.

observa que los principios del MPD siguen siendo esencialmente idénticos a los que se recogen en el Escudo de la privacidad[12] [en los que se basaron las revisiones conjuntas anuales del Grupo de Trabajo del artículo 29 (en lo sucesivo, «GT29») y el CEPD]. Los principios del MPD son también, en gran medida, los mismos que se recogen en el proyecto del Escudo de la privacidad en los que el GT29 basó su dictamen de 2016[13] (en lo sucesivo, «Dictamen 01/2016 del GP29»). Por lo que se refiere a los principios del MPD que siguen siendo esencialmente idénticos, el CEPD no considera necesario repetir todos los comentarios ya realizados por el GT29. El CEPD ha decidido centrarse en aspectos específicos que considera que son aún más pertinentes hoy en día, habida cuenta de la evolución del entorno jurídico y tecnológico.

13. Asimismo, de conformidad con la jurisprudencia del TJUE[14], una parte muy importante del análisis abarca el régimen jurídico del acceso por parte del Gobierno a los datos personales transferidos a los EE. UU.

14. En su evaluación, el CEPD tuvo en cuenta el marco de protección de datos europeo aplicable, incluidos los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «la Carta»), que protegen respectivamente el derecho al respeto de la vida privada y familiar, el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva y a un juez imparcial, y el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, «CEDH») que protege el derecho al respeto a la vida privada y familiar. Además de lo anterior, el CEPD consideró los requisitos del RGPD, la jurisprudencia pertinente y el documento relativo a las referencias sobre adecuación adoptado por el CEPD (en lo sucesivo, «Documento relativo a las referencias sobre adecuación con arreglo al RGPD»)[15].

15. El objetivo de este análisis es proporcionar a la Comisión un dictamen sobre la evaluación de la adecuación del nivel de protección de los datos conferido por el MPD. El TJUE ha ampliado el concepto de «nivel de protección adecuado», que ya existía en la Directiva 95/46/CE. Por lo tanto, cabe recordar la norma establecida por el TJUE en sus sentencias Schrems I[16] (que invalida los «principios de puerto seguro») y Schrems II[17] (que invalida el Escudo de la privacidad).

16. En su sentencia Schrems I, el TJUE dictaminó que, aunque el «nivel de protección» en el tercer país debe ser «sustancialmente equivalente» al garantizado en la UE, «los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la

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

[13] Grupo de Trabajo del artículo 29, Dictamen 01/2016 sobre el proyecto de Decisión sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., adoptado el 13 de abril de 2016 (en lo sucesivo, «Dictamen 01/2016 del GT29»).

[14] En particular: Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Maximilian Schrems/Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650, y sentencia del Tribunal de Justicia de 16 de julio de 2020, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559.

[15] Grupo de Trabajo del artículo 29, Documento relativo a las referencias sobre adecuación, WP 254 rev. 01, 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018, refrendado por el CEPD el 25 de mayo de 2018 (en lo sucesivo, «documento relativo a las referencias sobre adecuación con arreglo al RGPD»).

[16] Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Maximilian Schrems/Data Protection Commissioner, C-392/14, ECLI:EU:C:2015:650 (en lo sucesivo, «sentencia del TJUE Schrems I»).

[17] Sentencia del Tribunal de Justicia de 16 de julio de 2020, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559 (en lo sucesivo, «sentencia del TJUE Schrems II»).

Unión»[18]. Por tanto, el objetivo no es reflejar punto por punto la legislación europea, sino establecer los requisitos esenciales y básicos de dicha legislación objeto de examen. Se puede lograr la adecuación a través de una combinación de derechos para los interesados y obligaciones para aquellos que realizan el tratamiento de los datos personales, o que ejercen control sobre dicho tratamiento, y la supervisión por parte de organismos independientes. No obstante, las normas de protección de datos solo resultan efectivas si son exigibles y se siguen en la práctica. Por tanto, se debe tener en cuenta no solo el contenido de las normas aplicables a los datos personales transferidos a un tercer país u organización internacional, sino también el sistema existente para garantizar la efectividad de dichas normas. Unos mecanismos de aplicación eficientes son de vital importancia para la efectividad de las normas de protección de datos[19].

17. En la sentencia Schrems II, el TJUE consideró que las leyes que pueden invocar los servicios de inteligencia estadounidenses para acceder a los datos personales transferidos a los EE. UU. (artículo 702 de la FISA/EO 12333) limitan de manera desproporcionada los derechos consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «la Carta») y, por tanto, no están reguladas conforme a exigencias sustancialmente equivalentes a las requeridas, en el Derecho de la Unión, en el artículo 52, apartado 1, segunda frase, de la Carta[20].

18. Asimismo, el TJUE señaló que el marco jurídico anterior no ofrecía garantías sustancialmente equivalentes a las exigidas en el artículo 47 de la Carta, puesto que el mecanismo del Defensor del Pueblo no podía compensar la falta de protección de datos, por el hecho de que ni la PPD-28 ni la EO 12333 confieren a los ciudadanos no estadounidenses una tutela judicial efectiva[21]. El Defensor del Pueblo carecía de independencia con respecto al poder ejecutivo y no estaba facultado para adoptar decisiones vinculantes con respecto a los servicios de inteligencia estadounidenses[22].

19. El EO 14086, que en general sustituye a la PPD-28, introdujo dos requisitos nuevos en virtud del Derecho estadounidense que se hacen eco de la sentencia del TJUE Schrems II: por un lado, que las actividades de inteligencia de señales solo se realizarán en la medida necesaria para favorecer una prioridad de la inteligencia de señales validada y solo en la medida y del modo en que sean proporcionadas con respecto a dicha prioridad; y, por otro lado, un mecanismo de recurso.

20. En el presente dictamen, el CEPD evalúa especialmente la medida en que el MPD, así como el EO 14086 de reciente adopción abordan de forma efectiva las apreciaciones efectuadas por el TJUE en su sentencia.

1.3 Observaciones generales y preocupaciones

1.3.1 Evaluación del Derecho interno

21. El CEPD entiende que la evaluación contenida en el proyecto de Decisión se refiere a los principios del MPD. No obstante, el CEPD acogería con satisfacción disponer de información sobre el contexto jurídico de los EE. UU. en el que están operando las entidades adheridas al MPD. Esto permitiría comprender mejor la interacción del MPD con el Derecho estadounidense. Por ejemplo, en el anexo

[18] Sentencia del TJUE Schrems I, apartados 73-74.
[19] Documento relativo a las referencias sobre adecuación con arreglo al RGPD, p. 2.
[20] Sentencia del TJUE Schrems II, apartados 184-185.
[21] Sentencia del TJUE Schrems II, apartado 192.
[22] Sentencia del TJUE Schrems II, apartado 195.

I[23] se determina que los principios del MPD no limitan las obligaciones de privacidad, que por lo demás se aplican en virtud del Derecho estadounidense, pero no se describen estas obligaciones.

1.3.2 Compromisos internacionales contraídos por Estados Unidos

22. Con arreglo a lo dispuesto en el artículo 45, apartado 2, letra c), del RGPD y el documento relativo a las referencias sobre adecuación con arreglo al RGPD, al evaluar la adecuación del nivel de protección de un tercer país, la Comisión tendrá en cuenta, entre otras cosas, los compromisos internacionales asumidos por el tercer país, u otras obligaciones que deriven de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales, y el cumplimiento de las citadas obligaciones.

23. Los Estados Unidos son parte de varios acuerdos internacionales que garantizan el derecho a la privacidad, como el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Convención sobre los Derechos de las Personas con Discapacidad (artículo 22) y la Convención sobre los Derechos del Niño (artículo 16). Asimismo, los Estados Unidos, en calidad de miembro de la OCDE, se adhieren al Marco de privacidad de la OCDE, en particular a las directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales. El 14 de diciembre de 2022, los ministros y los altos representantes de los miembros de la OCDE y la Unión Europea adoptaron la Declaración de la OCDE sobre el acceso de los gobiernos a los datos personales en poder de entidades del sector privado. Los Estados Unidos también son parte del Convenio de Budapest sobre la Ciberdelincuencia.

24. Asimismo, son miembros del sistema de normas de privacidad transfronteriza de la Cooperación Económica Asia-Pacífico (en lo sucesivo, «APEC»), que es un régimen de certificación para la privacidad de los datos respaldado por el Gobierno al que las empresas pueden adherirse para demostrar el cumplimiento de las normas de privacidad reconocidas a escala internacional. Estas normas de privacidad han sido aprobadas por los líderes de la APEC.

25. El CEPD también toma nota de la participación de los Estados Unidos en calidad de Estado observador en el trabajo del Comité Consultivo del Convenio n.º 108 del Consejo de Europa.

26. Asimismo, el CEPD toma nota y acoge con satisfacción la participación continua de los órganos estadounidenses en el nuevo formato de 2021 de la «Mesa redonda de las autoridades de protección de datos y privacidad del G7» (en lo sucesivo, «Mesa redonda APDP G7»), que convoca a las autoridades de control de protección de datos y privacidad independientes de los países del G7. En este contexto, han respaldado, por ejemplo, el último comunicado de la Mesa redonda APDP G7[24] adoptado el 8 de septiembre de 2022 en Bonn (Alemania), que se centró en el concepto de «libre circulación de datos con confianza».

1.3.3 Avances en la legislación estadounidense en materia de protección de datos

27. El CEPD toma nota en particular de los avances operados en la legislación en materia de privacidad de datos a nivel estatal en los EE. UU. El CEPD acoge con satisfacción la adopción de leyes de protección

[23] Proyecto de Decisión, anexo I, sección I, última frase.
[24] Mesa redonda de las autoridades de protección de datos y privacidad del G7, «Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces» [Promoción de la libre circulación de datos con confianza e intercambio de conocimientos sobre las perspectivas para los espacios internacionales de datos], 8 de septiembre de 2022, documento en inglés, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

de datos que ya han entrado en vigor o que entrarán en vigor en 2023 en cinco estados (California, Colorado, Connecticut, Virginia y Utah)[25].

28. El CEPD también observa que ya se han puesto en marcha iniciativas correspondientes para la adopción de otras leyes estatales.

29. Asimismo, el CEPD acoge con satisfacción explícitamente los esfuerzos relacionados con la iniciativa bipartita para la creación de una ley de protección de datos federal, la *American Data Privacy and Protection Act* (ADPPA, Ley estadounidense sobre privacidad y protección de datos).

1.3.4 Ámbito de aplicación del proyecto de Decisión

30. Conforme al artículo 1 del proyecto de Decisión, la Comisión concluye que los Estados Unidos garantizan un nivel adecuado de protección para los datos personales transferidos desde la UE a entidades de los Estados Unidos que figuran en la «Lista del marco de privacidad de datos», mantenida y puesta a disposición del público por el Departamento de Comercio de los Estados Unidos (en lo sucesivo, «DoC»), de conformidad con la sección I.3 del anexo I[26].

31. El MPD está disponible para las sociedades sometidas a la jurisdicción de la FTC o del DoT. Cabe señalar que en el futuro podrían añadirse otros órganos estatutarios estadounidenses con facultades similares[27].

1.3.5 Limitaciones a la obligación de adherirse a los principios del MPD

32. La sección I.5 del anexo I dispone que la adhesión a los principios del MPD por parte de las entidades adheridas al MPD puede verse limitada, entre otros, por i) una orden judicial o exigencias de interés público, cumplimiento de la ley[28] o seguridad nacional[29] (incluso cuando una disposición legal o reglamentaria origine conflictos de obligaciones) y por ii) una disposición legal o reglamentaria o por orden judicial que prevea autorizaciones explícitas, siempre que las entidades adheridas al MPD que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios del MPD está limitado en la medida necesaria para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones.

33. Sin disponer de plenos conocimientos sobre la legislación estadounidense a escala tanto federal como estatal, resulta difícil para el CEPD evaluar de forma detallada el ámbito de aplicación de las exenciones establecidas en este apartado. Por tanto, el CEPD recomienda a la Comisión que incluya en el proyecto

[25] *California Consumer Privacy Act* (Ley de California sobre la privacidad de los consumidores) (2018; entrada en vigor el 1 de enero de 2020); *California Privacy Rights Act* (Ley de California sobre los derechos de privacidad) (2020; plenamente operativa el 1 de enero de 2023); *Colorado Privacy Act* (Ley de Colorado sobre privacidad) (2021; entrada en vigor el 1 de julio de 2023); *Connecticut Data Privacy Act* (Ley de Connecticut sobre privacidad de los datos) (2022; entrada en vigor el 1 de julio de 2023); *Virginia Consumer Data Protection Act* (Ley de Virginia sobre protección de los datos de los consumidores) (2021; entrada en vigor el 1 de enero de 2023); *Utah Consumer Privacy Act* (Ley de Utah sobre la privacidad de los consumidores) (2022; entrada en vigor el 31 de diciembre de 2023).

[26] Proyecto de Decisión, Consideraciones finales, artículo 1, p. 57. El CEPD entiende que el proyecto de Decisión no abarcará las transferencias desde entidades radicadas fuera de la UE, pero sujetas al RGPD en virtud del artículo 3, apartado 2, de dicho Reglamento, a entidades certificadas en los EE. UU.

[27] Proyecto de Decisión, anexo I, sección I.2.

[28] Véase la sección 3.1 del presente dictamen para más observaciones sobre el uso de los datos personales cubierto por el MPD UE-EE. UU. a efectos de aplicación de la ley.

[29] Véase la sección 3.2 del presente dictamen para más observaciones sobre el uso de los datos personales cubierto por el MPD UE-EE. UU. a efectos de seguridad nacional.

de Decisión una aclaración sobre el ámbito de aplicación de las exenciones, también sobre las garantías aplicables en virtud de la legislación estadounidense, al objeto de determinar mejor la repercusión de estas exenciones sobre el nivel de protección de los interesados. Asimismo, el CEPD subraya que la Comisión debería ser informada de la aplicación y la adopción de toda disposición legal o reglamentaria que pudiera afectar a la adhesión a los principios del MPD, así como supervisar dicha aplicación y adopción.

1.3.6 Cambios con respecto al Escudo de la privacidad

34. El CEPD acoge con satisfacción el esfuerzo realizado para responder a las exigencias de la sentencia Schrems II. No obstante, el CEPD habría apreciado que también se hubieran abordado otros problemas identificados i) en el Dictamen 01/2016 del GT29, y ii) en las revisiones conjuntas anteriores [30] con ocasión de las negociaciones del MPD.

35. El CEPD observa asimismo que, a pesar de los cambios y las explicaciones adicionales efectuados en relación con los considerandos del proyecto de Decisión, los principios del MPD que las entidades adheridas al MPD deben cumplir siguen siendo esencialmente idénticos a los que se aplicaban en virtud del Escudo de la privacidad.

1.3.7 Falta de claridad en los documentos del MPD

36. El CEPD señala que la estructura de los anexos y su numeración dificulta la localización de la información y su consulta. Esto contribuye a una presentación general compleja del nuevo marco, que compila en sus anexos documentos de valor jurídico diferente y puede dificultar la correcta comprensión de los principios del MPD por parte de los interesados, las entidades adheridas al MPD y las autoridades de protección de datos de la UE (en lo sucesivo, «APD UE»).

37. El CEPD también recalca que la terminología debería utilizarse de forma coherente a lo largo de todo el MPD. Eso es algo que no sucede, por ejemplo, por lo que se refiere a la noción de «tratamiento». De hecho, algunas partes del MPD enumeran ciertos tipos de operaciones de tratamiento de datos, en lugar de usar el término «tratamiento». Esto puede dar lugar a inseguridad jurídica y posibles lagunas en la protección[31].

38. El CEPD acoge con satisfacción la inclusión en el MPD de las definiciones de algunos de los términos utilizados[32]. Sin embargo, esto no ocurre con algunos otros términos esenciales como «agente» o «encargado del tratamiento», que, en opinión del CEPD, merecen una definición clara y específica en el anexo I, sección I.8, del MPD, y sobre los que tanto los EE. UU. como la UE coinciden, a fin de evitar

[30] Revisiones anuales: primera revisión conjunta anual del Escudo de la privacidad UE-EE. UU., WP 255, informe del GT29 adoptado el 28 de noviembre de 2017 (en lo sucesivo, «informe sobre la primera revisión conjunta»); segunda revisión conjunta anual del Escudo de la privacidad UE-EE. UU., informe del CEPD adoptado el 22 de enero de 2019 (en lo sucesivo, «informe sobre la segunda revisión conjunta»); tercera revisión conjunta anual del Escudo de la privacidad UE-EE. UU., informe del CEPD adoptado el 12 de noviembre de 2019 (en lo sucesivo, «informe sobre la tercera revisión conjunta»).

[31] Por ejemplo, i) conforme al texto del proyecto de Decisión, anexo I, sección III.6.(f), los principios del MPD solamente se aplicarían cuando la entidad almacene, utilice o divulgue los datos recibidos (es decir, no en el caso de que tengan lugar otras operaciones cubiertas por el término «tratamiento», como la recogida, el registro, la alteración, la recuperación, la consulta o la supresión) y ii) conforme al proyecto de Decisión, anexo I, sección II.4.(a), la seguridad de los datos solo se impondría para crear, mantener, utilizar o difundir información personal.

[32] Proyecto de Decisión, anexo I, sección I.8.

confusiones en una fase posterior para las entidades adheridas al MPD amparadas en él, las autoridades de control y el público en general.

39. Por lo que se refiere a la cuestión de las diferencias de interpretación en la UE y los EE. UU. en relación con el concepto de datos de recursos humanos (RR. HH.), el CEPD coincide con el informe de la tercera revisión de la Comisión sobre el objetivo de proseguir las conversaciones con las autoridades estadounidenses[33].

2 ASPECTOS GENERALES RELATIVOS A LA PROTECCIÓN DE DATOS

2.1 Principios relativos al contenido

2.1.1 Conceptos

40. Según el documento relativo a las referencias sobre adecuación con arreglo al RGPD, en el marco jurídico del tercer país deben existir conceptos y principios básicos relativos a la protección de datos. Aunque estos no tienen que reflejar punto por punto la terminología del RGPD, sí deben reflejar los conceptos consagrados en la legislación europea en materia de protección de datos y ser coherentes con ellos. Por ejemplo, el RGPD incluye los siguientes conceptos importantes: «datos personales», «tratamiento de datos personales», «responsable del tratamiento», «encargado del tratamiento», «destinatario» y «datos sensibles». El CEPD acoge con satisfacción la inclusión de las definiciones de los términos «datos personales», «tratamiento» y «responsable del tratamiento» en el MPD, como ya ocurría en el Escudo de la privacidad.

41. El CEPD señala que sigue sin estar clara la medida en que los principios del MPD son aplicables a las entidades adheridas al MPD que reciben datos personales de la UE con fines de «mero tratamiento» (denominados «agentes» o «encargados del tratamiento»). El MPD no distingue entre los principios del MPD aplicables a los agentes y los principios del MPD aplicables a los responsables del tratamiento, aunque algunas de las obligaciones contempladas en estos principios no sean adecuadas para los agentes o los encargados del tratamiento. Por ejemplo, los agentes o encargados del tratamiento no deben poder proporcionar a los particulares todos los elementos de la notificación completa exigida por el principio de notificación (por ejemplo, los fines para los que se recoge y utiliza la información personal sobre ellas)[34], ya que los agentes o encargados del tratamiento no pueden determinar por sí solos los medios y los fines del tratamiento[35].

2.1.2 Principio de limitación de la finalidad

42. El documento relativo a las referencias sobre adecuación con arreglo al RGPD, al igual que el propio Reglamento, establece que los datos personales deben tratarse con una finalidad específica y, posteriormente, solo deben utilizarse en la medida en que ello no sea incompatible con la finalidad del tratamiento.

---

[33] Informe de la tercera revisión conjunta, páginas 5, 15-16 y 30. Véase también el documento de trabajo de los servicios de la Comisión que acompaña al documento «Informe de la Comisión al Parlamento Europeo y al Consejo sobre la tercera revisión anual del funcionamiento del Escudo de la privacidad UE-EE. UU.», p. 17-18.

[34] Proyecto de Decisión, anexo I, sección II.1.(a).

[35] Véase también el Dictamen 01/2016 del GT29, p. 16.

43. El principio de integridad de los datos y de limitación de la finalidad establece que una entidad no podrá tratar información personal de manera incompatible con los fines que motivaron su recogida o que el interesado haya aprobado posteriormente[36]. El CEPD señala que, en los principios de notificación, de opción y de integridad de los datos y de limitación de la finalidad se utiliza terminología distinta. Como señala el GT29 y a pesar de la útil aclaración que se incluye en los considerandos del proyecto de Decisión, algunos términos como «finalidades diferentes», «finalidades sustancialmente diferentes» o «un uso que no es compatible con» se utilizan en el MPD sin una definición clara de estos conceptos y podrían generar inseguridad jurídica.

2.1.3 Derechos de acceso, rectificación, supresión y oposición

44. En el MPD, los derechos de acceso, rectificación y supresión de los interesados se abordan mediante el principio de acceso[37].

45. El principio de acceso se mantiene sin cambios con respecto al Escudo de la privacidad. En consecuencia, persisten algunos de los motivos de preocupación expresados en el Dictamen 01/2016 del GT29 que se indican más adelante.

46. Con respecto al derecho de acceso de los interesados, el CEPD considera necesario reiterar que convendría insertar los detalles de la obligación de responder a las solicitudes de los particulares en el texto principal del principio (siguen describiéndose solamente en una nota a pie de página[38]). Asimismo, ha de quedar claro que el acceso debe proporcionarse cuando una entidad adherida al MPD trata información personal, no solo cuando la «almacena»[39]. En opinión del CEPD, la redacción actual podría dar lugar a una interpretación restrictiva del derecho de acceso.

47. En relación con la lista de excepciones al derecho de acceso[40], algunas aún tienden a inclinar la balanza hacia los intereses de las entidades adheridas al MPD. Al CEPD le sigue preocupando que, en esos casos, parece no existir el requisito de tener en cuenta los derechos e intereses del particular[41].

48. Otra excepción, que el GP29[42] considera relacionada con la preocupación anterior y que el CEPD considera demasiado amplia, es la excepción al derecho de acceso a información accesible al público y la información de registros públicos[43]. El CEPD ha reiterado que, conforme al Derecho de la Unión, los interesados siempre deben tener el derecho a acceder a sus datos, con independencia de que estos hayan sido publicados o no. Si las solicitudes de acceso se rechazaran alegando que los datos se obtuvieron de fuentes accesibles al público o de registros públicos, los particulares perderían la capacidad de controlar la exactitud de los datos y de controlar si estos se pusieron legalmente a disposición del público en primera instancia.

49. El CEPD recuerda que el derecho de acceso está consagrado en el artículo 8, apartado 2, de la Carta. Aunque este no es un derecho absoluto, es fundamental para el derecho a la protección de los datos

[36] Proyecto de Decisión, anexo I, sección II.5.
[37] Proyecto de Decisión, anexo I, secciones II.6 y III.8.a.(i).
[38] Proyecto de Decisión, anexo I, sección III.8.a.(i)1. - nota a pie de página 14.
[39] Proyecto de Decisión, anexo I, sección III.8.d(ii).
[40] Proyecto de Decisión, anexo I, sección III.8.e.
[41] Dictamen 01/2016 del GT29, apartado 2.2.5.
[42] Dictamen 01/2016 del GT29, apartado 2.2.9.
[43] Proyecto de Decisión, anexo I, sección III.15.d-e.

personales, puesto que facilita el ejercicio de otros derechos del interesado, como la rectificación y la supresión, y el derecho de oposición[44].

50. Además de los derechos de acceso, cancelación y supresión, los interesados deben tener el derecho de oponerse en cualquier momento, por razones imperiosas y legítimas propias de su situación particular, al tratamiento de sus datos en virtud de las condiciones específicas establecidas en el marco jurídico del tercer país[45].

51. Con el principio de opción, el MPD establece un derecho de oposición (exclusión voluntaria) a la divulgación de información personal a un tercero o a la utilización de información personal para una finalidad sustancialmente distinta[46]. Asimismo, los particulares se benefician del derecho de exclusión voluntaria del uso de su información personal para fines de mercadotecnia directa[47]. Salvo por lo que se refiere al contexto de fines de mercadotecnia directa, no se definen las modalidades para el ejercicio del derecho de oposición, en particular el momento de ejercicio. Por tanto, el CEPD invita a la Comisión a que aclare el modo en que los particulares pueden ejercer su derecho de oposición.

52. Tal y como se indica en el Dictamen 01/2016 del GT29, el CEPD considera que la simple referencia a la existencia de este derecho en la política de privacidad no puede ser suficiente. Debe ofrecerse una oportunidad individualizada de ejercer este derecho, no solo en caso de divulgación o reutilización de la información personal. El CEPD subraya que debe ofrecerse un derecho general de oposición por razones imperiosas o legítimas propias de la situación particular del interesado en el MPD. El CEPD recomienda garantizar dicho derecho de oposición en todo momento, y que dicho derecho no se limite a la utilización de los datos con fines de mercadotecnia directa[48].

53. En relación con los datos de RR. HH., el CEPD aprecia las aclaraciones de la Comisión con respecto a la aplicación de los principios de notificación y de opción en los casos en los que una entidad estadounidense certificada trate de utilizar datos de RR. HH. para fines diferentes no relacionados con los laborales, como las comunicaciones de mercadotecnia[49]. Sin embargo, el CEPD mantiene que el tratamiento ulterior de datos de RR. HH. para fines no relacionados con los laborales se considerará, en la mayoría de los casos, incompatible con la finalidad original, y que el consentimiento rara vez será totalmente libre cuando se otorga en un contexto laboral.

54. El CEPD reitera asimismo las preocupaciones del GT29 en relación con la exención de los principios de notificación y opción para los datos de RR. HH. «en la medida y tiempo necesarios para que no haya perjuicio de los intereses legítimos de la entidad "cuando tome decisiones sobre ascensos, nombramientos y otras decisiones laborales similares"»[50], que al CEPD le parece amplia y vaga[51].

2.1.4 Limitaciones en materia de transferencias ulteriores

55. Las transferencias ulteriores de datos personales por parte del destinatario inicial de la transferencia de datos original solo se permitirán cuando otro destinatario (el destinatario de la transferencia ulterior) también esté sujeto a normas (incluidas normas contractuales) que otorguen un nivel de

[44] Dictamen 01/2016 del GT29, apartado 2.2.5.
[45] Documento relativo a las referencias sobre adecuación con arreglo al RGPD, sección 3.A.8.
[46] Proyecto de Decisión, anexo I, sección II.2.(a).
[47] Proyecto de Decisión, anexo I, sección III.12.(a).
[48] Dictamen 01/2016 del GT29, apartado 2.2.2.
[49] Proyecto de Decisión, anexo I, sección III.9.b.(i), y considerando 15 y nota a pie de página 27.
[50] Proyecto de Decisión, anexo I, sección III.9.b.(iv).
[51] Dictamen 01/2016 del GT29, apartado 2.2.7.

protección adecuado y cumplan las instrucciones pertinentes al tratar los datos en nombre del responsable del tratamiento. El nivel de protección de los particulares cuyos datos se transfieran no debe verse menoscabado por la transferencia ulterior. El destinatario inicial de los datos transferidos desde la UE será responsable de garantizar que se ofrecen garantías adecuadas para las transferencias ulteriores de datos en ausencia de una decisión de adecuación. Estas transferencias ulteriores de datos solo se deben realizar para unos fines limitados y específicos, y siempre que existan fundamentos jurídicos para dicho tratamiento[52].

56. Conforme al principio de responsabilidad de las transferencias ulteriores del MPD, las transferencias ulteriores solo pueden tener lugar con fines limitados y específicos, en virtud de un contrato entre la entidad adherida al MPD y un tercero (o de un acuerdo similar dentro de un grupo de empresas) y únicamente si dicho contrato exige que el tercero proporcione el mismo nivel de protección que el garantizado por los principios del MPD[53].

57. El CEPD desea recordar una vez más las preocupaciones expresadas en el Dictamen 01/2016 del GT29 en relación con la exención de la necesidad de un contrato para las transferencias dentro de un mismo grupo entre los responsables del tratamiento[54]. Por lo que se refiere a los datos de RR. HH., el CEPD aún no entiende la justificación de la exención de la obligación de ejecutar un contrato con un responsable del tratamiento tercero en el caso de las transferencias ulteriores para las «necesidades operativas ocasionales relacionadas con el empleo»[55].

58. Además, el CEPD desea reiterar la petición del GT29[56] de que las entidades adheridas al marco deben evaluar antes de una transferencia ulterior que los requisitos obligatorios de la legislación nacional del tercer país aplicables al destinatario no menoscabarían la continuidad de la protección de los interesados cuyos datos se transfieren[57].

59. El CEPD mantiene que las transferencias ulteriores de datos personales a terceros países podrían generar injerencias en los derechos fundamentales de los particulares e invita a la Comisión a que aclare que las garantías impuestas por el destinatario inicial al importador en el tercer país deben ser efectivas a la luz de la legislación del tercer país, antes de que se produzca una transferencia ulterior en el contexto del MPD[58].

---

[52] Documento relativo a las referencias sobre adecuación con arreglo al RGPD, sección 3.A.9.

[53] Proyecto de Decisión, anexo I, sección II.3.

[54] Proyecto de Decisión, anexo I, sección III.10.b(i), que se refiere a u otros instrumentos intragrupo (por ejemplo, programas de cumplimiento y control) que aparentemente no necesitan ser vinculantes.

[55] Proyecto de Decisión, anexo I, sección III.9.e(i), que se refiere a ejemplos como la cobertura de un seguro.

[56] Dictamen 01/2016 del GT29, apartado 2.2.3, p. 21.

[57] De conformidad con la sentencia Schrems II, el CEPD ha aclarado las obligaciones para los exportadores e importadores de datos en relación con las transferencias ulteriores en una serie de directrices y recomendaciones: véanse las Recomendaciones 01/2020 del CEPD sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE (versión 2.0, adoptadas el 18 de junio de 2021); Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia (adoptadas el 10 de noviembre de 2020); Directrices 04/2021 sobre códigos de conducta como herramienta para las transferencias (versión 2.0, adoptadas el 22 de febrero de 2022); Recomendaciones 1/2022 sobre la solicitud de aprobación y sobre los elementos y los principios que deben incluirse en las normas corporativas vinculantes para los responsables del tratamiento (adoptadas el 14 de noviembre de 2022); Directrices 07/2022 sobre la certificación como herramienta para transferencias (adoptadas previa consulta pública el 14 de febrero de 2023).

[58] Dictamen 01/2016 del GT29, apartado 2.2.3, p. 21.

2.1.5 Decisiones automatizadas y elaboración de perfiles

60. Las decisiones basadas únicamente en el tratamiento automatizado (decisiones individuales automatizadas), incluida la elaboración de perfiles, que producen efectos jurídicos o que afectan considerablemente al interesado, solo se pueden adoptar en determinadas condiciones establecidas en el marco jurídico del tercer país. En el marco europeo, estas condiciones incluyen, por ejemplo, la necesidad de obtener el consentimiento explícito del interesado o la necesidad de dicha decisión para la celebración de un contrato. Si la decisión no cumple las condiciones previstas por el marco jurídico del tercer país, el interesado tendrá derecho a no estar sujeto a ella. En cualquier caso, la legislación del tercer país debe ofrecer las garantías necesarias, incluido el derecho a ser informado sobre las razones específicas que sustentan la decisión y la lógica aplicada, a corregir información inexacta o incompleta, y a impugnar la decisión cuando esta haya sido adoptada sobre unos hechos incorrectos[59].

61. El MPD no proporciona garantías jurídicas específicas cuando los particulares están sujetos a decisiones que producen efectos jurídicos o que les afectan de manera significativa y que se basan únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, solvencia, fiabilidad o conducta.

62. Como ya se observó en el Dictamen 01/2016 del GT29 y en los dictámenes anteriores del CEPD sobre las decisiones de adecuación relativas a Japón y Corea del Sur[60], el CEPD considera que merecen especial atención los rápidos avances experimentados en el ámbito de las decisiones automatizadas y la elaboración de perfiles, que cada vez se realizan más a través de tecnología de IA[61].

63. El CEPD toma nota de los argumentos de la Comisión, según los cuales es improbable que la ausencia de normas específicas sobre las decisiones automatizadas en el MPD afecte al nivel de protección de los datos personales que han sido recogidos en la Unión (puesto que toda decisión basada en un tratamiento automatizado será adoptada normalmente por el responsable del tratamiento de los datos en la Unión que tiene una relación directa con el interesado de que se trate)[62]. Sin embargo, en opinión del CEPD, no se puede descartar la posibilidad de que un responsable del tratamiento radicado en los EE. UU. pudiera utilizar decisiones automatizadas sobre datos transferidos en virtud del proyecto de Decisión (por ejemplo, en el contexto del empleo, para evaluar el rendimiento en el trabajo, seguros, vivienda).

64. El CEPD acoge con satisfacción las referencias de la Comisión a las garantías específicas proporcionadas por la legislación estadounidense pertinente en distintos ámbitos[63]. Sin embargo, para el CEPD, el nivel de protección de los particulares parece variar de acuerdo con las normas sectoriales específicas, de haberlas, que se aplican a la situación de que se trate. Existe el riesgo de que algunas situaciones queden sin cubrir por no entrar en el ámbito de aplicación de los actos mencionados. Además, el contenido de derechos individuales en relación con las decisiones automatizadas se describe de forma diferente en los distintos actos.

---

[59] Documento relativo a las referencias sobre adecuación con arreglo al RGPD, sección 3.B.3.
[60] Dictamen 28/2018 del CEPD sobre el Proyecto de Decisión de Ejecución de la Comisión Europea sobre la protección adecuada de los datos personales en Japón, adoptado el 5 de diciembre de 2018; Dictamen 32/2021 del CEPD sobre el Proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación de la protección de los datos personales en la República de Corea, adoptado el 24 de septiembre de 2021.
[61] Véase, entre otros, el asunto C-634/21, OQ/Land Hesse, SCHUFA Holding y otros (Scoring), Petición de decisión prejudicial (en curso).
[62] Proyecto de Decisión, considerandos 33 y 34.
[63] Proyecto de Decisión, considerando 35.

65. Por consiguiente, el CEPD considera que, para proporcionar garantías suficientes en el MPD, se necesitan normas específicas relativas a las decisiones automatizadas, en concreto el derecho del particular de conocer la lógica subyacente, para impugnar la decisión y obtener intervención humana cuando la decisión le afecte significativamente[64].

2.2 Mecanismos relativos al procedimiento y la ejecución

66. El CEPD observa que el MPD sigue basándose en un sistema de autocertificación, aunque la Comisión se refiere a él como un sistema de «certificación».

67. El CEPD recuerda las mejoras conseguidas en el curso de las pasadas revisiones conjuntas. Por ejemplo, por lo que respecta al papel del DoC, en el proceso de autocertificación (o de su renovación) (...), la supervisión del cumplimiento por las empresas de los principios del MPD (por ejemplo, mediante verificaciones aleatorias o el uso de cuestionarios de cumplimiento) y la detección de declaraciones fraudulentas de participación y la respuesta a ellas (por ejemplo, a través de búsquedas en internet).

68. Al mismo tiempo, el GT29 y el CEPD expresaron su preocupación sobre una cierta falta de supervisión del cumplimiento de los requisitos del Escudo de la privacidad[65]. En particular, el CEPD coincide con las conclusiones de la Comisión después de la tercera revisión anual del Escudo de la privacidad de que, en virtud del Escudo de la privacidad, las verificaciones aleatorias del DoC tendían a limitarse a los requisitos formales (como la falta de respuesta de los puntos de contacto designados o la falta de accesibilidad en línea a la política de privacidad de una empresa)[66]. El CEPD considera cruciales las verificaciones del cumplimiento por lo que se refiere a los requisitos más sustantivos.

69. El CEPD también recuerda la importancia de la supervisión (también del cumplimiento de los requisitos sustantivos) y la ejecución efectiva del MPD. El CEPD supervisará estrechamente este aspecto, incluso en el contexto de las revisiones periódicas.

70. Por lo que respecta a la ejecución, el CEPD toma nota de los compromisos renovados recogidos en las cartas de la FTC[67] y del DoT[68] de priorizar la investigación de las supuestas infracciones del MPD, tomar las medidas de ejecución oportunas contra las entidades que realicen declaraciones de participación fraudulentas o engañosas, supervisar las órdenes de ejecución en relación con las infracciones del MPD y cooperar con las APD de la UE. A este respecto, el CEPD también reconoce que la FTC ha indicado que tiene la intención de seguir centrando sus medidas de ejecución en las infracciones sustantivas del MPD y de investigar (también) por iniciativa propia. El CEPD someterá estos aspectos a una estrecha vigilancia incluso en el contexto de las revisiones periódicas.

2.3 Mecanismos de recurso

[64] Véase también el Informe sobre la tercera revisión conjunta, apartado 76.
[65] Informe sobre la tercera revisión conjunta, apartado 7.
[66] Informe de la Comisión al Parlamento Europeo y al Consejo sobre la tercera revisión anual del funcionamiento del Escudo de la privacidad UE-EE. UU. [23.10.2019, COM(2019) 495 final], p. 4.
[67] Proyecto de Decisión, anexo IV.
[68] Proyecto de Decisión, anexo V.

71. El CEPD acoge con satisfacción la claridad de la presentación en el proyecto de Decisión de las siete vías de recurso ofrecidas a los interesados de la UE en caso de que sus datos personales se traten contraviniendo el MPD[69].

72. Estos mecanismos de recurso se establecen de acuerdo con los requisitos del principio de recurso, aplicación y responsabilidad y del principio complementario del punto 11 «Resolución de litigios y ejecución» establecidos por el DoC, y mencionados en el anexo I del proyecto de Decisión[70].

73. Tal y como señala la Comisión en su proyecto de Decisión, deben reconocerse al interesado recursos administrativos y acciones judiciales que sean efectivos[71]. Esto refleja el requisito del artículo 45, apartado 2, letra a), del RGPD, según el cual, al evaluar la adecuación del nivel de protección en un tercer país, la Comisión debe tener en cuenta, en particular, el reconocimiento de «derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos»[72]. Este requisito también se recuerda en el documento relativo a las referencias sobre adecuación con arreglo al RGPD[73].

74. El CEPD señala que estos mecanismos de recurso son los mismos que figuran en el antiguo Escudo de la privacidad, que habían sido objeto de observaciones por parte del GT29[74].

75. Por lo que se refiere al mecanismo de arbitraje, el CEPD señala que esta opción no está disponible con respecto a las excepciones a los principios del MPD[75] y, por tanto, remite a la observación realizada en el apartado 33.

76. Con respecto a las vías adicionales de recurso judicial disponibles en virtud de la legislación estadounidense, el CEPD apreciaría más detalles sobre la legislación citada[76] y remite al compromiso realizado en el apartado 21.

77. Asimismo, el CEPD acoge con satisfacción la carta de la FTC en la que expresa su intención de trabajar estrechamente con las APD de la UE[77]. El CEPD también acoge con satisfacción la priorización de las reclamaciones por parte de la FTC, aunque puede que esto no garantice al interesado que sus reclamaciones se tramitarán en todos los casos.

78. Por lo que se refiere a la posibilidad, en determinados casos, de que los particulares presenten sus reclamaciones ante una APD de la UE, el CEPD acogería favorablemente más información i) sobre si la posibilidad de las ADP de la UE de asesorar sobre medidas correctoras o compensatorias podría incluir recomendaciones de multas o el uso de competencias de investigación, y ii) en qué medida tendría en cuenta la FTC o el DoT la acción de las APD de la UE como prueba para la medida de ejecución[78].

79. El CEPD someterá a estrecha vigilancia la eficacia de los mecanismos de recurso también en el contexto de las revisiones periódicas.

---

[69] Proyecto de Decisión, considerando 67.
[70] Proyecto de Decisión, anexo I, secciones II.7 y III.11, y anexo I del anexo I.
[71] Proyecto de Decisión, considerando 64.
[72] Véase también el considerando 141 del RGPD que se refiere al artículo 47 de la Carta de los Derechos Fundamentales para el derecho a la tutela judicial efectiva en la UE.
[73] Documento relativo a las referencias sobre adecuación con arreglo al RGPD, p. 8.
[74] Véase en concreto el Dictamen 01/2016 del GT29, apartado 2.2.6, letra a).
[75] Proyecto de Decisión, anexo I del anexo I, A.
[76] Proyecto de Decisión, considerando 85.
[77] Proyecto de Decisión, anexo IV.
[78] Proyecto de Decisión, anexo I, sección III.5.b.(iii).

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

3.1 Acceso y utilización a efectos de control de la aplicación del Derecho penal

3.1.1 El acceso por parte de las autoridades policiales a los datos personales debe basarse en normas claras, precisas y accesibles

80. El CEPD acoge con satisfacción las explicaciones y la información más detallada, en comparación con la Decisión de adecuación anterior, proporcionadas en el proyecto de Decisión con respecto al acceso y la utilización de datos personales por parte de los poderes públicos de los EE. UU. a efectos de control de la aplicación del Derecho penal. El proyecto de Decisión, en su anexo VI, contiene también una carta del Departamento de Justicia de los EE. UU., Sección Penal, que ofrece una breve visión general de las principales herramientas de investigación utilizadas para la obtención de datos comerciales y otra información de registros de empresas en los Estados Unidos a efectos de la aplicación del Derecho penal o en aras del interés público (civil y legislativo), incluidas las limitaciones de acceso que acompañan a estas competencias. Conforme a esta carta, todos los procedimientos legales descritos en ella se utilizan para obtener información de empresas de los Estados Unidos, independientemente de la nacionalidad o el lugar de residencia del interesado y se derivan bien de la Constitución estadounidense directamente (la Enmienda IV), bien de las normas estatutarias y procedimentales, o bien de las directrices y políticas del Departamento de Justicia. Esta visión general no describe las herramientas de investigación de la seguridad nacional utilizadas por los organismos con funciones coercitivas en investigaciones sobre terrorismo y otras investigaciones de seguridad nacional[79].

81. El CEPD observa que el proyecto de Decisión y su anexo VI examinan principalmente la aplicación de la ley federal y las autoridades reguladoras[80] y no se refieren de manera específica a los textos legislativos estatales en los que se establecen estos procedimientos para obtener información. En el anexo VI también se menciona que existen otras bases jurídicas para que las sociedades puedan impugnar las solicitudes de datos de los órganos administrativos sobre la base de sus sectores concretos y de los tipos de datos que posean, ofreciendo además varios ejemplos no exhaustivos, como la *Bank Secrecy Act* (Ley de secreto bancario) y sus normativas para la implantación[81], la *Fair Credit Reporting Act* (Ley de informes de crédito justos)[82] y la *Right to Financial Privacy Act* (Ley del derecho a la privacidad financiera)[83]. El CEPD observa que las bases jurídicas aplicables a una solicitud de acceso determinada dependen de la naturaleza de los datos solicitados, la naturaleza de los procedimientos legales (penales, administrativos, relacionados con el interés público) y la naturaleza de la entidad que solicita el acceso. Puesto que todas las normas aplicables para limitar el acceso a los datos transferidos a los EE. UU. por parte de las autoridades policiales se basan en la Constitución, en el Derecho común y en políticas transparentes del Departamento de Justicia, el CEPD reconoce la accesibilidad de estas normas e invita a la Comisión a que refleje este elemento en el proyecto de Decisión. Conforme al anexo VI, estos textos legislativos se aplican independientemente de la

[79] Proyecto de Decisión, nota a pie de página 1 del anexo VI.
[80] Véase el proyecto de Decisión, considerandos 90 a 93.
[81] USC, título 31, artículo 5318; CFR, título 31, capítulo X
[82] USC, título 15, artículo 1681b
[83] USC, título 12, artículos 3401-3423.

nacionalidad o el lugar de residencia del interesado y, por lo general, incorporan los requisitos de la Enmienda IV (aunque suelen ir más allá e incluir también protecciones adicionales).

82. En conclusión, el CEPD toma nota de la evaluación más detallada que contiene el proyecto de Decisión en comparación con la Decisión de adecuación anterior por lo que se refiere al acceso por parte de las autoridades policiales federales. Por lo que se refiere al acceso por parte de las autoridades policiales estatales, el CEPD también toma nota de que, conforme al anexo VI, la protección conferida por la legislación nacional debe ser, como mínimo, igual que la que confiere la Constitución estadounidense, con inclusión de la Enmienda IV, entre otros. El CEPD invita la Comisión a que siga evaluando el elemento de protección de la legislación estatal en revisiones futuras.

3.1.2 Se deben demostrar la necesidad y la proporcionalidad respecto a los objetivos legítimos perseguidos

83. El CEPD señala que la solicitud de acceso a los datos a efectos de aplicación de la ley puede, en general, considerarse perseguir un objetivo legítimo. Sin embargo, al mismo tiempo, dichas injerencias solo son aceptables cuando son necesarias y proporcionadas[84].

84. Según la jurisprudencia reiterada del TJUE, el principio de proporcionalidad exige que las medidas legislativas que incorporen injerencias en los derechos a la vida privada y a la protección de datos personales «sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos»[85]. Por tanto, la evaluación de necesidad y proporcionalidad siempre se realiza, en principio, en relación con una medida específica prevista en la legislación.

85. Las autoridades estadounidenses especifican en el anexo VI que los fiscales federales y los agentes de investigación federales pueden acceder a documentos y otra información de registros de empresas estadounidenses utilizando varios tipos de procesos jurídicos vinculantes, entre ellos citaciones para comparecer ante un gran jurado, citaciones administrativas y órdenes de investigación, y podrán obtener otras comunicaciones gracias a las competencias penales federales relativas al registro de llamadas y las escuchas telefónicas[86]. Además, los organismos con responsabilidades civiles y reglamentarias podrán expedir requerimientos a las entidades para la obtención de registros comerciales, información almacenada electrónicamente u otros elementos tangibles[87]. Los propios procesos también se explican en los considerandos 90-93 del proyecto de Decisión. El CEPD toma nota,

[84] Véase la sentencia del Tribunal de Justicia de 6 de octubre de 2020, La Quadrature du Net y otros, asuntos acumulados C-511/18, C-512/18 y C-520/18, ECLI:EU:C:2020:791 (en lo sucesivo, «sentencia del TJUE La Quadrature du Net»), apartado 140. Véanse asimismo los documentos del SEPD, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit [Determinación de la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales: un conjunto de herramientas], 11 de abril de 2017, y Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data [Directrices del SEPD sobre la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la vida privada y a la protección de los datos personales], 19 de diciembre de 2019.

[85] Véase la sentencia del Tribunal de Justicia de 8 de abril de 2014, en los asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 (en lo sucesivo, «Sentencia del TJUE Digital Rights Ireland»), apartado 46 y la jurisprudencia allí citada.

[86] Proyecto de Decisión, anexo VI, p. 2.

[87] Proyecto de Decisión, anexo VI, p. 4.

a este respecto, de un avance positivo mencionado en el proyecto de Decisión en la jurisprudencia estadounidense en relación con la información almacenada de forma electrónica[88].

86. Asimismo, el anexo VI especifica que estos procedimientos legales son no discriminatorios y de uso generalizado para obtener información de las empresas en los EE. UU., con independencia de si están o no certificadas dentro del marco de privacidad de datos UE-EE. UU. e independientemente de la nacionalidad o el lugar de residencia del interesado.

87. Además, el anexo VI contiene conclusiones sobre las garantías previstas en la Enmienda IV de la Constitución de los Estados Unidos que dispone que los registros e incautaciones por parte de las fuerzas y cuerpos de seguridad requieren ante todo un mandamiento judicial por indicios razonables y requisitos de particularidad, y se refiere al hecho de que en las excepciones específicas previstas en las que no es necesario obtener dicho mandamiento, la adopción de medidas coercitivas queda supeditada a una prueba de «razonabilidad» en virtud de la Enmienda IV[89]. Una persona afectada por un registro o cuya propiedad está sujeta a un registro, puede intentar suprimir pruebas obtenidas en un registro ilegal o derivadas de este, si dichas pruebas se presentan contra dicha persona durante un juicio penal[90].

88. En conclusión, el CEPD observa que el sistema de herramientas de investigación utilizado para obtener datos comerciales y otra información de registros de empresas de los Estados Unidos a efectos de control de la aplicación del Derecho penal o en aras del interés público, incluidas las limitaciones de acceso y las garantías, constituye un sistema completo, pero también complejo, de medidas que reflejan, entre otras cosas, el carácter federal del Gobierno estadounidense.

89. Por tanto, podría considerarse que el sistema de medidas de investigación a efectos de aplicación de la ley en los EE. UU. cumple en general los requisitos de necesidad y proporcionalidad en relación con los derechos fundamentales a la vida privada y la protección de datos.

3.1.3 Debe existir un mecanismo de supervisión independiente

90. El CEPD señala el hecho de que la mayoría de los procedimientos descritos en el proyecto de Decisión y el anexo VI presuponen la existencia de una resolución de un órgano jurisdiccional antes de obtener el acceso a los datos [p. ej., órdenes judiciales para identificación y registro de llamadas entrantes y salientes[91], órdenes judiciales para la vigilancia de conformidad con la *Federal Wiretap Law* (Ley Federal de escuchas telefónicas)[92], órdenes de registro en virtud de la norma 41 de las normas federales de enjuiciamiento criminal[93]]. Sin embargo, parece que no todos ellos requieren la participación *a priori* de un órgano jurisdiccional. Por ejemplo, las autoridades civiles y reglamentarias podrán expedir requerimientos[94]. Sin embargo, en estos casos, existe la posibilidad de un control

[88] Véase el proyecto de Decisión, nota a pie de página 146. En una sentencia de 2018, el Tribunal Supremo de los Estados Unidos ratificó que las autoridades policiales también necesitan una orden de registro o una excepción a tal orden para acceder a registros de localizaciones que proporcionan una visión general completa de los movimientos de un usuario y que el usuario puede tener una expectativa razonable de privacidad con respecto a dicha información (Timothy Ivory Carpenter v. United States of America, n.º 16-402, 585 U.S. 2018).
[89] Véase el proyecto de Decisión, anexo VI, p. 2.
[90] Véase el proyecto de Decisión, considerando 90.
[91] Véase el proyecto de Decisión, considerando 92.
[92] Véase el proyecto de Decisión, anexo VI, p. 3.
[93] Véase el proyecto de Decisión, considerando 90, y el anexo VI, p. 3.
[94] Véase el proyecto de Decisión, anexo VI, p. 4, así como el considerando 91.

judicial *a posteriori* de la razonabilidad del requerimiento, ya que el destinatario de un requerimiento administrativo podrá impugnar la aplicación de un requerimiento ante el tribunal[95].

91. Asimismo, el proyecto de Decisión describe la supervisión de las fuerzas y cuerpos de seguridad federales por parte de varios organismos, desde el control interno por parte de los agentes responsables de la protección de la privacidad y de las libertades civiles hasta el control externo llevado a cabo por el inspector general y comisiones específicas en el Congreso de los Estados Unidos[96]. La Comisión Europea proporciona información matizada y detallada, y por lo general llega a conclusiones comprensibles. Por consiguiente, el CEPD se abstiene de reproducir en el presente dictamen las apreciaciones y evaluaciones de los hechos.

92. Sobre la base de la información disponible, el CEPD observa que, con respecto al acceso por parte de las autoridades policiales a los datos que obran en poder de las empresas de los Estados Unidos, existe un mecanismo de supervisión independiente bastante sólido.

3.1.4 Los particulares deben disponer de vías de recurso efectivas

93. Conforme a la jurisprudencia del TJUE, los particulares tienen derecho a la tutela judicial efectiva para satisfacer sus derechos cuando consideren que estos no se han respetado. El TJUE explicó en la sentencia Schrems I que «una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta. En efecto, el artículo 47, párrafo primero, de esta establece que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva, respetando las condiciones establecidas en dicho artículo»[97].

94. El proyecto de Decisión[98] y su anexo VI contienen más información sobre las posibles vías de recurso que se derivan del Derecho común, que estarían disponibles para los particulares cuando los poderes públicos obtengan acceso a sus datos de manera ilícita.

95. A este respecto, según la Comisión[99], el USC, título 5, artículo 702 [*Administrative Procedure Act* (APA, Ley de Procedimiento Administrativo)], establece que toda persona que sufra un perjuicio a causa de actuaciones de una agencia o que se haya visto adversamente afectada o perjudicada por la acción de una agencia, tiene derecho a interponer un recurso judicial.

96. Asimismo, la *Stored Communications Act* (SCA, Ley sobre Comunicaciones Almacenadas) [promulgada como título II de la *Electronic Communications Privacy Act* (Ley de Privacidad de las Comunicaciones Electrónicas)] establece que una persona agraviada por una infracción de dicho capítulo en la que la conducta que constituye la infracción se lleva a cabo a sabiendas o intencionadamente puede, en un procedimiento civil, obtener de la persona o entidad, aparte de los Estados Unidos, que cometió tal infracción la reparación que se considere adecuada[100]. Asimismo, toda persona agraviada por una infracción deliberada de dicho capítulo o del capítulo 119 podrá emprender acciones en el Tribunal de

[95] Véase el proyecto de Decisión, anexo VI, p. 4, así como el considerando 91.
[96] Véase el proyecto de Decisión, considerandos 103 a 106.
[97] Sentencia del TJUE Schrems I, apartado 95.
[98] Véase el proyecto de Decisión, considerandos 107 a 112.
[99] Véase el proyecto de Decisión, considerando 109.
[100] USC, título 18, artículo 2707.

Distrito de Estados Unidos contra los Estados Unidos para obtener una indemnización por daños y perjuicios económicos[101].

97. Asimismo, el proyecto de Decisión también contiene información sobre el derecho a obtener acceso a los registros de las agencias federales en virtud de la *Freedom of Information Act* (FOIA, Ley de Libertad de Información)[102] y otros textos legislativos que confieren a los particulares el derecho a iniciar acciones contra una autoridad o un funcionario público estadounidense con respecto al tratamiento de sus datos personales, como la *Wiretap Act* (Ley de Escuchas), la *Computer Fraud and Abuse Act* (Ley de Abuso y Fraude Informático), la *Federal Torts Claim Act* (Ley Federal de Responsabilidad Extracontractual), la *Right to Financial Privacy Act* (Ley sobre el Derecho a la Privacidad Financiera) y la *Fair Credit Reporting Act* (Ley de Informes de Crédito Justos)[103].

98. El CEPD, por tanto, acoge con satisfacción las aclaraciones proporcionadas por la Comisión por lo que se refiere al número de vías judiciales de recurso a las que los particulares pueden recurrir. El CEPD también invita a la Comisión a que aclare si estas vías de recurso prevén la posibilidad de que el interesado ejerza acciones «para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión», tal y como exige el TJUE.

3.1.5 Utilización ulterior de la información recogida

3.1.5.1 Utilización ulterior de los datos transferidos a los que accedan las autoridades policiales dentro de los Estados Unidos

99. El CEPD observa con satisfacción que el proyecto de Decisión evalúa la utilización ulterior de los datos a los que accedan las autoridades policiales dentro de los Estados Unidos. Sin embargo, el CEPD lamenta que solo se ofrezca un ejemplo de los motivos por los que la información puede seguir divulgándose[104]. A ese respecto, el CEPD recomienda a la Comisión que en el proyecto de Decisión incluya más aclaraciones sobre los principios y las garantías aplicables a la utilización ulterior de los datos, como los incluidos en la *Privacy Act* (Ley de Privacidad) (USC, título 5, artículo 552a)[105].

3.1.5.2 Transferencias ulteriores fuera de los Estados Unidos

100. El CEPD toma nota asimismo de que la Comisión Europea también se ha referido a las transferencias ulteriores por parte de las autoridades policiales de los Estados Unidos a autoridades en terceros países, pero nuevamente solo con respecto a las Directrices del Fiscal General para las operaciones nacionales del FBI AGG-DOM[106]. El CEPD considera que dicha información y evaluación son esenciales para permitir una revisión exhaustiva del nivel de protección que confiere el marco legislativo y las prácticas de los Estados Unidos en relación con la divulgación internacional de datos y el uso ulterior de los mismos. Dado que la Comisión solamente ha ofrecido un ejemplo limitado en relación con el asunto de las transferencias ulteriores fuera de los Estados Unidos en su conjunto, el CEPD invita a la Comisión a que aclare las normas y garantías aplicables a las transferencias ulteriores, el uso ulterior y

[101] USC, título 18, artículo 2712.
[102] Véase el proyecto de Decisión, considerando 111.
[103] Véase el proyecto de Decisión, considerando 112.
[104] Véase el proyecto de Decisión, considerando 102.
[105] Véanse las Directrices del Fiscal General para las operaciones nacionales del FBI (AGG-DOM), página 36, p. B (1)(g).
[106] Véase el proyecto de Decisión, considerando 102.

la divulgación de información personal recogida a efectos de aplicación de la ley en los Estados Unidos y transferida ulteriormente a terceros países, incluso a través de acuerdos internacionales.

3.2 Acceso y utilización a efectos de seguridad nacional

101. Como observación general, el CEPD reconoce que a los Estados se les concede un amplio margen de apreciación en materia de seguridad nacional, algo que también reconoce el TEDH. El CEPD recuerda además que, como se subraya en sus recomendaciones actualizadas sobre las garantías esenciales europeas para medidas de vigilancia[107], el artículo 6, apartado 3, del Tratado de la Unión Europea establece que los derechos fundamentales consagrados en el CEDH constituyen principios generales del Derecho de la Unión. Sin embargo, como recuerda el TJUE en su jurisprudencia, dicho Convenio no constituye, en la medida en que la Unión Europea no lo haya suscrito, un instrumento jurídico incorporado formalmente al Derecho de la Unión[108]. De tal manera, el nivel de protección de los derechos fundamentales exigido por el artículo 45 del RGPD debe determinarse en función de las disposiciones de dicho Reglamento, leído a la luz de los derechos fundamentales consagrados en la Carta de la UE. Dicho esto, de acuerdo con el artículo 52, apartado 3, de la Carta de la UE, los derechos que figuran en ella y se corresponden con derechos que garantiza el CEDH deben tener el mismo significado y alcance que los dispuestos en dicho Convenio. En consecuencia, como ha recordado el TJUE, la jurisprudencia del TEDH sobre derechos que están también previstos en la Carta de la Unión Europea se ha de tener en cuenta como umbral mínimo de protección para interpretar los derechos correspondientes en la Carta de la UE[109]. Sin embargo, con arreglo a la última frase del artículo 52, apartado 3, de la Carta de la UE «[e]sta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa».

102. Por lo tanto, en la siguiente evaluación, el CEPD ha tenido en cuenta la jurisprudencia del TEDH, en la medida en que la Carta de la UE, tal como la interpreta el TJUE, no prevé un nivel de protección superior que prescribe otros requisitos distintos de la jurisprudencia del TEDH.

103. Varios instrumentos jurídicos establecen la posibilidad de recoger, acceder ulteriormente y tratar datos para las agencias de inteligencia de los EE. UU. en el marco jurídico estadounidense.

104. Tal y como recuerda la Comisión Europea en su proyecto de Decisión, las agencias de inteligencia estadounidenses pueden solicitar acceso a los datos personales que se han transferido a organizaciones situadas en los Estados Unidos a efectos de seguridad nacional únicamente si está autorizado por ley, en concreto por la *Foreign Intelligence Surveillance Act* (FISA, Ley de Vigilancia de Inteligencia Exterior) o por disposiciones reglamentarias que autorizan el acceso a través de Cartas de Seguridad Nacional[110]. Las agencias de inteligencia estadounidenses también pueden recoger datos personales fuera de los Estados Unidos, lo que puede abarcar datos personales en tránsito entre la Unión y los Estados Unidos, en virtud del *Executive Order* 12333 (EO 12333)[111].

105. Con respecto a los regímenes específicos de recogida de datos, en particular el artículo 702 de la FISA y el EO 12333, el EO 14086 establece ahora nuevas normas para mejorar las garantías para las actividades de inteligencia de señales de los Estados Unidos. Estas normas se aplican de manera

[107] Véanse las Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia.
[108] Véase la sentencia del TJUE Schrems II, apartado 98.
[109] Véase la sentencia del TJUE La Quadrature du Net, apartado 124.
[110] Véase el proyecto de Decisión, considerando 115.
[111] Véase el proyecto de Decisión, considerando 117.

horizontal y deben seguirse aplicando a través de una serie de normas y procedimientos institucionales que incorporan los principios generales a las instrucciones específicas aplicables a las operaciones cotidianas[112]. El EO 14086 ha sido en gran parte sustituido por la *Presidential Policy Directive 28* (Directiva de Política Presidencial 28) (en lo sucesivo «PPD-28»)[113].

106. Al objeto de evaluar el marco jurídico que se aplica a la recogida, el acceso y el tratamiento ulterior de los datos a efectos de seguridad nacional, es importante examinar el marco jurídico específico que regula la recogida de datos dentro y fuera de los Estados Unidos, es decir, el artículo 702 de la FISA y el EO 12333, que no han cambiado desde la revisión anterior del Escudo de la privacidad, teniendo en cuenta el hecho de que el nuevo EO 14086 establece la aplicación de garantías también en el contexto de la recogida de datos sobre la base de textos concretos como el artículo 702 de la FISA y el EO 12333.

3.2.1 Garantía A - El tratamiento debe efectuarse con arreglo a la legislación y basarse en normas claras, precisas y accesibles

107. Para esta evaluación del contexto general de la recogida de datos a efectos de seguridad nacional, el CEPD desea recordar la primera de las cuatro «garantías esenciales europeas», según la cual «el tratamiento debe basarse en normas claras, precisas y accesibles»[114].

108. Según la jurisprudencia reiterada del TJUE, cualquier limitación del derecho a la protección de los datos personales debe ser establecida por la ley, y la base legal que permite la injerencia en dicho derecho debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate[115]. El Tribunal recordó que «[d]icha normativa debe ser legalmente imperativa en Derecho interno»[116]. A este respecto, la jurisprudencia del TEDH aclara que el término «ley» debe entenderse en su acepción material y no en su acepción formal. Puede abarcar tanto los textos de rango inferior al rango legislativo, como actos reglamentarios adoptados por un colegio profesional, por delegación del Parlamento, en el marco de sus facultades normativas autónomas, y el «derecho no escrito». Para ser «ley», una norma debe ser, como mínimo, suficientemente accesible y estar formulada con precisión suficiente[117].

109. El grado de precisión exigido debe medirse en relación con la medida de la limitación del derecho[118]. Asimismo, en relación con la «previsibilidad» de la ley, el TEDH recordó en la sentencia Zakharov que, en el contexto de las medidas de vigilancia secretas, «la exigencia de previsibilidad no puede significar que se deba permitir a un individuo que prevea si sus comunicaciones corren el riesgo de ser

[112] Véase el proyecto de Decisión, considerando 120.
[113] Este EO revoca la PPD-28, salvo por lo que se refiere a los artículos 3 y 6 de dicha Directiva y el anexo clasificado de esta, que permanecen en vigor. Véase el memorando presidencial sobre seguridad nacional de 7 de octubre de 2022.
[114] Recomendaciones 02/2020 del CEPD sobre las garantías esenciales europeas para medidas de vigilancia, adoptadas el 10 de noviembre de 2020. Véanse los apartados 175 y 180 de la sentencia del TJUE Schrems II y el Dictamen 1/15 (Acuerdo PNR UE-Canadá) de 26 de julio de 2017, apartado 139 y jurisprudencia citada.
[115] Véase la sentencia del TJUE Schrems II, apartados 174-175 y la jurisprudencia citada. Véanse también, con respecto al acceso por parte de los poderes públicos de los Estados miembros, el asunto C-623/17, Privacy International, ECLI:EU:C:2020:790 (en lo sucesivo, «sentencia del TJUE Privacy International»), apartado 65; y la sentencia del TJUE La Quadrature du Net, apartado 175.
[116] Sentencia del TJUE Privacy International, apartado 68.
[117] Sentencia del TEDH de 26 de abril de 1979, Sunday Times c. Reino Unido (n.º 1) (CE:ECHR:1979:0426JUD000653874) (en lo sucesivo, «sentencia del TEDH Sunday Times c. Reino Unido n.º 1»), apartado 49.
[118] Sentencia del TEDH Sunday Times c. Reino Unido n.º 1, apartado 49.

interceptadas por las autoridades y cuándo puede suceder esto, para que pueda regular su conducta en consecuencia». Sin embargo, conviene establecer normas claras y detalladas para prevenir los riesgos de arbitrariedad cuando una facultad conferida en el ejecutivo se ejerza en secreto. El Derecho interno debe ser lo bastante claro para indicar a los ciudadanos de forma suficiente en qué circunstancias y en qué condiciones habilita a los poderes públicos a recurrir a tales medidas[119].

110. Además, el TJUE aclaró que la evaluación de la legislación de terceros países aplicable debe centrarse en si los particulares pueden invocarla ante un órgano jurisdiccional. Los derechos conferidos a los interesados deben ser exigibles y los particulares deben disponer de derechos exigibles frente a los poderes públicos[120], lo que no ocurría en el contexto de la anterior PPD-28. El EO 14086, que, al entender del CEPD, tiene el mismo efecto jurídico que la PPD-28 dentro del ordenamiento jurídico de los Estados Unidos (es decir, vinculante para el ejecutivo), ahora establece derechos exigibles frente a los poderes públicos. En la sección sobre recurso se ofrece una evaluación detallada de los nuevos derechos exigibles de los interesados.

111. En los considerandos 114-152 del proyecto de Decisión y el anexo VII se ofrece un resumen de algunos aspectos del marco jurídico vigente, las limitaciones a la recogida, las limitaciones a la conservación y la divulgación, el cumplimiento y la supervisión, la transparencia y el recurso. El sistema jurídico estadounidense para las actividades de inteligencia consta de una serie de documentos, entre los que se incluyen informes, políticas y procedimientos de agencias individuales. A este respecto, la evaluación del CEPD se centra en un número limitado de cuestiones que considera cruciales.

112. Conforme a los considerandos 115 a 119 del proyecto de Decisión, el acceso a los datos personales transferidos por las autoridades nacionales de seguridad estadounidenses solo puede tener lugar en virtud de la FISA, en virtud de disposiciones estatutarias (USC, título 12, artículo 3414; USC, título 15, artículos 1681u-1681v, y USC, título 18, artículo 2709) o, en relación con los datos personales en tránsito, sobre la base del EO 12333. Se desprende de los considerandos 116 y 118 del proyecto de Decisión que la Comisión centra su evaluación, en relación con el acceso a los datos personales por parte de las autoridades nacionales de seguridad estadounidenses, en los artículos 105, 302, 402, 501 y 702 de la FISA (actividades de inteligencia exterior destinadas a personas que no son ciudadanos estadounidenses ni residen en los EE. UU.) y el EO 12333 (actividades de inteligencia exterior en datos personales en tránsito), por ser los más pertinentes. El dictamen del CEPD se limita, por tanto, a la evaluación de estas disposiciones realizada por la Comisión, teniendo en cuenta las limitaciones y las garantías establecidas en el EO 14086[121].

113. A este respecto, cabe destacar que todos los instrumentos jurídicos mencionados en el proyecto de Decisión son accesibles para el público en general (dentro y fuera de los Estados Unidos) y están disponibles en línea. Además, los requisitos establecidos en el EO son vinculantes para todos los servicios de inteligencia[122] y se aplican de manera transversal a todas las actividades con fines de inteligencia exterior.

114. El concepto de «inteligencia de señales» no se define en el EO 14086. Este último hace referencia a las definiciones que figuran en el EO 12333 para establecer el alcance de la inteligencia exterior y la

[119] Sentencia del TEDH de 4 de diciembre de 2015, Zakharov c. Rusia (en lo sucesivo, «sentencia del TEDH Zakharov»), apartado 229.

[120] Sentencia del TJUE Schrems II, apartado 181.

121 Este EO revoca la PPD-28 salvo por lo que se refiere a los artículos 3 y 6 de dicha Directiva y el anexo clasificado de esta, que permanecen en vigor. Véase el memorando presidencial sobre seguridad nacional de 7 de octubre de 2022.

122 Véase el proyecto de Decisión, considerando 120.

contrainteligencia, que se definen de manera amplia. A este respecto, aunque se ha aducido que desde la introducción de la FISA, el EO 12333 solo puede utilizarse para la recogida de datos fuera del territorio de los Estados Unidos, el CEPD recuerda que el propio EO 12333, que permanece intacto, carece de detalles suficientes en relación con su alcance geográfico, la medida en la que los datos se pueden recoger, conservar o divulgar ulteriormente, o la naturaleza de los delitos que pueden dar lugar a vigilancia o el tipo de información que se puede recoger o utilizar. En principio, toda recogida de datos de inteligencia exterior que entre en el ámbito de aplicación del EO 12333 puede tener lugar a discreción del Presidente de los Estados Unidos[123]. Sin embargo, al entender del CEPD, el objetivo principal del EO 14086 es prescribir los límites para la recogida y el tratamiento de datos personales en el contexto de la inteligencia exterior, independientemente del programa de vigilancia que se utilice y de la procedencia de los datos. Por tanto, el CEPD entiende que las garantías adicionales establecidas en virtud del EO 14086 también se aplican en el contexto de los programas de vigilancia aplicables a los datos personales en tránsito que tienen lugar en el marco del EO 12333[124].

115. A este respecto, el EO 14086 enumera doce objetivos legítimos que deben perseguirse a la hora de realizar la recopilación de inteligencia de señales y cinco objetivos para los que no debe realizarse dicha recopilación[125], así como seis objetivos legítimos para el uso de los datos recopilados en bloque[126]. Si bien algunos de ellos están bastante detallados (como «rescate de rehenes»), otros son más generales (como «seguridad mundial»). El EO 14086 también establece una lista de objetivos prohibidos, que abarca principalmente la supresión o restricción de «intereses legítimos de privacidad»[127]. Asimismo, el EO 14086 también prevé la posibilidad de que el Presidente de los Estados Unidos añada a la lista otros objetivos para los que se permite la recopilación, que podrían, a discreción del Presidente, no divulgarse al público si este considera que hacerlo entrañaría un riesgo para la seguridad nacional de los Estados Unidos[128]. Dichas actualizaciones solo podrán autorizarse «a la luz de nuevos imperativos de seguridad nacional».

116. Los objetivos no pueden, por sí mismos, ser invocados por las agencias de inteligencia para justificar la recopilación de inteligencia de señales, sino que deben documentarse, con fines operativos, en prioridades más concretas. El EO 14086 detalla el procedimiento para la validación de las prioridades para las que puede recopilarse inteligencia de señales[129]. El CEPD entiende que el proceso para definir las prioridades de inteligencia validadas en principio es responsabilidad del director de los Servicios de inteligencia, y reconoce que debe, como norma, implicar la evaluación del responsable de la protección de las libertades civiles de la Oficina del Director de Inteligencia Nacional (CLPO, por sus siglas en inglés), con la que el director puede disentir, en cuyo caso, incluirá la evaluación del CLPO y las opiniones del director a la hora de presentar al Presidente el Marco de Prioridades de Inteligencia Nacional[130].

117. Sin embargo, el CEPD también observa que, conforme a la definición de «prioridad de inteligencia validada», dichas prioridades significan para la mayoría de las actividades de recopilación de

[123] Conforme al artículo II de la Constitución de los Estados Unidos, la responsabilidad de garantizar la seguridad nacional, en particular la recopilación de inteligencia exterior, recae en la autoridad del Presidente como Comandante en Jefe de las Fuerzas Armadas.
[124] Véase el proyecto de Decisión, considerando 134.
[125] Véase el EO 14086, artículo 2(b)(ii)(A)(1) a (5).
[126] Véase el proyecto de Decisión, considerando 134, y el EO 14086, artículo 2(c)(ii).
[127] Véase el EO 14086, artículo 2(b)(ii)(A)(2).
[128] Véase el EO 14086, artículo 2(b)(i)(B).
[129] Véase el proyecto de Decisión, considerando 129.
[130] Véase el EO 14086, artículo 2(b)(iii)(B).

inteligencia de señales de los Estados Unidos[131] una prioridad validada en virtud del artículo 2(b)(iii) del EO (descrita en el apartado anterior). El proceso de validación puede, en algunos casos, diferir de este proceso en «circunstancias limitadas», en cuyo caso, el Presidente o el responsable de un servicio de inteligencia podrá establecer una prioridad «en la medida de lo posible» de conformidad con los criterios establecidos por el mismo artículo 2(b)(iii)(A)(1) - (3), que abarca el requisito de un examen adecuado de la privacidad y las libertadas civiles de todas las personas, pero sin la participación del CLPO.

118. Además, el EO 14086 subraya que las actividades de recopilación de inteligencia de señales se adaptarán lo máximo posible para favorecer una prioridad de inteligencia validada, y que los Servicios de inteligencia considerarán la disponibilidad, la viabilidad y la idoneidad de otras fuentes menos intrusivas y establece los requisitos generales de necesidad y proporcionalidad[132].

119. Asimismo, según el artículo 5(h), el EO 14086 crea un derecho a presentar reclamaciones cualificadas ante el CLPO y a obtener una revisión de las decisiones del CLPO por parte del Tribunal de Revisión de la Protección de Datos de acuerdo con el mecanismo de recurso establecido en el artículo 3 del EO.

120. El texto de la FISA parece ser más claro y preciso que el del EO 12333 por lo que se refiere al tipo de operaciones de inteligencia que se pueden autorizar. La FISA y el EO 12333 deben aplicarse ahora a la luz del EO 14086 y, en particular, teniendo en cuenta entre otras cosas los principios de necesidad y proporcionalidad.

121. Los requisitos establecidos en el EO 14086 se deben seguir aplicando a través de una serie de políticas y procedimientos institucionales que incorporan los principios generales a las instrucciones específicas aplicables a las operaciones cotidianas. A este respecto, el EO 14086 concede a las agencias de inteligencia de los Estados Unidos un máximo de un año para actualizar sus políticas y procedimientos vigentes (es decir, hasta el 7 de octubre de 2023) y armonizarlos con los requisitos del EO. Dichas políticas y procedimientos actualizados deben desarrollarse en consulta con el Fiscal General, el CLPO y el Consejo de Supervisión de la Privacidad y las Libertades Civiles (PCLOB) y ponerse a disposición del público en la máxima medida posible[133].

122. El CEPD acogería con satisfacción que, no solo la entrada en vigor, sino también la adopción de la Decisión, se condicionen a, entre otras cosas, la adopción de unas políticas y procedimientos actualizados para la aplicación del EO 14086 por parte de todas las agencias de inteligencia estadounidenses. El CEPD recomienda a la Comisión que evalúe estas políticas y procedimientos actualizados y comparta su evaluación con el CEPD.

123. Por último, en relación con la conservación de los datos transferidos una vez recogidos a efectos de seguridad nacional, el CEPD observa que el EO 14086 garantiza que las normas aplicables a los datos personales de los ciudadanos estadounidenses también son aplicables a los datos personales de los ciudadanos no estadounidenses[134]. Del proyecto de Decisión se desprende que estas normas se establecen en el artículo 309 de la *Intelligence Authorization Act for Fiscal Year 2015* (Ley de Autorización de Inteligencia del Ejercicio Fiscal 2015)[135], que establece, en principio, un período de conservación máximo de cinco años de las comunicaciones telefónicas o electrónicas no públicas obtenidas sin el consentimiento de la persona. El CEPD recomienda a este respecto que la Comisión

[131] Véase el EO 14086, artículo 4(n).
[132] Véase el EO 14086, artículo 2(c)(i)(A) y (B).
[133] Véase el EO 14086, artículo 2(c)(iv)(B) y (C).
[134] Proyecto de Decisión, considerando 150.
[135] Proyecto de Decisión, nota a pie de página 272.

proporcione mayor claridad en relación con su evaluación de las normas de conservación aplicables a los datos personales de ciudadanos estadounidenses en la Decisión.

3.2.2 Garantía B - Se deben demostrar la necesidad y la proporcionalidad respecto a los objetivos legítimos perseguidos

3.2.2.1 Garantías horizontales proporcionadas por el nuevo EO 14086 - Necesidad y proporcionalidad

124. El nuevo EO 14086 que, en general, sustituye a la PPD-28, tiene por objeto proporcionar normas para mejorar las garantías para las actividades de inteligencia de señales de los Estados Unidos, que serán posteriormente desarrolladas por cada servicio de inteligencia en sus políticas y procedimientos internos.

125. El EO 14086 introduce dos nuevos requisitos en virtud de la legislación estadounidense que se hacen eco de los requisitos recordados por el TJUE en su sentencia Schrems II, a saber, que las actividades de inteligencia de señales deben llevarse a cabo solo cuando sea necesario para favorecer una prioridad de inteligencia validada y solo en la medida y de un modo que sea proporcionado con dicha prioridad[136].

126. El CEPD entiende que estos elementos se han incluido para reflejar los principios de necesidad y proporcionalidad previstos en el Derecho de la Unión y en la jurisprudencia del TJUE y del TEDH, cuya finalidad es garantizar que la recogida y el tratamiento de los datos se limiten a lo que es necesario y proporcionado.

127. A este respecto, el CEPD recuerda el proceso previsto para la validación de las prioridades de inteligencia, así como la posible excepción (véanse los apartados 116 y 117).

128. Asimismo, el CEPD señala que estos principios de necesidad y proporcionalidad previstos en el EO deberán ser puestos en práctica y aplicados, en el plazo de un año, en las políticas y los procedimientos de cada servicio de inteligencia[137].

3.2.2.2 Garantías específicas para la recopilación de inteligencia de señales

129. El CEPD también señala que el EO 14086 establece limitaciones con respecto a los objetivos para los que los datos personales pueden o no pueden recogerse, en el contexto de la recopilación de inteligencia de señales[138].

130. El CEPD acoge con satisfacción el hecho de que el EO establezca que la recopilación selectiva debe priorizarse sobre la recopilación en bloque[139]. En el contexto de la recopilación de inteligencia de señales, el EO establece una lista de doce objetivos para los que los datos se pueden recoger, que deben ser documentados en prioridades de inteligencia (véase el apartado 117), así como una lista de cinco objetivos para los que no podrán realizarse actividades de recopilación de inteligencia de

[136] Véase el EO 14086, artículo 2(a)(ii)(A) y (B).
[137] Véase el EO 14086, artículo 2(c)(iv)(B).
[138] Véase el EO 14086, artículo 2(b)(i)(A)(1) a (12).
[139] Véase el EO 14086, artículo 2(c)(ii)(A).

señales[140]. En principio, estas disposiciones constituyen una garantía que asegura la necesidad de la recogida de los datos.

131. No obstante, el CEPD recuerda que el EO 14086 también prevé la posibilidad de que el Presidente de los Estados Unidos añada otros objetivos a la lista (véanse los apartados 114 y 115)[141].

3.2.2.3 Garantías específicas para la recopilación en bloque

132. El TJUE subrayó en su sentencia Schrems I que la «protección del derecho fundamental al respeto de la vida privada al nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario»[142] y declaró que «se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta».

133. En asunto Schrems II[143], por lo que respecta a su análisis de la recopilación en bloque en relación con la lectura correlativa del EO 12333 y la PPD-28, y en particular los apartados 183 a 185, el Tribunal recalcó, tal y como se ha señalado anteriormente, que la posibilidad de la recopilación en bloque «que permite, en el marco de los programas de vigilancia basados en la E.O. 12333, acceder a datos en tránsito hacia los Estados Unidos sin que dicho acceso sea objeto de ningún control judicial, no regula, en cualquier caso, de manera suficientemente clara y precisa el alcance de la antedicha recopilación en bloque de datos personales ».

134. Por tanto, el CEPD señala que el TJUE no excluyó, por principio, la recopilación en bloque, pero consideró en la sentencia Schrems II que para que dicha recopilación en bloque tenga lugar de manera legal, deben establecerse límites suficientemente claros y precisos para delimitar el alcance de dicha recopilación.

135. El CEPD también reconoce que, al tiempo que sustituye a la PPD-28, el EO 14086 establece nuevas garantías y límites para la recogida y la utilización de los datos recogidos fuera de los Estados Unidos, puesto que las limitaciones de la FISA y otras leyes estadounidenses más específicas no son de aplicación.

136. Con respecto a la recopilación en bloque de datos, el CEPD toma nota de que el EO 14086 prevé que la recopilación en bloque sigue estando permitida. De hecho, el CEPD subraya que la definición de recopilación en bloque sigue siendo la misma que en la PPD-28 anterior, según la cual la recopilación «en bloque» de la inteligencia de señales es una recopilación autorizada de datos que, debido a consideraciones técnicas u operativas, es obtenida sin el uso de discriminantes (por ejemplo, sin el uso de identificadores o criterios de selección específicos)[144].

137. Desde la sentencia Schrems II, el Tribunal no ha detallado con precisión las garantías exigidas para que tenga lugar la recopilación en bloque. Sin embargo, el CEPD recuerda que el TEDH ha adoptado decisiones importantes en relación con la recopilación en bloque y las garantías pertinentes en este contexto.

[140] Véase el EO 14086, artículo 2(b)(ii)(A)(1) a (5).
[141] Véase el EO 14086, artículo 2(b)(i)(B).
[142] Sentencia del TJUE Schrems I, apartado 92.
[143] Véase la sentencia del TJUE Schrems II.
[144] Véase el EO 14086, artículo 4(b).

138. El CEPD recuerda que la recopilación en bloque, que permite la recogida de grandes cantidades de datos sin discriminantes, plantea mayores riesgos para los particulares[145] que la recopilación selectiva y, por tanto, requiere aducir garantías adicionales.

139. El CEPD también observa que el TJUE ha desarrollado jurisprudencia adicional relativa a la conservación de los datos de tráfico y de localización, y el acceso ulterior a estos datos conservados por los operadores del sector de telecomunicaciones, incluso a efectos de seguridad nacional, que, aunque no se pueden considerar directamente aplicables en este contexto, en cierta medida podrían ser pertinentes en el contexto de la presente evaluación de la recopilación en bloque en el contexto del EO 12333.

1) Limitación de la finalidad

140. El EO establece que la recopilación en bloque debe tener lugar solo tras una decisión de que la información necesaria para favorecer una prioridad de inteligencia validada no se puede obtener razonablemente a través de la recopilación selectiva[146], y que el servicio de inteligencia aplicará métodos razonables y medidas técnicas para limitar los datos recogidos a lo estrictamente necesario para favorecer una prioridad de inteligencia validada, reduciendo a su vez al mínimo la recopilación de información no pertinente[147]. Además de estas garantías, el CEPD también reconoce que los datos recopilados en bloque se utilizarán para alcanzar uno o más de los seis objetivos enumerados[148]. El CEPD hace hincapié en que, si bien estos objetivos están más detallados que los que se establecían en la PPD-28 anterior, sustituida en general por el EO 14086, las posibilidades de dicha recopilación siguen siendo potencialmente amplias, es decir, engloban grandes volúmenes de datos.

141. Asimismo, el CEPD recuerda que el EO 14086 también prevé la posibilidad de que el Presidente de los Estados Unidos añada otros objetivos a la lista (véase el apartado 115)[149].

2) Autorización previa independiente

142. El CEPD incide en que el TEDH concede una importancia significativa a la autorización previa independiente en el contexto de la recopilación en bloque de datos a efectos de seguridad nacional. De hecho, el Tribunal declaró que para minimizar el riesgo de que se produzca un abuso de la facultad de interceptación masiva, el Tribunal considera que el proceso debe estar sujeto a «garantías integrales», lo que significa que, a escala nacional, debe hacerse una evaluación en cada etapa del proceso acerca de la necesidad y la proporcionalidad de las medidas adoptadas; que la interceptación masiva debe estar sujeta a autorización independiente desde el principio, cuando se definen el objeto y el alcance de la operación; y que la operación debe estar sujeta a supervisión y control *a posteriori*. En opinión del Tribunal, estas son garantías fundamentales que constituyen la piedra angular de cualquier régimen de interceptación masiva conforme al artículo 8[150].

[145] Véase, por ejemplo, la sentencia del TEDH de 25 de mayo de 2021 (Gran Sala), Big Brother Watch y otros c. Reino Unido (en lo sucesivo, «sentencia del TEDH Big Brother Watch»), considerando 363, donde el Tribunal indica que no está convencido de que la obtención de datos de comunicaciones conexas a través de la interceptación masiva sea necesariamente menos intrusiva que la adquisición de contenido.
[146] EO 14086, artículo 2(c)(ii)(A).
[147] EO 14086, artículo 2(c)(ii)(A).
[148] EO 14086, artículo 2(c)(ii)(B).
[149] Véase el EO 14086, artículo 2(c)(ii)(C).
[150] Véase la sentencia del TEDH Big Brother Watch, apartado 350.

143. El CEPD también toma nota del siguiente apartado de esta sentencia de la Gran Sala, en el que el Tribunal de Estrasburgo pone de relieve que coincide con la Sala en que, si bien la autorización judicial es una garantía importante contra la arbitrariedad no es un requisito necesario (véanse los apartados 318-320 de la sentencia de la Sala). No obstante, la interceptación en bloque debe ser autorizada por un organismo independiente; es decir, un organismo que sea independiente del poder ejecutivo[151].

144. En este contexto, el CEPD observa que el Decreto no prevé dicha autorización previa independiente para la recopilación en bloque, y que esta tampoco se prevé en el EO 12333 (véase el siguiente apartado sobre el EO 12333).

3) <u>Normas de conservación</u>

145. El CEPD recuerda que otro conjunto importante de garantías son las normas sobre la duración de la recogida y conservación de los datos. A este respecto, el TEDH subrayó que el Derecho interno debe fijar un límite a la duración de la interceptación, el procedimiento que debe seguirse para el análisis, la utilización y la conservación de los datos recogidos, las precauciones que se deben adoptar para la comunicación de los datos a otras partes y las circunstancias en las que se puede o se debe proceder a la supresión o destrucción[152], ya que estas garantías son igualmente importantes para la interceptación en bloque[153].

146. A este respecto, el CEPD entiende que el EO proporciona normas relativas a la conservación de datos para los datos personales recogidos a través de inteligencia de señales, incluso en bloque[154]. El CEPD señala que, conforme al artículo 2(c)(iii)(A) del EO 14086, cada servicio de inteligencia que maneja información personal recogida a través de inteligencia de señales establecerá y aplicará políticas y procedimientos diseñados para reducir al mínimo la divulgación y la conservación de dicha información. Sin embargo, estas normas no establecen un período de conservación específico, sino que se refieren en general a las mismas normas que se aplican a la conservación de datos relativos a los ciudadanos estadounidenses y a situaciones en las que no se ha adoptado una decisión firme sobre la conservación. El CEPD está, por tanto, preocupado porque estos períodos de conservación no están claramente definidos en este EO con respecto a los datos recopilados en bloque, a diferencia de lo que ocurre con la recopilación selectiva (véase el apartado 122). Insta a la Comisión a que comparta su evaluación sobre la necesidad y la proporcionalidad de los períodos de conservación aplicables a los ciudadanos estadounidenses y la información disponible en relación con los períodos de conservación en la práctica cuando no se ha adoptado ninguna decisión firme sobre la conservación en virtud de la legislación estadounidense, puesto que en su estado actual, el proyecto de Decisión solamente recuerda esta norma general en un breve apartado[155] y una nota a pie de página[156], lo que no permite determinar si estos períodos de conservación son necesarios y proporcionados. Puesto que, como subraya el TEDH, para los interesados es una garantía crucial poder ejercer sus derechos en un contexto en el que se ha adoptado una medida particularmente intrusiva para recoger sus datos inicialmente, el CEPD insta a la Comisión Europea a que proporcione más aclaraciones en relación con los distintos períodos de conservación en la práctica.

[151] Véase la sentencia del TEDH Big Brother Watch, apartado 351.
[152] Véase la sentencia del TEDH Big Brother Watch, apartado 348.
[153] Véase la sentencia del TEDH Big Brother Watch, apartado 348.
[154] Véase el EO 14086, artículo 2(c)(iii)(A)(2)(a)-(c).
[155] Véase el proyecto de Decisión, apartado 150.
[156] Véase el proyecto de Decisión, nota a pie de página 271.

4) Garantías relativas a la «divulgación»

147. Asimismo, el CEPD recuerda que, para garantizar la efectividad de la necesidad y la proporcionalidad y el principio de limitación de la finalidad, el TEDH también ha reconocido la importancia de las normas dispuestas en la legislación en relación con la divulgación ulterior de los datos recogidos, incluso en el contexto de la recopilación en bloque[157].

148. El artículo 2(c)(iii)(A)(1)(c) del EO 14086 establece que la información sobre ciudadanos no estadounidenses que se recogió a través de inteligencia de señales solo se puede divulgar si una persona autorizada y adecuadamente formada considera que existen indicios razonables de que la información personal se protegerá de forma adecuada y el destinatario necesita conocer la información.

149. Teniendo esto en cuenta, el CEPD entiende que las disposiciones relativas a la divulgación en el marco del EO 14086 no prevén una prohibición expresa de divulgación para fines distintos de los de seguridad nacional por lo que se refiere a la divulgación a las autoridades estadounidenses competentes[158]. El CEPD insta a la Comisión a aclarar las normas y garantías aplicables en este caso.

150. Por tanto, al CEPD le preocupa que los datos obtenidos por los servicios de inteligencia competentes puedan divulgarse a las autoridades estadounidenses competentes a efectos de lucha contra la delincuencia, incluso delitos graves, en el contexto de investigaciones penales, lo que brinda a las autoridades policiales la posibilidad, sin más restricciones específicas, de obtener datos que habrían tenido prohibido recoger directamente e insta a la Comisión a evaluar este punto con mayor profundidad.

151. En el contexto específico de las transferencias ulteriores (divulgación a destinatarios fuera del Gobierno de los Estados Unidos, en particular a un gobierno extranjero o una organización internacional[159]), el CEPD opina que la protección conferida a los datos también debe mantenerse en el contexto de las transferencias ulteriores, incluso en el ámbito de la seguridad nacional[160].

152. A este respecto, el EO establece determinadas garantías, a saber, el requisito de tomar debida cuenta de la finalidad de la divulgación —aunque sin exigir expresamente que la finalidad de la divulgación también sea la protección de la seguridad nacional— la naturaleza y el alcance de la información personal que se divulga y las posibles repercusiones negativas para la persona o personas afectadas antes de divulgar los datos.

153. Aunque el CEPD reconoce que algunas de estas garantías, en particular la obligación de tener en cuenta las posibles repercusiones negativas[161] para los interesados afectados, reflejan algunos requisitos del CEDH, también señala que el Tribunal de Estrasburgo exige además una obligación legalmente vinculante de analizar y determinar si el destinatario extranjero de inteligencia ofrece un nivel mínimo aceptable de garantías[162], que el CEPD no encuentra específicamente en las disposiciones del EO en

[157] Véase la sentencia del TEDH Big Brother Watch, apartado 348.
[158] Véase el EO 14086, artículo 2(c)(iii)(A)(1).
[159] Véase el EO 14086, artículo 2(c)(iii)(A)(1)(d) en particular.
[160] Véase, por ejemplo, el Dictamen 14/2021 sobre el proyecto de Decisión de Ejecución de la Comisión Europea de conformidad con el Reglamento (UE) 2016/679 sobre la protección adecuada de los datos personales en el Reino Unido. Adoptado el 13 de abril de 2021, secciones 4.3.2.1 y 4.3.2.2.
[161] Véase el EO 14086, artículo 2(c)(iii)(A)(1), (d).
[162] Véase la sentencia del TEDH (Gran Sala) de 25 de mayo de 2021, del asunto Centrum För Rättvisa c. Suecia, apartado 326.

relación con la divulgación a destinatarios extranjeros. Por tanto, el CEPD invita a la Comisión a que evalúe este elemento con mayor profundidad.

154. El CEPD señala, además, que, en el marco de su evaluación sobre la adecuación, la Comisión Europea no consideró la existencia de los acuerdos internacionales celebrados con terceros países u organizaciones internacionales que pueden prever disposiciones específicas para la transferencia internacional de datos personales por parte de los servicios de inteligencia a terceros países. El CEPD considera que es probable que la celebración de acuerdos bilaterales y multilaterales con terceros países a efectos de cooperación en materia de inteligencia afecten al marco jurídico de protección de datos evaluado.

155. Por tanto, el CEPD invita a la Comisión Europea a que aclare si dichos acuerdos existen y en qué condiciones se pueden celebrar, y a que evalúe si las disposiciones de los acuerdos internacionales pueden afectar al nivel de protección conferido a los datos personales transferidos desde el EEE por el marco legislativo y las prácticas en relación con trasferencias ulteriores a efectos de seguridad nacional.

5) Recopilación en bloque temporal para respaldar la fase técnica inicial de la recopilación selectiva

156. El CEPD recuerda que, en el contexto de la última revisión conjunta del Escudo de la privacidad, los debates se centraron principalmente en la interpretación y la aplicación del motivo (situación/escenario) adicional para la recopilación en bloque previsto por la primera oración de la nota a pie de página 5 del artículo 2 de la PPD-28, que indicaba que las limitaciones contenidas en ese artículo no se aplicaban a los datos de inteligencia de señales que se obtienen de forma temporal para facilitar la recopilación selectiva. Las autoridades estadounidenses explicaron en su momento el significado de la expresión «datos de inteligencia de señales que se obtienen de forma temporal para facilitar la recopilación selectiva». A raíz de estos debates, el CEPD entendió que esta nota a pie de página significaba que los datos podían recogerse en bloque —y con independencia de las seis finalidades previstas— si ello se hace de forma temporal, con vistas a establecer un identificador para un objetivo definido. Este sería, por tanto, un motivo adicional para recopilar datos en bloque, y en este caso seguirían aplicándose solo los principios generales del artículo 1 de la PPD-28. Como se ha indicado anteriormente, en la sentencia Schrems II, el TJUE consideró que la combinación del EO 12333 y la PPD-28 con respecto a la recopilación en bloque «no regula, en cualquier caso, de manera suficientemente clara y precisa el alcance de la antedicha recopilación en bloque de datos personales»[163].

157. El CEPD observa que el EO 14086 sigue incluyendo una excepción que permite este tipo de recopilación en bloque[164]; sin embargo, el CEPD acoge con satisfacción el hecho de que esta excepción se haya reducido en comparación con la que prevé la PPD-28, y que se hayan incluido garantías adicionales en el EO 14086.

158. El CEPD entiende que el nuevo EO 14086 establece garantías que siguen siendo aplicables en el contexto de este tipo de recopilación en bloque técnica temporal, en particular los principios generales de necesidad y proporcionalidad en relación con la prioridad de inteligencia validada cuando los datos se obtienen sin discriminantes antes de que tenga lugar la recopilación selectiva [artículo 2(a)-(b) y

[163] Sentencia del TJUE Schrems II, apartado 183.

[164] Véanse el EO 14086, artículo 2(c)(ii)(D), y el proyecto de Decisión, nota a pie de página 226.

artículo 2(c)(i) del EO 14086]. El CEPD también entiende que dicha recogida en bloque que respalda una recogida de inteligencia de señales selectiva ulterior también está sujeta a las garantías adicionales previstas a partir de la subsección (2)(c)(iii)[165].

159. Sin embargo, el CEPD también recuerda —véase el apartado 117 anterior— que la definición de «prioridad de inteligencia validada» prevé un procedimiento de excepción que no implicaría a la CLPO de la Oficina del director de Inteligencia Nacional.

160. Sin embargo, el CEPD sigue señalando que las garantías de la subsección relativa a la recopilación en bloque no se aplican a la recopilación en bloque temporal utilizada para respaldar la fase técnica inicial de la recopilación selectiva de inteligencia de señales del modo que se establece en el artículo 2(c)(ii)(D) del EO 14086, lo que significa que, en este contexto, los datos recopilados en bloque se pueden utilizar para otros fines distintos de los previstos en la subsección 2(c)(ii). El CEPD acogería con satisfacción algunas aclaraciones en el proyecto de Decisión sobre las finalidades para las que pueden utilizarse los datos recopilados en bloque en este contexto, así como la aplicación de las limitaciones establecidas en la subsección 2(c)(i) para la recopilación de inteligencia de señales en general (a saber, solo para los objetivos legítimos allí enumerados) en el contexto de la recopilación en bloque temporal.

161. Para concluir, el CEPD también subraya que siguen sin estar claras tanto esta excepción para la recopilación en bloque temporal para respaldar la recopilación selectiva como las garantías restantes que se aplicarán, en particular qué garantías del EO 14086 se aplicarían en qué fase (recopilación en bloque, recopilación selectiva) e insta a la Comisión a que evalúe estos elementos con mayor profundidad y a que analice estos aspectos también en la práctica en futuras revisiones conjuntas.

162. Asimismo, el CEPD considera que, si bien el término «temporalmente» se ha detallado un poco más en el EO que en la PPD-28, al entender del CEPD sigue pareciendo significar que la recopilación en bloque puede continuar hasta que no se identifique el objetivo. A este respecto, el CEPD recuerda la necesidad de disponer de normas claras y precisas, y hace hincapié en la importante garantía que estas normas constituyen para los interesados.

163. En conclusión, con respecto a las garantías aplicables a la recopilación en bloque, al CEPD le sigue preocupando que, a pesar de las garantías adicionales previstas en el EO 14086, sigue brindándose la posibilidad de recoger datos en bloque (es decir, sin discriminantes) sin garantías clave como la autorización previa para recoger estos datos —incluso en la situación de excepción de la recopilación en bloque técnica temporal—, teniendo asimismo en cuenta la necesidad de realizar más aclaraciones y las preocupaciones expresadas con respecto a la limitación estricta de la finalidad para acceder a los datos de forma ulterior, normas claras y estrictas en materia de conservación de datos y garantías más estrictas en relación con la divulgación de los datos recogidos en bloque, incluso en el contexto de las transferencias ulteriores.

164. En general, el CEPD subraya que la sentencia antes citada del TEDH muestra una vez más la importancia de una supervisión completa por parte de las autoridades de control independientes. El CEPD enfatiza que la supervisión independiente en todas las fases del proceso de acceso gubernamental a efectos de seguridad nacional es una garantía importante frente a medidas de vigilancia arbitrarias y, por tanto, para la evaluación de un nivel adecuado de la protección de los datos. El objetivo de la garantía de independencia de las autoridades de control en el sentido del artículo 8, apartado 3, de la Carta es asegurar un control eficaz y fiable del cumplimiento de las normas sobre protección de los particulares en lo que respecta al tratamiento de datos personales. Esto se aplica especialmente en circunstancias

[165] Véanse las secciones anteriores para conocer otros elementos de estas disposiciones.

en las que, debido a la naturaleza secreta de la vigilancia, se priva al particular de la posibilidad de solicitar control o de participar directamente en cualquier procedimiento de control antes o durante la ejecución de la medida de vigilancia.

165. El CEPD recuerda que su opinión es que la evaluación de la adecuación depende de todas las circunstancias del caso, en particular de la eficacia de la supervisión *ex post* y del acceso a vías de recurso según lo previsto en el marco jurídico.

3.2.2.4 Marco jurídico que regula la recopilación selectiva a efectos de seguridad nacional por parte de los servicios de inteligencia dentro y fuera del territorio de los Estados Unidos

166. En su sentencia Schrems II, el TJUE señaló, en relación con el artículo 702 de la FISA que de este texto «en modo alguno se desprende la existencia de limitaciones a la habilitación que dicho artículo otorga para la ejecución de programas de vigilancia con fines de inteligencia exterior ni tampoco la existencia de garantías para las personas no nacionales de los Estados Unidos que sean potencialmente objeto de esos programas»[166]. Esto llevó al Tribunal a considerar que «[e]n estas circunstancias [...] el referido artículo no puede garantizar un nivel de protección sustancialmente equivalente al garantizado por la Carta [...], conforme a la cual una base legal que permita injerencias en los derechos fundamentales, para cumplir el principio de proporcionalidad, debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate y establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas»[167].

167. En relación con el EO 12333, el Tribunal señaló que «tampoco confiere derechos exigibles a las autoridades estadounidenses ante los tribunales»[168] y también concluyó que «en el marco de los programas de vigilancia basados en la E.O. 12333, acceder a datos en tránsito hacia los Estados Unidos sin que dicho acceso sea objeto de ningún control judicial, no regula, en cualquier caso, de manera suficientemente clara y precisa el alcance de la antedicha recopilación en bloque de datos personales»[169], tras el análisis de las condiciones en virtud de las que podría tener lugar la recopilación en bloque conforme a este decreto, junto con la PPD-28.

168. Con respecto a estos regímenes de recopilación selectiva de datos, el EO 14086 establece ahora normas nuevas.

3.2.2.4.1 Recogida de datos a efectos de seguridad nacional en virtud del artículo 702

169. El CEPD recuerda que las apreciaciones sobre el artículo 702 de la FISA[170] de que, en la práctica, los ciudadanos no estadounidenses también se benefician de las restricciones de acceso y conservación impuestas por los procedimientos de minimización o fijación de objetivos de las distintas agencias debido a que el coste y la dificultad de identificar y eliminar información de ciudadanos estadounidenses de un gran conjunto de datos implica que todo el conjunto de datos se maneja de conformidad con las normas estadounidenses en materia de datos más estrictas, fueron muy bien acogidas en el último informe del PCLOB.

170. Conforme a estas apreciaciones, el programa no se aplica mediante la recopilación de comunicaciones en bloque. Los informes estadísticos de transparencia de 2014 y 2021 emitidos por la ODNI

[166] Véase la sentencia del TJUE Schrems II, apartado 180.
[167] Véase la sentencia del TJUE Schrems II, apartado 180.
[168] Véase la sentencia del TJUE Schrems II, apartado 182.
[169] Véase la sentencia del TJUE Schrems II, apartado 183.
[170] Véase el Informe del PCLOB sobre el Programa de Vigilancia aplicado en virtud del artículo 702 de la FISA, página 100.

confirmaron esta apreciación. Además, conforme al informe del PCLOB, se utilizan «selectores asignados», como una dirección de correo electrónico o un número de teléfono, para especificar la vigilancia.

171. No obstante, el CEPD también recuerda que, al mismo tiempo, en el contexto del artículo 702, durante la última revisión del Escudo de la privacidad se aclaró que una «persona» sujeta a identificación como objetivo podía referirse a varios particulares que utilizan el mismo identificador, siempre que todos estos particulares fueran ciudadanos no estadounidenses y cumplieran los criterios aplicables para ser segmentados. Además, el CEPD recuerda que durante la tercera revisión conjunta anual del Escudo de la privacidad realizada en 2019, se solicitó una mayor aclaración en el contexto del programa UPSTREAM para excluir la posibilidad de que se produjera un acceso masivo e indiscriminado a los datos personales de ciudadanos no estadounidenses[171].

172. Asimismo, el CEPD recuerda que, el hecho de que la recogida de datos en virtud del artículo 702 de la FISA se justifique con que uno de sus principales fines sea obtener información de inteligencia exterior, sigue existiendo incertidumbre con respecto a la limitación de la finalidad y la necesidad. El CEPD señala, no obstante, que de acuerdo con el EO 14086, artículo 2(a)(A) y (B), las actividades de inteligencia de señales solo deben llevarse a cabo tras la decisión de que son necesarias para favorecer una prioridad validada y en la medida y de un modo que sea proporcionado con dicha prioridad, y que la recogida debe estar lo más adaptada posible para favorecer la prioridad validada, teniendo en cuenta factores pertinentes como el carácter intrusivo de la recogida y el carácter delicado de los datos, y no debe afectar negativamente a la privacidad y las libertades civiles. El CEPD sigue esperando más aclaraciones sobre el modo concreto en que esto se aplicará y se pondrá en práctica, incluso en el contexto de la aplicación del artículo 702 de la FISA.

173. A este respecto, en ausencia de acceso directo a esta información por sí mismo, el CEPD solicitó una evaluación independiente de la necesidad y proporcionalidad de la definición de «objetivos» y del concepto de «inteligencia exterior» en virtud del artículo 702 de la FISA (incluso en el contexto del programa Upstream) tras su renovación. El CEPD considera que su solicitud anterior de evaluación independiente del proceso de aplicación de selectores en casos específicos («asignación de selectores»), así como de aclaración en el contexto del programa Upstream es pertinente. Por tanto, teniendo en cuenta el nuevo EO 14086, el CEPD solicita información complementaria para evaluar y supervisar también de qué forma y en qué medida estos principios de necesidad y proporcionalidad recientemente introducidos se aplicarán en la práctica en este contexto, y espera que esto también sea evaluado en el contexto de futuras revisiones conjuntas.

174. El CEPD acoge con satisfacción el hecho de que el Consejo de Supervisión de la Privacidad y las Libertades Civiles (PCLOB) plenamente operativo, en calidad de agencia de control independiente, haya decidido llevar a cabo un proyecto de control para examinar el programa de vigilancia que el poder ejecutivo aplica en virtud del artículo 702 de la *Foreign Intelligence Surveillance Act* (FISA, Ley de Vigilancia de Inteligencia Exterior), antes de la fecha de expiración de diciembre de 2023 para el artículo 702 y la futura consideración pública y parlamentaria de su reautorización[172]. El CEPD también acoge con satisfacción el hecho de que la revisión abarque ámbitos de interés seleccionados para la investigación, incluso, entre otros, las consultas de información recogida en virtud del artículo 702 por

[171] Véase el Informe de la tercera revisión conjunta, página 17, apartado 83.
[172] Véase NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) [COMUNICACIÓN DEL PROYECTO DE CONTROL DEL PCLOB QUE EXAMINA EL ARTÍCULO 702 DE LA LEY DE VIGILANCIA DE INTELIGENCIA EXTERIOR (FISA)].

parte de ciudadanos estadounidenses y la recogida «hacia arriba» llevada a cabo de conformidad con dicho artículo[173], y que también abarque la revisión del valor y la eficacia pasados y previstos del programa, así como la adecuación de las garantías vigentes de protección de la privacidad y las libertades civiles[174]. En consecuencia, el CEPD recalca que sería necesario acceder a las apreciaciones del PCLOB en este informe sobre el artículo 702 para evaluar de forma adecuada y completa las garantías de protección de la privacidad previstas y aplicadas en el contexto de este programa de vigilancia.

175. Teniendo en cuenta el nuevo EO 14086, el CEPD solicita asimismo información complementaria para evaluar y supervisar también de qué forma y en qué medida estos principios de necesidad y proporcionalidad recientemente introducidos se aplicarán en la práctica en este contexto.

3.2.2.4.2 Recogida de datos a efectos de seguridad nacional en virtud del EO 12333

176. Tal y como reconoció el TJUE en su sentencia Schrems II, el análisis de las leyes del tercer país cuya adecuación está sujeta a consideración no debe limitarse a las leyes y las prácticas que permiten la vigilancia dentro de las fronteras físicas del país, sino que también abarca el análisis de los fundamentos jurídicos de la legislación de ese tercer país que permiten llevar a cabo una vigilancia fuera de su territorio por lo que se refiere a los datos de la UE. Las limitaciones necesarias del acceso del Gobierno a los datos deben extenderse a los datos «en tránsito» hacia el país, para los que se reconoce la adecuación.

177. El CEPD acoge con satisfacción el informe público general emitido por el PCLOB en el EO 12333 y publicado en abril de 2021, pero observa que este informe sigue siendo general, puesto que la mayoría de las constataciones están clasificadas.

178. En este contexto, de nuevo, habida cuenta de la incertidumbre y la falta de claridad sobre el modo en que el EO 12333 solía aplicarse, y de la importancia de aclarar cómo se aplicará a la luz del nuevo EO 14086, el CEPD hace hincapié en la importancia de los esperados informes del PCLOB sobre este texto[175]. Sin embargo, entiende que es probable que la mayor parte del contenido permanezca clasificado, de manera que no se pondría a disposición ni del público ni del CEPD información adicional sobre la aplicación concreta del EO 12333 y sobre su necesidad y proporcionalidad.

179. El CEPD, por tanto, acogería con especial satisfacción que el informe del PCLOB sobre la aplicación del EO 14086 no estuviera clasificado, sino que fuera totalmente accesible una vez concluido, incluso por lo que respecta a las partes que evaluarían el modo en que las garantías del EO 14086 se aplicarán a la recogida de datos en virtud del EO 12333. El CEPD también invita a la Comisión a que esté especialmente atenta a este punto en el contexto de las revisiones conjuntas futuras.

180. En general, por lo que respecta a los diversos instrumentos jurídicos que establecen la posibilidad de recoger, acceder ulteriormente y tratar datos para las agencias de inteligencia estadounidenses en el marco jurídico de los EE. UU., el CEPD acogería con satisfacción aclaraciones sobre su interacción con el nuevo EO 14086 y espera garantías de que las preocupaciones expresadas en los dictámenes anteriores del CEPD a este respecto se resuelvan por medio de la adopción de estas nuevas garantías.

[173] Véase *supra*.
[174] Véase *supra*.
[175] El informe general sobre el EO 12333 ha permanecido clasificado en su mayor parte y solo se ha publicado una versión pública abreviada, al igual que ocurre con el informe y las Recomendaciones sobre las actividades de lucha contra el terrorismo de la CIA llevadas a cabo de conformidad con el EO 12333, que solo se han desclasificado parcialmente.

181. El CEPD también insta a la Comisión a que esté especialmente atenta a estos aspectos en el contexto de las revisiones conjuntas futuras.

3.2.2.4.3 Informe del PCLOB

182. El CEPD acoge con satisfacción el hecho de que el EO 14086 también establezca el requisito de que el PCLOB elabore un informe relativo a la aplicación del EO. El CEPD subraya que este informe debe incluir una evaluación de la posibilidad específica prevista en el EO para recoger datos, a los efectos enumerados para la recopilación selectiva, así como la recopilación en bloque, incluso por razones técnicas, con vistas a entender los términos clave del EO 14086 y cómo se entienden y aplican estos en la práctica en los distintos programas de vigilancia. Este informe también sería necesario para evaluar la forma en que el EO se aplicará en los procedimientos y las políticas internos de los servicios de inteligencia.

3.2.3 Garantía C - Supervisión

3.2.3.1 Introducción

183. Las actividades de inteligencia estadounidenses están sujetas a un proceso de supervisión de varios niveles. La estructura de supervisión en los EE. UU. se puede dividir en supervisión interna y externa. Todos los servicios de inteligencia disponen de agentes encargados de la supervisión y el cumplimiento, que llevan a cabo una supervisión periódica de las actividades de inteligencia de señales, entre ellos los responsables de la protección de la privacidad y las libertades civiles y los inspectores generales. Además, existen organismos de supervisión externa, como el Consejo de Supervisión de la Privacidad y las Libertades Civiles (PCLOB) y la Junta de Supervisión de Inteligencia.

184. El CEPD recuerda que una injerencia tiene lugar en el momento de la recogida de los datos, pero también en el momento en que un poder público accede a los datos para su tratamiento ulterior. El TEDH ha especificado que cualquier injerencia en el derecho a la privacidad y la protección de datos debe estar sujeta a un sistema de supervisión eficaz, independiente e imparcial que debe brindar un juez u otro organismo independiente[176] (por ejemplo, una autoridad administrativa o una instancia parlamentaria).

185. Si bien el TEDH ha expresado su preferencia por que un juez sea el responsable de mantener la supervisión, esto no excluye que otro órgano pueda ser responsable, siempre que dicha autoridad sea suficientemente independiente del poder ejecutivo[177] y de las autoridades encargadas de la vigilancia y tenga poderes de supervisión suficientes y eficaces[178].

186. El TEDH añadió que, a la hora de evaluar la independencia, deben tenerse en cuenta la modalidad de designación y la situación jurídica de los miembros del órgano de supervisión[179].

[176] Sentencia del TEDH de 6 de septiembre de 1978, Klass y otros c. Alemania (en lo sucesivo, «sentencia del TEDH Klass»), apartados 17 y 51.
[177] Sentencia del TEDH Zakharov, apartado 258; sentencia del TEDH de 10 de febrero de 2009, Iordachi y otros c. Moldavia, apartados 40 y 51; sentencia del TEDH de 26 de abril de 2007, Dimitru Popescu c. Rumanía, apartados 70-73.
[178] Sentencia del TEDH Klass, apartado 56.
[179] Sentencia del TEDH Zakharov, apartado 278.

187. El TEDH también señaló que debe examinarse si las actividades del órgano de supervisión están sometidas al control público. Por ejemplo, esto podría cumplirse, cuando el órgano de supervisión informe con carácter anual al Gobierno, mediante la presentación de informes públicos al Parlamento y su debate en él[180].

188. El TJUE también tuvo en cuenta la supervisión independiente de la aplicación de las medidas de vigilancia en la sentencia Schrems II en el sentido de que «[...] el control ejercido por el FISC tiene por objeto comprobar si esos programas de vigilancia se atienen a la finalidad de obtener información en materia de inteligencia exterior, pero no tiene por objeto determinar "si [las personas objetivo seleccionadas son adecuadas] para recabar información de inteligencia exterior"»[181].

3.2.3.2 Supervisión interna

3.2.3.2.1 Inspectores generales

189. El CEPD reconoce que los inspectores generales tienen encomendado un amplio abanico de facultades, necesarias para supervisar las actividades de inteligencia. En particular, los inspectores generales tienen acceso a toda la información necesaria para evaluar el cumplimiento general del trabajo de las agencias con la legislación, también, entre otras, con las leyes en materia de privacidad y protección de datos, y pueden expedir requerimientos, así como tomar juramento a cualquier persona en relación con la investigación de los inspectores generales.

190. Por todas estas razones, el CEPD considera que los inspectores generales tienen, en general, amplias facultades de investigación. Sin embargo, no disponen de facultades correctoras vinculantes y solo emiten recomendaciones no vinculantes[182].

191. El CEPD reconoce que, en principio, a los inspectores generales no se les impedirá ni prohibirá iniciar, llevar a cabo o concluir auditorías o investigaciones, ni emitir requerimientos durante el curso de una auditoría o investigación[183]. En este contexto, el CEPD señala, no obstante, que los inspectores generales se encuentran bajo la autoridad, la dirección y el control del jefe de departamento respectivo, que puede prohibirles acceder a la información, llevar a cabo una investigación y, entre otros, emitir requerimientos en casos en los que el jefe de departamento determine que dicha prohibición es necesaria para preservar los intereses nacionales. Sin embargo, el jefe de departamento debe informar a los comités responsables del Congreso de los Estados Unidos del ejercicio de esta facultad[184].

192. El CEPD observa que los inspectores generales solo pueden ser destituidos por el Presidente de los Estados Unidos, que debe informar al Congreso de los motivos de dicha destitución.

193. El CEPD observa que no se han introducido modificaciones sustanciales en el mecanismo de supervisión interna desde los dictámenes del GT29 y posteriormente del CEPD. Por tanto, el CEPD

[180] Sentencia del TEDH Zakharov, apartado 283; sentencia del TEDH de 9 de junio de 1990, L. c. Noruega; sentencia del TEDH de 18 de mayo de 2010, Kennedy c. Reino Unido, apartado 166.
[181] Sentencia del TJUE Schrems II, apartado 179.
[182] Proyecto de Decisión, considerando 105.
[183] Véase la *Inspector General Act* (Ley de Inspectores Generales) de 1978, artículo 3(a).
[184] Véanse, por ejemplo, la *Inspector General Act* (Ley de Inspectores Generales) de 1978, artículos 8 (para el Departamento de Defensa); 8E (para el Departamento de Justicia); 8G (d)(2)(A), (B) (para la NSA); USC, título 50, artículo 403q, letra b) (para la CIA); y la *Intelligence Authorization Act For Fiscal Year 2010* (Ley de Autorización de Actividades de Inteligencia para el Ejercicio 2010), artículo 405, letra f) (para los servicios de inteligencia).

coincide con el Dictamen 01/2016 del GT29[185] de que, en general, existen mecanismos de supervisión interna suficientes.

3.2.3.3 Supervisión externa

194. El CEPD observa que, aparte de los órganos citados más adelante, otros órganos del Gobierno de los Estados Unidos supervisan las actividades de las agencias de inteligencia estadounidenses, como la Junta de Supervisión de Inteligencia (IOB, por sus siglas en inglés) o las comisiones parlamentarias. Estas últimas pueden llevar a cabo sus propias investigaciones y elaborar sus propios informes.

3.2.3.3.1 Consejo de Supervisión de la Privacidad y de las Libertades Civiles (PCLOB)

195. El CEPD reconoce la función de supervisión integral del PCLOB con respecto al nuevo mecanismo de recurso y la aplicación del EO 14086.

196. En primer lugar, sus nuevas funciones abarcan consultas con el Fiscal General en relación con la designación de los jueces del DPRC y los letrados especiales. En segundo lugar, el PCLOB revisará anualmente el procedimiento de recurso, es decir, la tramitación de las reclamaciones cualificadas previstas en el mecanismo de recurso. Esto abarca si el CLPO y el Tribunal de Revisión de la Protección de Datos tramitan las reclamaciones cualificadas a su debido tiempo, disponen de pleno acceso a la información necesaria y actúan conforme al EO 14086, así como el cumplimiento por parte de los servicios de inteligencia de las decisiones del CLPO y el DPRC.

197. Asimismo, en el momento en que las agencias de inteligencia actualizan sus políticas y procedimientos internos para aplicar el EO 14086 estas deben consultar al PCLOB. Además, el PCLOB llevará a cabo una revisión de las políticas y los procedimientos actualizados y evaluará su cumplimiento del EO 14086[186]. Si bien las constataciones del PCLOB no son vinculantes *stricto sensu*, el jefe de cada servicio de inteligencia está obligado a tener debidamente en cuenta y aplicar, o abordar de otro modo, todas las recomendaciones contenidas en dicha revisión, de conformidad con la legislación aplicable[187]. El CEPD invita a la Comisión a que, en caso de aprobarse el proyecto de Decisión, en futuras revisiones preste especial atención a si las recomendaciones del PCLOB se han aplicado a nivel de agencia y cómo se han aplicado.

198. El CEPD recuerda que, puesto que el PCLOB es independiente, se le «anima», pero no se le obliga, a revisar si las garantías establecidas en el EO 14086 se tienen en cuenta debidamente y si los servicios de inteligencia cumplen plenamente con los requisitos del procedimiento de recurso. No obstante, el CEPD entiende que el PCLOB ha indicado en su explicación complementaria al CEPD así como en público[188] que asumirá el papel previsto en el EO 14086.

199. Asimismo, el CEPD acoge con satisfacción el hecho de que esté previsto publicar los resultados de los informes del PCLOB. Habida cuenta de que los diversos órganos que intervienen en el mecanismo de recurso y los órganos de los servicios de inteligencia tienen, en principio, que aplicar las recomendaciones de los informes del PCLOB o abordarlas de otro modo, el CEPD reconoce que estas recomendaciones desempeñan un papel importante en las garantías de protección de la privacidad.

---

[185] Dictamen 01/2016 del GT29.
[186] EO 14086, artículo 2(c)(iv) y artículo 2(c)(v).
[187] EO 14086, artículo 2(c)(v)(B).
[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

200. El CEPD observa que el acceso del PCLOB a la información está restringido, si el Presidente de los Estados Unidos autoriza la realización de «acciones encubiertas»[189] por parte de departamentos, agencias o entidades del Gobierno de los Estados Unidos[190].

201. A raíz de los dictámenes anteriores, el CEPD considera al PCLOB un organismo independiente, cuyas recomendaciones han significado una importante contribución a las reformas en los Estados Unidos, y cuyos informes han resultado particularmente útiles para entender el funcionamiento de los diversos programas de vigilancia, y es un elemento esencial de la estructura de supervisión.

202. Sin embargo, el CEPD lamentó que en su tercera revisión conjunta anual del antiguo. Escudo de la privacidad UE-EE. UU. el PCLOB tan solo proporcionara a la CEPD la misma información que al público en general. Asimismo, lamentó que el PCLOB no emitiera más informes sobre la PPD-28 para dar seguimiento a su primer informe al objeto de proporcionar elementos adicionales sobre el modo de aplicar las garantías de la PPD-28, así como un informe general actualizado sobre el artículo 702 de la FISA.

203. Por tanto, el CEPD acoge con satisfacción el anuncio del PCLOB a la CEPD de que en un futuro cercano emitirá un informe de seguimiento sobre el artículo 702 de la FISA. Además, el CEPD ha comprobado con satisfacción que el PCLOB informó sobre su compromiso de dar publicidad a sus informes en relación con el EO 14086. Sin embargo, el CEPD recuerda que la publicación de informes desclasificados está regulada por la legislación estadounidense y debe coordinarse con las agencias de los servicios de inteligencia, es decir, que no lo puede decidir el PCLOB por sí solo.

204. Por tanto, de adoptarse el proyecto de Decisión, el CEPD recuerda que en futuras revisiones del marco de protección de datos UE-EE. UU., expertos habilitados del CEPD deben poder revisar los documentos complementarios y debatir los elementos clasificados adicionales que sean necesarios para garantizar que la información contenida en los informes se pueda evaluar de forma adecuada, teniendo en cuenta a su vez los intereses de seguridad nacional pertinentes y las protecciones de la privacidad aplicables.

205. El CEPD acoge con satisfacción la independencia del PCLOB y la supervisión de los servicios de inteligencia nacionales, que deben cumplir las recomendaciones del PCLOB o abordarlas de otro modo, que se indicará en el informe del PCLOB al Congreso de los Estados Unidos.

206. Habida cuenta de los requisitos del TEDH relativos al control público[191] de que los informes de un órgano de control deben presentarse al Parlamento y debatirse en él, el CEPD considera suficiente que el PCLOB presente sus informes con una frecuencia mínima semestral al Presidente de los Estados Unidos y, en particular, a las comisiones parlamentarias del Senado y de la Cámara de Representantes[192], que son los órganos parlamentarios de los Estados Unidos.

[189] Conforme al USC, título 50, artículo 3093, letra e)(1), el término «acción encubierta» significa una actividad o actividades del Gobierno de los Estados Unidos encaminadas a influir en las condiciones políticas, económicas o militares en el extranjero, ya sea con la intención de que el papel del Gobierno de los Estados Unidos pase desapercibido o no se conozca públicamente, pero no incluye 1) actividades cuyo principal propósito sea adquirir inteligencia, actividades tradicionales de contrainteligencia [...].

[190] USC, título 42, artículo 2000ee, letra g) (5); USC, título 50 artículo 3093, letra a).

[191] Sentencia del TEDH Zakharov, apartado 283; sentencia del TEDH de 9 de junio de 1990, L. c. Noruega; sentencia del TEDH de 18 de mayo de 2010, Kennedy c. Reino Unido, apartado 166.

[192] USC, título 42, artículo 2000ee, letra e).

3.2.3.3.2 Tribunal de Vigilancia de la Inteligencia Exterior (FISC)

207. El Tribunal de Vigilancia de la Inteligencia Exterior es responsable de la supervisión de la recogida de datos personales conforme al artículo 702 de la FISA[193] y sus resoluciones se pueden recurrir ante el Tribunal de Revisión de la Vigilancia de la Inteligencia Exterior (FISCR).

208. El FISC supervisa el proceso de certificación para la recogida de información de inteligencia exterior en virtud del artículo 702 de la FISA y autoriza la vigilancia electrónica, el registro físico y otras medidas de investigación con fines de inteligencia exterior[194]. El FISC también autoriza los procedimientos de fijación de objetivos, minimización y consulta de certificados, que son legalmente vinculantes para las agencias de inteligencia estadounidenses[195]. Si el FISC considera que los requisitos no se han cumplido, podrá denegar la certificación de forma total o parcial y exigir la modificación de los procedimientos.

209. Si se determina la existencia de infracciones de los procedimientos de fijación de objetivos, el FISC puede ordenar a la agencia de inteligencia pertinente que adopte medidas correctoras[196]. Estas medidas correctoras pueden abarcar desde medidas individuales a medidas estructurales, por ejemplo, desde el cese de la obtención de datos y la supresión de los datos obtenidos de forma ilegal hasta un cambio en la práctica de recopilación, incluso en términos de orientación y formación del personal.

210. El CEPD reconoce que el EO 14086 establece que el CLPO y el DPRC deben notificar las violaciones al fiscal general adjunto de Seguridad Nacional, que a su vez se las notificará al FISC[197].

211. Tal y como el TJUE señaló en su sentencia Schrems II, el FISC no autoriza medidas de vigilancia individuales, sino que autoriza programas de vigilancia[198]. Por tanto, el CEPD sigue mostrándose preocupado por el hecho de que el FISC no proporciona supervisión judicial eficaz en relación con la fijación como objetivos a ciudadanos no estadounidenses, algo que parece no resolverse en el nuevo EO 14086.

212. Con respecto a la autorización previa independiente[199] de la vigilancia en virtud del artículo 702 de la FISA, el CEPD lamenta que, según se desprende del proyecto de Decisión[200] y de las explicaciones proporcionadas por el Gobierno de los Estados Unidos, el FISC no parece estar vinculado a las garantías adicionales del EO 14086 a la hora de certificar los programas que autorizan la fijación como objetivos a ciudadanos no estadounidenses. En opinión del CEPD, las garantías adicionales contenidas en este EO deberían, no obstante, ser tenidas en cuenta en este contexto. El CEPD recuerda que los informes del PCLOB resultarían particularmente útiles para evaluar el modo en que se ejecutarán las garantías del EO 14086 y cómo se aplicarán cuando los datos se recojan en virtud del artículo 702 de la FISA.

[193] USC, título 50, artículo 1881, letra a).
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.
[195] USC, título 50, artículo 1881a, letra i).
[196] USC, título 50, artículo 1803, letra h).
[197] EO 14086, artículo 3(c)(i)(D); EO 14086, artículo 3(d)(i)(F).
[198] Sentencia del TJUE Schrems II, apartado 179.
[199] Al CEPD le preocupa la ausencia de un proceso de autorización previa para la recopilación de datos en bloque en el marco del EO 12333 (véase la Garantía B) cuando el FISC no sea competente.
[200] Proyecto de Decisión, considerando 165.

3.2.4 Garantía D - Los particulares deben disponer de vías de recurso efectivas

213. El CEPD recuerda que los derechos del individuo efectivos y exigibles tienen una importancia vital para lograr un nivel adecuado de protección de los datos en un tercer país. Los interesados tienen derecho a la tutela judicial efectiva para satisfacer sus derechos cuando consideren que estos no se han respetado. El TJUE explicó en sus sentencias Schrems I y Schrems II que «una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta»[201].

214. El sistema estadounidense relativo a los recursos judiciales contiene un límite importante que dificulta mucho el ejercicio de acciones judiciales contra las medidas de vigilancia del Gobierno de los Estados Unidos ante los tribunales ordinarios. La Constitución de los Estados Unidos exige la demostración de legitimación, es decir, demostrar la existencia de un perjuicio concreto, particularizado y real o inminente[202]. En los casos de vigilancia, dicho requisito parece quedar anulado por la falta de notificación a los particulares que son objeto de la vigilancia, incluso una vez finalizadas estas medidas.

215. En este contexto, el CEPD acoge con satisfacción el hecho de que el EO 14086 establezca un mecanismo de recurso específico para gestionar y resolver reclamaciones de ciudadanos no estadounidenses, con respecto a las actividades de inteligencia de señales de los EE. UU. En virtud de este nuevo mecanismo, el requisito de legitimación no es aplicable: conforme al artículo 4(k)(ii) del EO 14086, el reclamante no tiene que demostrar que sus datos han estado, de hecho, sujetos a actividades de inteligencia de señales de los EE. UU. Los interesados pueden, por tanto, invocar las garantías previstas en el EO 14086, incluso aquellas previstas por otras leyes y disposiciones pertinentes a que se refiere el artículo 4(d)(iii) del EO 14086[203]. A este respecto, el nuevo mecanismo añade una vía de recurso que de otra forma no existiría.

216. El nuevo mecanismo consta de dos niveles: en el primer nivel, los particulares pueden presentar una reclamación ante el responsable de la protección de las libertades civiles (CLPO) de la Oficina del Director de Inteligencia Nacional. En el segundo nivel, los particulares pueden recurrir la decisión del CLPO ante un órgano de nueva creación, el denominado Tribunal de Revisión de la Protección de Datos (DPRC). Las siguientes secciones se centran principalmente en el segundo nivel del mecanismo de recurso. El CEPD considera que al CLPO, en calidad de funcionario público, no se le ha otorgado un grado de independencia suficiente del poder ejecutivo y, por tanto, no puede, por sí mismo, cumplir adecuadamente los requisitos previstos en el artículo 47 de la Carta. Esta evaluación ha sido confirmada por la Comisión en varias ocasiones.

3.2.4.1 ¿Puede el establecimiento del DPRC sobre la base de un Decreto ser suficiente por sí mismo?

217. El DPRC no es un tribunal ordinario establecido por el Congreso en virtud del artículo III de la Constitución de los Estados Unidos, sino que se basa en un Decreto emitido por el Presidente de los Estados Unidos. Aunque el CEPD es consciente de la consideración de base, a saber, evitar el requisito de demostrar legitimación (véase también el apartado 215) y la acoge con satisfacción, esto plantea una pregunta fundamental: ¿puede el mecanismo de recurso satisfacer (en modo alguno) los requisitos del artículo 47 de la Carta? Conforme a esta disposición, toda persona cuyos derechos y

[201] Sentencia del TJUE Schrems I, apartado 95; sentencia del TJUE Schrems II, apartado 187.
[202] Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. p. 10.
[203] El EO 14086, artículo 5(h), crea explícitamente un derecho para los interesados de presentar reclamaciones de acuerdo con el mecanismo de recurso.

libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva ante un juez establecido previamente por la ley.

218. Aunque la redacción en inglés del artículo 47 de la Carta se refiere a un «tribunal», otras versiones lingüísticas dan preferencia al término «juez»[204]. En la sentencia Schrems II, el TJUE ha reiterado que «los justiciables han de tener la posibilidad de ejercer acciones en Derecho ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión»[205]. Sin embargo, en el mismo contexto de evaluación de la adecuación del nivel de protección de los datos, el TJUE considera que una tutela judicial efectiva contra tales injerencias no solo puede ser garantizada por un juez, sino también por un organismo, que ofrezca garantías sustancialmente equivalentes a las exigidas por el artículo 47 de la Carta[206]. Asimismo, el CEDH estipula que toda persona cuyos derechos y libertades hayan sido violados tiene derecho a un recurso efectivo ante una instancia nacional[207], que, según el TEDH ha reconocido en jurisprudencia reiterada, no tiene por qué ser necesariamente una autoridad judicial[208]. Los poderes y las garantías procesales que posee una autoridad, en particular si es independiente del poder ejecutivo y garantiza la justicia de los procedimientos, son pertinentes para evaluar la eficacia del recurso ante dicha autoridad[209]. Parece que ambos tribunales no basan su evaluación en criterios puramente formales, sino que consideran decisivas las garantías sustantivas.

219. En la sentencia Schrems II, el TJUE prestó especial atención a las vías de recurso eficaces en el área del acceso a los datos personales a efectos de seguridad nacional. El CEPD toma nota de que, al hacerlo, el TJUE sin embargo no debatió el elemento «establecido previamente por la ley» del artículo 47 de la Carta, aunque la figura del Defensor del Pueblo en el ámbito del Escudo de la privacidad tampoco se basaba en el Derecho común estadounidense. En lugar de abordar este asunto, el TJUE evaluó distintos aspectos para su prueba de adecuación, como la falta de facultades correctoras. Por tanto, la sentencia Schrems II no prevé ninguna orientación sobre la evaluación del elemento «establecido previamente por la ley» conforme al artículo 47 de la Carta. Sin embargo, existen otras sentencias en las que el TJUE se ha manifestado sobre este asunto. Haciéndose eco de la jurisprudencia reiterada del TEDH a este respecto, el TJUE recordó en sus asuntos C-487/19 y C-132/20 que la razón de la introducción del elemento «establecido previamente por la ley» es garantizar que la organización del sistema judicial en una sociedad democrática no dependa de la discreción del poder ejecutivo, sino que esté regulada por una ley adoptada por el poder legislativo de conformidad con las normas que delimitan el ejercicio de su competencia[210]. Como se puede comprobar en esta sentencia, el derecho a un juez establecido previamente por la ley está muy estrechamente relacionado con la garantía de independencia.

220. Habida cuenta de lo anterior, el CEPD concluye que, en el contexto de la evaluación de la adecuación del nivel de protección, el mecanismo de recurso específico creado en virtud del EO 14086 por oposición al recurso del artículo III no es insuficiente *per se*. El análisis del nivel de protección a este

[204] Por ejemplo, «Gericht» en la versión alemana.
[205] Sentencia del TJUE Schrems II, apartado 194.
[206] Véase la sentencia del TJUE Schrems II, apartado 197.
[207] Artículo 13 del CEDH.
[208] Sentencia del TEDH Klass, apartado 67; sentencia del TEDH Big Brother Watch, apartado 359.
[209] Sentencia del TEDH Klass, apartado 67; sentencia del TEDH Big Brother Watch, apartado 359.
[210] Véase la sentencia del TJUE de 6 de octubre de 2021, W.Ż, C-487/19, ECLI:EU:C:2021:798 y la sentencia del TJUE de 29 de marzo de 2022, Getin Noble Bank S.A., C-132/20, ECLI:EU:C:2022:235, apartado 129 y apartado 121.

respecto depende de si las garantías previstas en el EO 14086 y complementadas por el Reglamento FG garantizan de forma suficiente la independencia del DPRC frente a otros poderes.

221. La Comisión debe supervisar continuamente si las normas establecidas en el EO 14086 y sus disposiciones complementarias, en particular aquellas que están diseñadas para promover la independencia del DPRC, son plenamente aplicadas y funcionan de forma efectiva en la práctica. Además, todas las modificaciones del marco deben revisarse detenidamente para determinar la repercusión en la evaluación de la Comisión conforme al proyecto de Decisión. A este respecto, el CEPD señala que las modificaciones del EO 14086 y el Reglamento FG pueden dar lugar a la adopción de actos de ejecución de aplicación inmediata para suspender, derogar o modificar la Decisión de adecuación[211].

3.2.4.2 Independencia suficiente del poder ejecutivo

222. En su sentencia Schrems II, el TJUE subrayó que se debía garantizar la independencia del juez o el organismo, especialmente del poder ejecutivo, con todas las garantías necesarias, incluso con respecto a sus condiciones de cese o revocación del nombramiento. Más en concreto, el TJUE ha criticado el hecho de que el Defensor del Pueblo fuera nombrado por el Secretario de Estado y rindiera cuentas directamente a este. El Defensor del Pueblo se consideró una parte integral del Departamento de Estado de los EE. UU. El TJUE también consideró que no existían garantías particulares para el cese o la revocación del nombramiento del Defensor del Pueblo, lo que socavaba su independencia con respecto al poder ejecutivo.

223. El CEPD reconoce que las disposiciones del EO 14086 y el Reglamento FG complementario no imponen al DPRC una obligación de notificación al Fiscal General, como ocurriría en el caso de una relación de subordinación. El DPRC tampoco está sujeto a la «supervisión cotidiana» del Fiscal General[212]. Estas garantías constituyen una mejora significativa con respecto al Escudo de la privacidad. Sin embargo, el DPRC está establecido en el seno de la función ejecutiva, a saber, el Departamento de Justicia. Por esta razón en particular, la aplicación y el funcionamiento efectivo de las garantías en la práctica serán esenciales para determinar si el DPRC que, sin ser una parte integral del Departamento de Justicia, es una entidad no obstante situada en el seno del poder ejecutivo, puede considerarse suficientemente independiente en la práctica. El CEPD insta a la Comisión a que supervise atentamente si estas garantías se reflejan plenamente en la práctica. Además, el CEPD recomienda la aclaración del término «supervisión cotidiana» al objeto de que los «jueces» del DPRC no estén sujetos a supervisión de ningún tipo. La Comisión ha confirmado que «supervisión cotidiana» debe entenderse en este sentido.

224. Al margen de las garantías antedichas, el MPD UE-EE. UU. prevé determinadas garantías en relación con la designación y el cese de los «jueces» del DPRC. Aunque son designados por el Fiscal General, su designación se basa en los criterios utilizados para evaluar a los candidatos a los juzgados federales e implica una consulta con el PCLOB. El cese de los «jueces» durante un procedimiento en curso o antes de la expiración de su mandato solo es posible en circunstancias estrictamente definidas, que, a entender del CEPD, siguen el modelo de las disposiciones aplicables a los jueces federales[213]. La aplicación de estas normas representa un paso más para reforzar la posición independiente del DPRC, por lo que, de nuevo, su aplicación en la práctica será crucial. Sin embargo, en el proyecto de Decisión no queda claro si el cumplimiento de estos requisitos se observará en los Estados Unidos y cómo se hará. Sobre la base de las explicaciones adicionales ofrecidas por la Comisión y el Gobierno de los

[211] Proyecto de Decisión, considerando 212.
[212] Reglamento FG, artículo 201.7, letra d).
[213] EO 14086, artículo 3(d)(iv); Reglamento FG, artículo 201.7.

Estados Unidos, el CEPD entiende que el PCLOB podrá abordar las disposiciones antes citadas en su revisión anual del procedimiento de recurso y que la responsabilidad de supervisar y garantizar el cumplimiento de todos los requisitos legales del inspector general del Departamento de Justicia abarca los requisitos previstos en el EO 14086 y los reglamentos relativos a la creación del DPRC. El CEPD invita a la Comisión a que aclare este aspecto en el proyecto de Decisión. Dicho esto, la Comisión tendrá en cuenta estas garantías a la hora de supervisar la práctica real del tratamiento de datos personales según lo previsto en este proyecto de Decisión.

225. El proyecto de Decisión no aborda la cuestión de si el Presidente de los Estados Unidos tiene potestad para cesar o destituir «jueces» del DPRC y, en caso afirmativo, en qué condiciones. El CEPD entiende que dicha potestad no existiría, tal y como ha explicado la Comisión Europea y han confirmado representantes del Gobierno de los Estados Unidos. El CEPD sugiere aclarar este aspecto en la Decisión de adecuación.

226. Los «jueces» del DPRC se nombran para un mandato renovable de cuatro años y, en el momento de su designación inicial, no deben haber trabajado en la rama ejecutiva en los dos años anteriores[214]. Durante su mandato como «jueces» del DPRC, no tendrán ningún otro cometido oficial o empleo en el seno del Gobierno de los Estados Unidos[215]. No obstante, podrán, a diferencia de los jueces federales de los EE. UU., desarrollar actividades extrajudiciales, como actividades empresariales y financieras, actividades de recaudación de fondos sin ánimo de lucro, actividades fiduciarias y el ejercicio de la abogacía, siempre que dichas actividades no interfieran en el desempeño imparcial de sus obligaciones o la eficacia o independencia del DPRC[216]. La independencia judicial no solo emana de la ausencia de instrucciones, sino también de la independencia personal. En este contexto, factores como el mandato, la posibilidad de volver a ser designado y la posibilidad de conflictos de intereses son pertinentes. El mandato de cuatro años previsto en el EO 14086 y en el Reglamento FG, aun siendo más corto que los mandatos de los jueces del TJUE (seis años con la posibilidad de ser nuevamente designados) y del TEDH (nueve años sin posibilidad de ser nuevamente designados), no genera inquietudes graves. El CEPD no conoce ninguna jurisprudencia que imponga un mandato mínimo a este respecto[217]. El CEPD también reconoce que la posibilidad de desarrollar actividades extrajudiciales está sujeta a la condición, en pocas palabras, de que estas no generen conflictos de intereses que comprometan las obligaciones del DPRC. El CEPD entiende, a partir de las explicaciones adicionales del Gobierno de los Estados Unidos, que estos requisitos también están sujetos a la revisión y la supervisión del PCLOB y del inspector general del Departamento de Justicia (véase el apartado 226 *supra*). En las revisiones conjuntas también deberá abordarse cómo se aplicará y se demostrará en la práctica este requisito.

227. Conforme al artículo 3(d)(i)(B) del EO 14086, todos los «jueces» deben tener habilitaciones de seguridad para acceder a información clasificada, es decir, para desempeñar su función de resolver asuntos que afectan a la seguridad nacional[218]. Por el contrario, algunas disposiciones legales y reglamentarias europeas en materia de habilitación de seguridad eximen a los jueces del requisito de una habilitación de seguridad en tanto estén desempeñando funciones judiciales, si dicho control escrupuloso vulnera potencialmente la independencia judicial[219]. Conforme a las explicaciones del Gobierno de los Estados Unidos, mientras que los candidatos a puestos judiciales en un tribunal

[214] Reglamento FG, artículo 201.3, letra a).
[215] Reglamento FG, artículo 201.3, letra c).
[216] Reglamento FG, artículo 201.7, letra c).
[217] Véase también, *mutatis mutandis*, la sentencia del TEDH (Gran Sala) de 25 de mayo de 2021, Centrum För Rättvisa c. Suecia, apartado 346.
[218] Véase también el Reglamento FG, artículo 201.11, letra b) y el proyecto de Decisión, considerando 177.
[219] P. ej., artículo 2(3) de la Ley alemana relativa a las habilitaciones de seguridad.

estadounidense se someten a un escrutinio minucioso, los jueces federales de los tribunales estadounidenses no están obligados a obtener una habilitación de seguridad para acceder a documentos clasificados pertinentes para el asunto.

228. En opinión del CEPD, las circunstancias descritas anteriormente revelan parcialmente diferencias entre la posición y la situación de los jueces federales estadounidenses y los «jueces» del DPRC. Sin embargo, las garantías previstas no permiten dudar de la independencia del DPRC. El CEPD urge a la Comisión a que, de adoptarse el proyecto de Decisión, las garantías antes citadas sean una prioridad durante la primera revisión conjunta del MPD UE-EE. UU. Asimismo, el CEPD espera que la Comisión dé seguimiento a su compromiso de suspender, derogar o modificar la Decisión, de adoptarse, en caso de que el poder ejecutivo de los Estados Unidos decidiera restringir las garantías establecidas en el EO[220].

3.2.4.3 Poderes del DPRC

3.2.4.3.1 Acceso a la información

229. La tutela judicial efectiva requiere que un órgano jurisdiccional disponga de facultades de investigación suficientes para revisar la medida impugnada. En el asunto Kadi II, el TJUE declaró con respecto al artículo 47 de la Carta que el juez de la Unión Europea debe asegurarse de que una decisión disponga de unos fundamentos de hecho suficientemente sólidos[221]. El TJUE establece que «incumbe al juez de la Unión proceder a ese examen solicitando, en su caso, a la autoridad competente de la Unión que presente los datos o pruebas, confidenciales o no, pertinentes para ese examen»[222], por lo que «no cabe oponer el secreto o la confidencialidad de tales datos o pruebas»[223].

230. Conforme al considerando 181 del proyecto de Decisión, el DPRC revisa las decisiones tomadas por el CLPO sobre la base, como mínimo, del expediente de la investigación del CLPO, así como de toda la información y los datos presentados por el reclamante, el letrado especial o una agencia de inteligencia. El proyecto de Decisión establece además que el DPRC tiene acceso a toda la información necesaria, que podrá obtener a través del CLPO. Esto se basa en la disposición del artículo 201.9, letra b), del Reglamento FG, que autoriza al DPRC a solicitar al CLPO de la ODNI que complemente el expediente con información explicativa o aclarativa específica y que realice comprobaciones fácticas adicionales cuando sea necesario para permitir al panel del DPRC llevar a cabo su revisión. El CEPD entiende que la evaluación llevada a cabo por el DPRC no está, por tanto, de ninguna forma limitada a las comprobaciones realizadas por el CLPO en el primer nivel del nuevo mecanismo de recurso. Por el contrario, el DPRC puede solicitar información legal complementaria y, lo que es más importante, más circunstancias fácticas para su análisis de si se ha producido una infracción encubierta. Al mismo tiempo, el CEPD también toma nota de que estas amplias facultades de investigación no se extienden al acceso directo a los datos que obran en poder del particular. La Comisión ha explicado que el CLPO siempre actuará como un intermediario cuando el DPRC necesite más información. Por tanto, el acceso por parte del DPRC a la información necesaria para resolver de manera independiente una solicitud de revisión depende, en cierta medida, de que el CLPO proporcione la información necesaria. El CEPD reconoce que el CLPO tiene la obligación de prestar el apoyo necesario al DPRC y las agencias de inteligencia están obligadas a proporcionar al CLPO acceso a la información necesaria para llevar a

[220] Proyecto de Decisión, considerando 212.
[221] Sentencia del TJUE de 18 de julio de 2013, Comisión y otros/Kadi, asuntos acumulados C-584/10 P, C-593/10 P y C-595/10 P (en lo sucesivo, «sentencia del TJUE Kadi II»), apartado 119.
[222] Sentencia del TJUE Kadi II, apartado 120.
[223] Sentencia del TJUE Kadi II, apartado 125.

cabo la revisión del DPRC[224]. El CEPD también señala, no obstante, que el propio CLPO no es independiente y lleva a cabo la investigación inicial de una reclamación en la primera fase del procedimiento de recurso. Por tanto, el CEPD acoge con satisfacción el hecho de que el PCLOB verificará durante sus revisiones anuales del mecanismo de recurso si el DPRC ha obtenido pleno acceso a toda la información necesaria[225]. Asimismo, el CEPD invita a la Comisión a incluir este aspecto en las revisiones conjuntas, en caso de adoptarse el proyecto de Decisión, para examinar las implicaciones de este sistema en la práctica.

3.2.4.3.2 Facultades correctoras

231. Una de las principales deficiencias del Escudo de la privacidad que provocó su invalidación por parte del TJUE en el asunto Schrems II fue la falta de facultades correctoras vinculantes del Defensor del Pueblo. El TJUE consideró que «no contiene ninguna indicación de que dicho defensor del pueblo esté facultado para adoptar decisiones vinculantes con respecto a esos servicios»[226]. El simple compromiso (político) del Gobierno estadounidense de que el servicio de inteligencia en cuestión corregiría cualquier infracción de las normas aplicables detectada por el Defensor del Pueblo no bastaba para garantizar el nivel de protección equivalente en lo esencial al garantizado en el artículo 47 de la Carta.

232. Por el contrario, conforme al nuevo mecanismo de recurso, las decisiones adoptadas por el CLPO y por el DPRC tienen un efecto vinculante[227]. El CEPD reconoce, por un lado, que esta autoridad no se limita a medidas específicas, sino que permite medidas correctoras apropiadas para corregir plenamente una infracción encubierta. En particular, el artículo 4(a) del EO 14086 menciona explícitamente la supresión de datos recogidos de manera ilícita. Por otro lado, el CEPD observa que la redacción del artículo 4(a) del EO 14086 genera cierta incertidumbre por lo que se refiere al proceso de determinación de dichas medidas correctoras apropiadas. Si bien una medida debe diseñarse para corregir plenamente una infracción, también deben tenerse en cuenta las formas en que se ha abordado habitualmente una infracción del tipo detectado[228]. El significado y el efecto de dicho requisito no están claros. Por tanto, el CEPD invita a la Comisión a que supervise detenidamente las medidas correctoras adoptadas en la práctica.

3.2.4.4 Presentación de una reclamación en virtud del nuevo mecanismo de recurso

233. El mecanismo de recurso establecido en virtud del EO 14086 solo es aplicable a las reclamaciones cualificadas transmitidas por el poder público apropiado en un estado cualificado por lo que se refiere a las actividades de inteligencia de señales de los Estados Unidos para una infracción encubierta[229]. Por tanto, para beneficiarse de esta protección jurídica, deben cumplirse varias condiciones.

3.2.4.4.1 Designación de estado cualificado

234. En primer lugar, la organización de la integración económica regional o nacional desde la que se transfirieron los datos a los Estados Unidos debe contar con la designación de estado cualificado antes de la transferencia de los datos que subyace a la reclamación[230]. Evidentemente, es esencial que el mecanismo de recurso previsto esté disponible cuando la Decisión de adecuación entre en vigor. En

[224] EO 14086, artículo 3(c)(i)(H) y artículo 3(d)(iii).
[225] EO 14086, artículo 3(e)(i).
[226] Sentencia del TJUE Schrems II, apartado 196.
[227] EO 14086, artículo 3(c)(ii) y artículo 3(d)(ii), respectivamente.
[228] EO 14086, artículo 4(a).
[229] EO 14086, artículo 3(a).
[230] EO 14086, artículos 4(d)(i) y 4(k)(i).

consecuencia, el considerando 196 del proyecto de Decisión establece que la entrada en vigor de la Decisión está condicionada, entre otras cosas, a la designación de la Unión como entidad cualificada a los efectos del mecanismo de recurso. De hecho, la Comisión parece asumir que la designación se producirá antes de la adopción de la Decisión, puesto que el proyecto ya incluye un espacio reservado para la designación de la UE por parte del Fiscal General[231] (por oposición a la inclusión de la designación como condición previa en la parte dispositiva del proyecto de Decisión).

3.2.4.4.2 Efecto perjudicial para los intereses en materia de privacidad y libertades civiles y «legitimación»

235. Una «reclamación cualificada» debe basarse en una supuesta «infracción encubierta» que, a su vez, exige una infracción que tenga un efecto perjudicial para los intereses en materia de privacidad y libertades civiles individuales del reclamante[232]. Conforme a las explicaciones adicionales ofrecidas por la Comisión, el CEPD entiende que la expresión «efecto perjudicial» no implica ninguna forma de restricción en relación con la admisibilidad de una reclamación. Según señaló la Comisión, dicho efecto perjudicial se referiría más bien a cualquier reclamación relacionada con el tratamiento de datos personales a efectos de actividades de inteligencia de señales contraviniendo las disposiciones a que se refiere el artículo 4(d)(iii), por ejemplo, las garantías previstas en el EO 14086. El CEPD lamenta que esto no se especifique en el texto del proyecto de Decisión e invita a la Comisión a que aclare la noción de sufrir un «efecto perjudicial» para garantizar que toda infracción de los derechos de los interesados se evalúe y corrija, y que no es necesario demostrar ningún nivel de «gravedad» para tener acceso a una vía de recurso y una reparación adecuada.

236. Como ya se ha indicado, una reclamación presentada en el marco del EO 14086 no exige al reclamante que demuestre legitimación (véase el apartado 215)[233]. El CEPD acoge con satisfacción la aclaración del artículo 4(k) del EO 14086 de que se aplicará una «prueba de creencia» y que no es necesario demostrar que se ha accedido a los datos del reclamante mediante actividades de inteligencia de señales. El establecimiento del mecanismo de recurso constituye un paso importante, ya que el requisito de legitimación dificulta mucho la impugnación de las medidas de vigilancia ante los tribunales ordinarios de los Estados Unidos.

237. Por todas estas razones, el CEPD no considera que el recurso a tribunales ordinarios, al que también se refiere el proyecto de Decisión[234], ofrezca un nivel adecuado de protección[235]. A este respecto, el CEPD recuerda sus preocupaciones ya expresadas en numerosas ocasiones en relación con el requisito de legitimación ante los tribunales ordinarios[236]. Es más, a raíz de las declaraciones adicionales del Gobierno de los Estados Unidos, el CEPD entiende que, si bien el EO 14086 no impide recurrir a los tribunales de competencia general, no está claro el modo en que un tribunal de este tipo aplicaría este EO. Esta cuestión podría explorarse más a fondo en futuras revisiones, en caso de adoptarse el proyecto de Decisión.

[231] Proyecto de Decisión, nota a pie de página 320.
[232] EO 14086, artículo 4(k)(i) y 4(d)(ii).
[233] Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. p. 10.
[234] Proyecto de Decisión, considerando 187 y ss.
[235] Véase también la sentencia del TJUE Schrems II, apartados 191 y 192.
[236] Véase también el Dictamen 01/2016 del GT29, p. 43.

3.2.4.4.3 El procedimiento de reclamación

238. El CEPD aprueba, en principio, el procedimiento para canalizar una reclamación a través de las autoridades de control de los Estados miembros y sigue creyendo que la identificación del reclamante debe tener lugar en el territorio de la UE. Sin embargo, al igual que ocurría en el mecanismo del Defensor del Pueblo del Escudo de la privacidad, el proyecto de Decisión establece que el interesado que desee presentar una reclamación debe enviarla a una autoridad de control de un Estado miembro de la UE con competencia para la supervisión de los servicios de seguridad nacional o el tratamiento de datos personales por parte de los poderes públicos[237]. A este respecto, el CEPD reitera sus preocupaciones ya expresadas en el Dictamen sobre el Escudo de la privacidad del GT29, por ejemplo, las posibles dificultades que existen para que los particulares identifiquen a la autoridad competente, habida cuenta de la variedad de mecanismos de supervisión de los servicios de seguridad nacional en los Estados miembros[238]. Teniendo en cuenta la participación de las autoridades nacionales responsables de la protección de datos en la aplicación y la supervisión del MPD UE-EE. UU., es más apropiado canalizar las reclamaciones a través de estas.

3.2.4.5 La decisión del DPRC

239. Tras la conclusión de la revisión de la solicitud del reclamante, el DPRC no debe revelar si el reclamante estuvo o no sujeto a actividades de inteligencia de señales de los EE. UU. En su lugar, se notifica al reclamante bien que en la revisión no se detectó ninguna de las infracciones cubiertas, o bien que el Tribunal de Revisión de la Protección de Datos dictó una resolución que requiere una reparación adecuada[239]. Esta respuesta tipo sirve al fin legítimo general de proteger información delicada sobre las actividades de inteligencia de los EE. UU. Sin embargo, al CEPD le preocupa que el EO 14086 no establezca ninguna excepción a la respuesta tipo del DPRC.

240. En el asunto Kadi II, el TJUE tuvo que pronunciarse sobre el conflicto de intereses del secreto de estado, por un lado, y la imparcialidad del proceso y, en la medida de lo posible, el principio de contradicción, por otro. El TJUE declaró que, cuando existen consideraciones imperiosas relacionadas con la seguridad nacional que se opongan a que se comuniquen ciertos datos o pruebas a la persona afectada, los jueces deben aplicar técnicas que, en el contexto del control jurisdiccional, permitan conciliar las consideraciones legítimas de seguridad en cuanto a la naturaleza y a las fuentes de la información y la necesidad de garantizar en grado suficiente al justiciable el respeto de sus derechos procedimentales, tales como el derecho a ser oído y el principio de contradicción[240]. Asimismo, el TJUE especificó que incumbe a los jueces verificar, mediante un examen de todos los datos de hecho y de Derecho aportados por la autoridad competente de la Unión Europea, si son fundadas las razones que dicha autoridad ha invocado para oponerse a esa comunicación[241]. Si queda manifiesto que las razones invocadas por la autoridad competente de la Unión se oponen efectivamente a la comunicación a la persona afectada de datos o pruebas, será necesario alcanzar un equilibrio apropiado entre las exigencias derivadas del derecho a una tutela judicial efectiva y las derivadas de la seguridad nacional[242]. Para alcanzar ese equilibrio, cabe recurrir a posibilidades tales como comunicar un resumen del contenido de los datos o pruebas de que se trate[243]. Aunque las conclusiones del juez no

[237] Proyecto de Decisión, considerando 169.
[238] Dictamen 01/2016 del GT29, pp. 48 y 49.
[239] EO 14086, artículo 3(d)(i)(H). El EO 14086 también establece esta respuesta para el CLPO.
[240] Sentencia del TJUE Kadi II, apartado 125.
[241] Sentencia del TJUE Kadi II, apartado 126.
[242] Sentencia del TJUE Kadi II, apartado 128.
[243] Sentencia del TJUE Kadi II, apartado 129.

imponen exigencias a la resolución dictada por un juez, sino que tienen que ver con la decisión de la autoridad competente y con la sustanciación de un procedimiento judicial, proporcionan indicaciones sobre el equilibrio de los intereses anteriores en el contexto del derecho a la tutela judicial efectiva. Para obtener más orientaciones, también se puede hacer referencia al asunto Big Brother Watch, en el que el TEDH, aludiendo a la imparcialidad del proceso, y en particular al principio de contradicción, estimó que las resoluciones de un órgano jurisdiccional u otro organismo independiente deben motivarse[244].

241. El CEPD reconoce que las resoluciones del DPRC están motivadas. Se exige expresamente al DPRC que emita una resolución por escrito en la que se establezcan sus decisiones y los detalles de toda reparación apropiada[245]. Asimismo, el CEPD toma nota de que el particular será notificado si la información relativa a una revisión por parte del DPRC se ha desclasificado[246]. El CEPD también reconoce la función de los letrados especiales prevista en el nuevo mecanismo de recurso, que incluye la defensa en relación con el interés del reclamante en el asunto[247]. Sin embargo, habida cuenta de las implicaciones de la jurisprudencia del TJUE y del TEDH señalada anteriormente y teniendo en cuenta que la resolución del DPRC no se puede recurrir, sino que es firme[248], el CEPD tiene dudas sobre la aplicación general de la respuesta tipo del DPRC. El CEPD recuerda que el PCLOB revisará de manera independiente el funcionamiento del nuevo mecanismo de recurso e invita a la Comisión a que preste especial atención a este asunto, incluida cualquier evaluación sobre este aspecto por parte del PCLOB, durante futuras revisiones de la Decisión, en caso de adoptarse.

4 APLICACIÓN Y SUPERVISIÓN DEL PROYECTO DE DECISIÓN

242. Con respecto a la supervisión y la revisión del proyecto de Decisión, el CEPD señala que, según la jurisprudencia del TJUE, «dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión en virtud del [artículo 45 del RGPD], comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión. En cualquier caso esa comprobación es obligada cuando hay indicios que generan una duda en ese sentido»[249].

243. Asimismo, el CEPD observa que la carta del DoC estipula que el DoC y otras agencias estadounidenses, en su caso, celebrarán reuniones periódicas con la Comisión, las APD de la UE interesadas y los representantes pertinentes del CEPD[250].

244. El CEPD considera que, durante el desarrollo de las próximas revisiones periódicas, los siguientes asuntos merecerán una atención especial: la protección conferida por la legislación estatal en relación con el acceso a los datos por parte de las autoridades policiales, la excepción relativa a la recopilación en bloque temporal a la espera de la recopilación selectiva por parte de las autoridades de seguridad nacionales, la aplicación en la práctica de los principios de necesidad y proporcionalidad recientemente introducidos, incluso en el contexto del programa Upstream, la interacción entre el EO 14086 y los distintos instrumentos jurídicos de los EE. UU. que permiten a las agencias de inteligencia estadounidenses recoger y tratar ulteriormente los datos personales, la aplicación de políticas y

[244] Sentencia del TEDH Big Brother Watch, apartado 359.
[245] Reglamento FG, artículo 201.9, letra g).
[246] EO 14086, artículo 3(d)(v).
[247] Reglamento FG, artículo 201.8, letra g).
[248] Reglamento FG, artículo 201.9, letra g).
[249] Sentencia del TJUE Schrems I, apartado 76. Véase también el proyecto de Decisión, artículo 3, apartado 4.
[250] Proyecto de Decisión, anexo III.

procedimientos internos, el modo en que estas garantías se tendrán en cuenta en el contexto de la supervisión llevada a cabo por el FISC, y el modo en que el mecanismo de recurso funcionará en la práctica, y la cuestión de las transferencias ulteriores, las decisiones automatizadas, la supervisión y la ejecución sustantivas y efectivas de los principios del MPD, así como las vías de recurso eficaces.

245. El CEPD observa que la revisión de la constatación de adecuación tendrá lugar un año después de la fecha de notificación de la Decisión de adecuación a los Estados miembros y, posteriormente, como mínimo cada cuatro años[251]. Con vistas a seguir reforzando la supervisión continua de la Decisión de adecuación, el CEPD insta a la Comisión a llevar a cabo las revisiones posteriores como mínimo cada tres años.

246. Por lo que respecta a la participación práctica del CEPD y sus representantes en la preparación y el desarrollo de las revisiones periódicas futuras, el CEPD reitera que toda documentación pertinente debe compartirse por escrito con el CEPD, incluso la correspondencia, con antelación suficiente a la fecha de las revisiones. Como ocurrió en las revisiones realizadas en virtud del Escudo de la privacidad, el CEPD recomienda que, como mínimo tres meses antes de que se lleve a cabo la revisión, la Comisión, la administración estadounidense y el CEPD acuerden las modalidades del procedimiento de revisión.

247. Asimismo, el CEPD observa y acoge con satisfacción que el considerando 212 del proyecto de Decisión ofrezca ejemplos de modificaciones que socavan el nivel de protección que podrían justificar el inicio de un «procedimiento de derogación de emergencia» que se centra en las modificaciones que podrían tener lugar en relación con el EO 14086 y el Reglamento FG conexo.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)

[251] Proyecto de Decisión, artículo 3, apartado 4.