TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL Y EL NUEVO MARCO DE PRIVACIDAD DE DATOS UE-EE.UU.

Alfonso Ortega Giménez



COLEX READER

eBook en www.colex.es

COLEX

COLEX READER



¡Gracias por confiar en Colex!

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

Funcionalidades eBook

Acceso desde cualquier dispositivo

Idéntica visualización a la edición de papel

Navegación intuitiva

Tamaño del texto adaptable

Puede descargar la APP «Editorial Colex» para acceder a sus libros y a todos los códigos básicos actualizados.

Available on the iPhone App Store

GET IT ON Google play

Síguenos en:

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL Y EL NUEVO MARCO DE PRIVACIDAD DE DATOS UE-EE.UU.

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL Y EL NUEVO MARCO DE PRIVACIDAD DE DATOS UE-EE.UU.

Alfonso Ortega Giménez

COLEX 2023

Copyright © 2023

Queda prohibida, salvo excepción prevista en la ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual (arts. 270 y sigs. del Código Penal). El Centro Español de Derechos Reprográficos (www.cedro.org) garantiza el respeto de los citados derechos.

Editorial Colex S.L. vela por la exactitud de los textos legales publicados. No obstante, advierte que la única normativa oficial se encuentra publicada en el BOE o Boletín Oficial correspondiente, siendo esta la única legalmente válida, y declinando cualquier responsabilidad por daños que puedan causarse debido a inexactitudes e incorrecciones en los mismos.

Editorial Colex S.L. habilitará a través de la web www.colex.es un servicio online para acceder a las eventuales correcciones de erratas de cualquier libro perteneciente a nuestra editorial, así como a las actualizaciones de los textos legislativos mientras que la edición adquirida esté a la venta y no exista una posterior.

© Alfonso Ortega Giménez

© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, C.P. 15004
info@colex.es
www.colex.es

SUMARIO

NOTA SOBRE EL AUTOR 9

PARTE I

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL: CUESTIONES GENERALES

I. Planteamiento: el crecimiento exponencial, hoy día, de las transferencias internacionales de datos de carácter personal. 13

II. Concepto de transferencia internacional de datos de carácter personal. 18

III. Sujetos de una transferencia internacional de datos de carácter personal 22

IV. Tipología de transferencias internacionales de datos de carácter personal 25

IV.1. Atendiendo al criterio del país de destino de la transferencia internacional de datos 26

IV.2. Atendiendo a su objeto. 31

IV.3. Atendiendo a los sujetos intervinientes 32

IV.4. Atendiendo a la finalidad o marco jurídico en el que se realizan. 33

V. Decisiones de aplicación de la comisión relativas a las cláusulas contractuales tipo 35

V.1. Características principales de las Decisiones relativas a las cláusulas contractuales tipo 38

a) Función de las cláusulas contractuales tipo 39

b) Los subencargados 40

c) Las transferencias posteriores 40

d) Derechos de los interesados y garantías 41

e) Evaluación y diligencia 41

f) Medidas técnicas y organizativas 42

V.2. Derecho aplicable y competencia judicial internacional relativas a las cláusulas contractuales tipo 43

V.3. Cambios relevantes de las cláusulas contractuales tipo. 44

V.4. Obligaciones para los importadores 45

PARTE II

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL UE-EE.UU.

I. Antecedentes en la regulación de las transferencias internacionales de datos de carácter personal desde la UE a entidades ubicadas en los EE.UU. . . . 47

II. Los principios de *Safe Harbour* o la apuesta por restaurar la confianza en las transferencias internacionales entre los EE.UU. y la UE.: «Scherems I» 50

III. Un nuevo esfuerzo (baldío) por restaurar la confianza en las transferencias internacionales entre los EE.UU. y la UE.: «Scherems II». 55

IV. La sentencia «Schrems II» 59

IV.1. Sobre el ámbito de aplicación del RGPD 59

IV.2. Sobre el nivel de protección adecuado para la transferencia de datos a terceros países 60

IV.3. Sobre las obligaciones de control de las autoridades 63

IV.4. Sobre la validez de la Decisión 2010/87/UE 65

IV.5. Sobre la validez de la Decisión «Escudo de Privacidad» 68

V. ¿Y a la tercera va la vencida?: el nuevo marco transatlántico de privacidad de datos 71

V.1. Contexto 71

V.2. Rasgos característicos. 73

V.3. Especial atención a las reservas del Comité Europeo de Protección de Datos al nuevo Marco transatlántico de privacidad de datos 77

V.4. Valoración crítica 80

V.5. Perspectivas de futuro. 83

CONCLUSIONES 87

BIBLIOGRAFÍA BÁSICA CONSULTADA Y RECOMENDADA 93

ANEXO.- Decisión de ejecución de la Comisión de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre UE y los EE.UU. 97

NOTA SOBRE EL AUTOR

ALFONSO ORTEGA GIMÉNEZ es **Doctor Honoris Causa** por la Universidad Autónoma San Sebastián de San Lorenzo-UASS, en la ciudad de San Lorenzo (Paraguay), a 6 de diciembre de 2022; **Doctor Honoris Causa** por la Universidad Autónoma San Sebastián de San Lorenzo (Paraguay, 2022) y por el Instituto Interamericano de Investigación y Docencia en Derechos Humanos, en la Universidad Juárez Autónoma de Tabasco (México, 2021); **Doctor en Derecho**, 2014 (Calificación: Sobresaliente *Cum Laude* por unanimidad); Premio extraordinario de Doctorado, 2018; Licenciado en Derecho, 2000; y, **Master en Comercio Internacional** también por la Universidad de Alicante, 2001.

Profesor Titular de Derecho internacional privado de la Universidad Miguel Hernández de Elche. Director del Observatorio Provincial de la Inmigración de Alicante. Vicedecano de Grado en Derecho de la Facultad de Ciencias Sociales y Jurídicas de Elche. Director del Máster Universitario en Abogacía de la Universidad Miguel Hernández (UMH) de Elche, desde el curso académico 2021/2022. **Director de la Cátedra de Relaciones Privadas Internacionales UMH-ICAO de la Universidad Miguel Hernández de Elche**, desde marzo de 2022. **También es Magistrado Suplente de la Audiencia Provincial de Castellón** (según Acuerdo de 11 de agosto de 2022, de la Comisión Permanente del Consejo General del Poder Judicial, por el que se resuelve el concurso para provisión de plazas de Magistrado/a suplente y de Juez/a sustituto/a en el año 2022/2023, en el ámbito de los Tribunales Superiores de Justicia de Andalucía, Ceuta y Melilla, Aragón, Principado de Asturias, Illes Balears, Canarias, Cantabria, Castilla y León, Castilla-La Mancha, Cataluña, Comunidad Valenciana, Extremadura, Galicia, Comunidad de Madrid, Región de Murcia, Comunidad Foral de Navarra, País Vasco y La Rioja, convocado por Acuerdo de 17 de marzo de 2022). Publicado en el BOE número 205, Sección II.A., página 120569, de fecha viernes, 26 de agosto de 2022. **Visitante ilustre de la Universidad de San Lorenzo (Paraguay). Académico de Honor de la Academia Internacional de Ciencias, Tecnología, Educación y Humanidades, desde 2018, y Vocal del Observatorio Valenciano de la Inmigración. Socio-Director de COEX International Trade, *Spin-Off* de la Universidad Miguel Hernández de Elche, que se dedica al Asesoramiento, Consultoría y Formación en Internacionalización de la Empresa y Planificación Jurídica Internacional**.

Es Consultor de Derecho internacional privado de la Universitat Oberta de Catalunya (UOC), desde el segundo semestre del curso académico 2008/2009, y **Consejero académico del despacho de Abogados ARA Y ASOCIADOS, con sede principal en Alicante y oficinas en Murcia, Madrid y Beijing (China) y de la Asesoría GRUPO ASESOR ROS, con sede en Elche**.

Reconocidos dos Sexenios de Investigación correspondientes al tramo 2002-2007 CNEAI (Fecha concesión: 23/10/19), al tramo 2009-2017 CNEAI (Fecha concesión: 21/06/18) y al tramo 2010-2016. AVAP (Fecha concesión: 18/01/18).

Miembro de la Asociación para la Docencia e Innovación en Derecho (Ludoteca Jurídica), desde julio de 2021. Miembro de la Asociación de Política Exterior Española. Miembro de la Asociación de Derecho del Arte (ADA). Miembro de Número del Capítulo Reino de España, otorgado por la Academia Norte-Americana de Literatura Moderna Internacional y por la Junta Directiva del Estado de New Jersey (EE.UU.). Miembro del ELI *(European Law Institute)*. Miembro de la Red Española de Política Social-REPS. Miembro de la Sociedad Latinoamericana de Derecho Internacional-SLADI. Miembro de la Asociación Americana de Derecho Internacional Privado-ASADIP. Miembro de número de la Asociación Española de Profesores de Derecho Internacional y Relaciones Internacionales-AEPDIRI; Miembro de la Asociación Española para el Fomento de la Seguridad de la Información-ISMS Forum Spain; Ha sido Vicepresidente de la Asociación del Master en Comercio Internacional de la Universidad de Alicante-AMCI hasta julio 2018; Miembro de la Asociación Española para el Estudio del Derecho Europeo-AEDEUR; Miembro de la Asociación Castellano-Manchega de Sociología-ACMS. Miembro de la Asociación Española de Derecho del Entretenimiento- DENAE. Miembro del Instituto de Derecho Iberoamericano-IDIBE.

Ha recibido numerosos premios en docencia e investigación: Visitante Ilustre de la Universidad San Lorenzo (UNISAL), otorgado por el Consejo Académico mediante Resolución n.° 110/2022-CSU, en Paraguay, a 5 de diciembre de 2022. Premio «INSTITUTO VASCO DE DERECHO PROCESAL» de Artículos Doctrinales sobre el fomento del estudio del Derecho Procesal, en su XII Edición por el trabajo inédito titulado «Resolución de problemas de competencia judicial internacional y de determinación de la ley aplicable en materia de derechos reales en España», en San Sebastián (País Vasco), 11 de octubre de 2022. Premio en la convocatoria de «Premios UMH al Talento Docente» para el año 2021, dentro de la rama académica de Ciencias Sociales, Jurídicas y Humanidades, por Resolución Rectoral n.° 04858/21, de fecha 23 de noviembre de 2021, en el marco del PROGRAMA DOCENTIA-UMH, aprobadas por el Consejo de Gobierno de la Universidad Miguel Hernández de Elche, en sesión de 14 de diciembre de 2020, en Elche, a 02 de diciembre de 2021. Ganador *ex-aequo* en la categoría «Aula responde» del XVIII del Certamen Innova-Emprende de la Universidad Miguel Hernández de Elche, en Elche, a 1 de julio de 2021. Premio en el I Certamen de Artículos Jurídi-

cos Breves del Derecho del Entretenimiento y Tecnologías de la información, organizado por la Asociación Española de Derecho del Entretenimiento —DENAE—, por el artículo «Los contratos inteligentes» (Smart Contracts) ni son «contratos» ni son «inteligentes», en Madrid, a 24 de junio de 2020. Premio «Instituto Vasco de Derecho Procesal» en su IX Edición, por el trabajo «La alegación y prueba del Derecho extranjero tras la nueva Ley de Cooperación Jurídica Internacional», en Donostia —San Sebastián—, a 29 de noviembre de 2019. Cruz al Mérito, en virtud de su destacada y meritoria labor académica y científica profesional, acordado por la Junta de Gobierno de la Academia Internacional de Ciencias, Tecnología, Educación y Humanidades, en Valencia, a 9 de noviembre de 2019. Reconocimiento al Mérito Universitario, en virtud de su destacada y meritoria labor académica y científica profesional, acordado por la Junta de Gobierno de la Academia Internacional de Ciencias, Tecnología, Educación y Humanidades, en Valencia, a 9 de noviembre de 2019. Premio a la excelencia en la práctica jurídica de Economist & Jurist, en Madrid, 3 de diciembre de 2018. Premio UMH 2018 a la Productividad Investigadora, otorgado por el Vicerrector de Investigación e Innovación de la Universidad Miguel Hernández de Elche. Premio UMH 2017 a la Productividad Investigadora, otorgado por el Consejo de Gobierno de la Universidad Miguel Hernández de Elche. Premio «Investigación» en la modalidad de «Jóvenes Investigadores» 2017. Premio UMH al Talento Docente 2017. Premio «Investigación» en la modalidad de «Jóvenes Investigadores» 2016. Premio UMH 2016 a la Productividad Investigadora. Premio a la excelencia en la Práctica Jurídica de ISDE 2016. Premio Joven Investigador por el Consejo Social de la Universidad Miguel Hernández de Elche (XII edición). Premio al profesional de Comercio exterior del año 2016, otorgado por la Asociación Española de Profesionales de Comercio Exterior a las empresas (ACOCEX) y BANKIA. Premio «INSTITUTO VASCO DE DERECHO PROCESAL» en su V Edición (Premio de Artículos Doctrinales sobre el fomento del estudio del Derecho Procesal), en el año 2015. Premio UMH 2015 a la productividad investigadora. Premio UMH 2014 a la productividad investigadora. Premio Santander al mejor Ensayo Corto convocado por la Red Cátedra Santander de Responsabilidad Social Corporativa (Convocatoria 2015). Primer accésit de la XII edición del Premio de Ensayo Breve de la Asociación Castellano-Manchega de Sociología «Fermín Caballero»; V Premio Jurídico Internacional Instituto Superior de Derecho y Economía (ISDE); Accésit en la categoría de «Investigación» de la XVIII edición de los «Premios de Protección de Datos 2014» de la Agencia Española de Protección de Datos. Búho de oro al mejor profesor del Curso 2013/2014 de la Escuela Superior de Marketing (ESUMA). Premio UMH al Talento Docente, años 2014, 2017 y 2019.

Ponente habitual en numerosos cursos organizados en España y en el extranjero en materia de Derecho internacional privado, Derecho de la nacionalidad, Derecho de extranjería, Derecho del comercio internacional, Contratación internacional y Protección de datos de carácter personal, entre otros. Ha dirigido infinidad de TFG y TFM y dos Tesis doctorales.

Autor de diferentes artículos, notas, recensiones y comentarios relacionados con dichas materias publicados en Revistas científicas, técnicas y de divulgación, españolas y extranjeras; **ha participado, como autor, coautor, director y/o coordinador, entre capítulos de libros, libros docentes y/o trabajos de investigación, en más de 225 libros**.

PARTE I

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL: CUESTIONES GENERALES

I. Planteamiento: el crecimiento exponencial, hoy día, de las transferencias internacionales de datos de carácter personal

El crecimiento de los flujos internacionales de información ha multiplicado las solicitudes de autorización de transferencias internacionales de datos de carácter personal: comunicaciones de datos personales entre las filiales de una empresa multinacional, utilización de herramientas multiacceso, prestación de servicios desde distintos países, o la gestión integral de los procesos de recursos humanos de una multinacional, están a la orden del día[1].

El aumento de las transferencias internacionales de datos personales en áreas tales como la de los recursos humanos, los servicios financieros, la banca, la educación, el comercio electrónico, el auxilio judicial internacional o la investigación en el área de la salud son ahora una parte integral de la economía globalizada[2].

En materia de regulación de la protección de datos de carácter personal pueden diferenciarse tres grandes grupos. Un primer grupo formado por los Estados donde existe legislación en materia de protección de datos actual, vigente y adaptada al momento actual (p. ej., sería el caso de los Estados miembros de la Unión Europea (UE), Argentina, México, Canadá o EE.UU.); el segundo grupo, el formado por aquellos países en los que se está trabajando

1 *Vid.*, en particular, Rafael García del Poyo y Francisco Gari, «Régimen jurídico aplicable a las transferencias internacionales y sus implicaciones en la actividad mercantil de las empresas multinacionales», en *Revista Española de Protección de Datos*, núm. 2, Agencia de Protección de Datos de la Comunidad de Madrid-Thomson-Civitas, 2007, pp. 239-266.

2 *Vid.* Juan Manuel Fernández López, «Movimiento internacional de datos y buen gobierno corporativo», en *Boletín del Ilustre Colegio de Abogados de Madrid*, núm. 35, 3.ª ép., febrero 2007, p. 177.

en pro de una legislación en materia de protección de datos (p. ej., en algunos países de la región latinoamericana, como en Perú[3], Ecuador[4], Colombia[5], Chile[6] o Uruguay[7] se están planteando en la actualidad «adaptaciones» de su legislación en materia de protección de datos)[8]; y el tercer grupo es el integrado por aquellos países donde, a día de hoy, la legislación en materia de protección de datos brilla por su ausencia (el caso, p. ej., de países como Rusia, Malasia o Taiwán).

Los principales sectores de actividad en que operan las entidades exportadoras de datos son telecomunicaciones, energía, servicios informáticos, banca, industria química y farmacéutica y publicidad directa. El conjunto de estos factores pone de manifiesto que se están produciendo decisiones empresariales autónomas que llevan consigo un fenómeno de deslocalización de actividades empresariales en estos sectores y países, para las que la obtención de una autorización de transferencia internacional de datos es un elemento instrumental necesario desde el punto de vista legal[9].

En efecto, atendiendo a la modalidad, objeto y destino de las transferencias internacionales de datos autorizadas, destacan tres fenómenos interrelacionados donde debemos extremar la protección tuitiva del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita: 1) que la principal modalidad de transferencia es la que se lleva a cabo entre un responsable ubicado en España,

---

3 *Vid.* Reglamento de la Ley núm. 29733 peruana de «Protección de Datos Personales» (Decreto Supremo núm. 003-2013-JUS), *Diario El Peruano*, Lima, viernes 22/03/2013.

4 *Vid.* Proyecto de Ley sobre «Protección a la Intimidad y a los Datos Personales».

5 *Vid.* Ley Estatutaria núm. 1581, de 17 de octubre de 2012, «por el cual se dictan disposiciones generales para la protección de datos personales».

6 *Vid.* las modificaciones planteadas a la Ley núm. 19628 sobre «Protección a la vida privada o protección de datos de carácter personal», de 28/08/1999.

7 *Vid.* Ley núm. 18331 de «Protección de datos Personales y Acción de "Habeas Data"» de 11/08/2008; y su Decreto regulatorio de 31/08/2009.

8 Si bien los países de América Latina han mirado hacia el modelo europeo, también han mantenido particularidades y motivaciones diferentes a la hora de aprobar su normativa de protección de datos.

9 Las transferencias internacionales de datos responden a diversos objetivos que se pueden diferenciar entre: *a)* Aquellas relacionadas con la gestión empresarial en un contexto global. Las empresas multinacionales requieren la realización de transferencias internacionales de datos para finalidades tales como la gestión, mantenimiento y soporte técnico de los sistemas de información (sobre todo en relación con la gestión eficiente de los recursos humanos, los clientes y los proveedores, así como la prestación de servicios de apoyo administrativo en relación con estos); y *b)* Aquellas relacionadas con la atención telefónica a los clientes y otras acciones de marketing telefónico dirigidas a mejorar el grado de satisfacción de los mismos, como la gestión centralizada de los servicios de atención al cliente. En este grupo destacan principalmente las prestaciones de servicios de atención al cliente o *telemarketing*.

principalmente dedicado a servicios de telecomunicaciones, y una empresa prestadora de servicios en un tercer país (= encargado del tratamiento de datos), al amparo de las cláusulas contractuales tipo previstas en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que sustituyó a la Directiva 95/46/CE (RGPD)[10]; 2) la diversificación de las áreas geográficas a las que se transfiere los datos personales: los EE.UU. siguen siendo el primer importador de datos desde España y los países latinoamericanos se consolidan en segunda posición (principalmente, Chile, Colombia, Perú, Paraguay y Uruguay). Pero han aparecido nuevos países de destino de las transferencias en Asia, destacando India, que en los últimos años ha triplicado el número de expedientes tramitados y tiende a convertirse en uno de los principales importadores de datos personales. También ha aumentado el número de autorizaciones con destino a Marruecos; y, 3) que las transferencias autorizadas corresponden, en un alto porcentaje, a prestaciones de servicios que se realizan en terceros países, lo que es indicativo de la importancia que va adquiriendo la deslocalización de actividades que se externalizan en dichos países[11].

La transferencia internacional de datos de carácter personal merece especial atención tanto desde un punto de vista socioeconómico como jurídico por parte de todas las legislaciones en materia de protección de datos de nuestro entorno; aunque legalmente no se haya conceptuado de forma completa lo que debe entenderse por «transferencia internacional de datos»[12].

---

10 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), disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&qid=1601305740744&from=ES

11 Desde la perspectiva española, las categorías de transferencias internacionales de datos de carácter personal son, en la práctica, de tres tipos: *a)* Transferencias de datos personales derivadas de la optimización de la gestión de recursos por una empresa, cuya matriz, española o central, se halla en un país extranjero; *b)* Transferencias de datos personales ligadas a la naturaleza de la actividad o producto (p. ej., reservas de billetes de avión o de plazas hoteleras en el extranjero contratadas a través de agencias de viajes en España); y, *c)* Transferencias de datos personales destinadas a mejorar el servicio al cliente (p. ej., en los casos en los que se encarga el tratamiento de datos a un tercero en el extranjero, cuya gestión permitirá que el servicio que se presta al cliente sea más eficaz).

12 Se trata de un tema tratado ampliamente por la doctrina más autorizada, nacional y extranjera. *Vid.*, entre otros, Cristina Almuzara Almaida (Coord.) y otros, *Estudio práctico sobre la protección de datos de carácter personal*, 2. ª ed., Lex Nova, Valladolid, 2007, pp. 383-417; Oscar José Álvarez Civantos, *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Comares, Granada, 2001, pp. 88-111; Javier Aparicio Salom, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Elcano (Navarra), 2000, pp. 213-214; Miguel Ángel Davara Rodríguez, (Dir.), *Anuario de Derecho de las Tecnologías de la Información y las Comuni-*

Todos sabemos que el RGPD proporciona distintos mecanismos para la realización de las transferencias de datos desde el Espacio Económico Europeo (EEE) a países terceros, a saber:

- Mediante una decisión de adecuación de la Comisión Europea se puede declarar que un Estado no perteneciente al EEE ofrece un nivel de protección de datos adecuado, lo cual significa que se pueden transferir datos a una entidad de ese Estado no perteneciente al EEE sin que el exportador de los datos deba ofrecer más garantías o esté sujeto a condiciones adicionales. En otras palabras, las transferencias a ese tercer país se asimilarán a una transmisión de datos dentro del EEE.
- A falta de una decisión de adecuación, la transferencia puede hacerse mediante el establecimiento de garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Tales garantías adecuadas incluyen, entre otras:
  - En el caso de los grupos empresariales o la unión de empresas dedicadas a una actividad económica conjunta, que las empresas pueden transferir los datos personales basándose en las denominadas «Normas Corporativas Vinculantes»,
  - Acuerdos contractuales con el destinatario de los datos personales que utilizan, por ejemplo, las cláusulas contractuales tipo aprobadas por la Comisión Europea,

caciones (TIC) 2004, Fundación VODAFONE, Madrid, 2004, pp. 15-27 y 38-56; *Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones (TIC)* 2003, Fundación VODAFONE, Madrid, 2003, pp. 3-21; Gabriel Freixas Gutiérrez, *La protección de los datos de carácter personal en el Derecho español. Aspectos teóricos y prácticos*, Bosch, Barcelona, 2001, pp. 345-356; Ana Garriga Domínguez, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004, pp. 177-181; Vicente Guasch Portas, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, 2014, pp. 46-48; y Ves Poullet, «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid- CIVITAS, Madrid, 2007, pp. 93-113; François Rigaux, «Le régime des données informatisées en droit international privé», en *Journal du droit international*, vol. 113, 1986, pp. 311-328; y, Santiago Ripoll Carulla, «El Movimiento Internacional de Datos en la Ley Española de Protección de Datos», en *Informática y Derecho. Revista Iberoamericana de Derecho Informático*, números 6-7, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura en Mérida, Mérida, 1994, pp. 313-322. *Vid.*, sobre la terminología a utilizar —«transmisión internacional de datos», «flujo internacional De Datos» O «Transferencia Internacional De Datos»—, Joan Piñol i Rull y Olga Estadella Yuste, «La regulación de la transmisión internacional de datos en la L.O. 5/1992 de 29 de octubre», en Santiago Ripoll I Carulla (Coord.), *La protección de los datos personales: regulación nacional e internacional de la seguridad informática*, Universitat Pompeu Fabra, Barcelona, 1993, pp. 78-79.

  - La adhesión a un código de conducta o un mecanismo de certificación junto con compromisos vinculantes y exigibles asumidos por el destinatario en relación con la aplicación de las garantías adecuadas para la protección de los datos transferidos.

- Por último, si se prevé realizar una transferencia de datos personales a un tercer país que no está sujeto a una decisión de adecuación y en ausencia de garantías adecuadas, se puede realizar la transferencia basándose en varias excepciones para situaciones específicas, por ejemplo, cuando una persona haya consentido explícitamente a la transferencia propuesta tras haber recibido toda la información necesaria sobre los riesgos relacionados con dicha transferencia.

Así, p. ej., de los mecanismos mencionados, las normas corporativas vinculantes constituyen el mecanismo frecuentemente utilizado por las empresas para legitimar las transmisiones de datos entre miembros de un mismo grupo empresarial, dado que se encuentran diseñadas para ser una solución global para empresas multinacionales al garantizar que las transferencias intragrupo se realicen en cumplimiento de las normas respectivas. Pues bien, suponiendo que un grupo empresarial cuenta con Normas Corporativas Vinculantes aprobadas por una autoridad de control de un Estado-Miembro, no existen dudas de que se encuentra habilitado para transferir datos de los titulares residentes en el Espacio Económico Europeo a empresas/filiales del mismo grupo en países terceros.

Ahora bien, no podrá transferir datos de residentes en países fuera del Espacio Económico Europeo (EEE) basándose en las mismas Normas Corporativas Vinculantes, puesto que este mecanismo es considerado válido tan solo en países donde el RGPD resulta de aplicación y alguno otro país cuya legislación local también así lo considere (por ejemplo, Argentina[13]). En estos casos, el Delegado de Protección de Datos del grupo deberá, antes de realizar la transferencia, hacer una evaluación de la normativa local para saber qué requisitos existen para la realización de transferencias internaciones. Los requisitos pueden ser bastante dispares dependiendo del país al que queremos realizar la transferencia. A título de ejemplo, en China —a partir de un determinado umbral— se necesita no solo una autorización de la autoridad de control, también se exige además que los datos se encuentren alojados localmente antes de ser transferidos. En Botsuana la autoridad de control acaba de publicar una lista de 45 países para los cuales se pueden transferir datos y queda prohibido realizar transferencias a países que no estén en dicha lista. En definitiva, ante la ausencia de una normativa global, con una autoridad de control única, la casuística es muy amplia y necesariamente hay que consultar la normativa local[14].

13 *Vid.* Resolución N.° 159/2018 de la Agencia de Acceso a la Información Pública.

14 *Vid.* Ortega Giménez, Alfonso, «One World, One Privacy, One Authority», en *LA LEY Privacidad*, número 11, Editorial Wolters Kluwer, Madrid, enero-marzo 2022, pp. 1-4.

II. Concepto de transferencia internacional de datos de carácter personal

La expresión «transferencia internacional de datos»[15] debe considerarse aplicable a todos los flujos de datos a través de las fronteras, independientemente de cuál sea el soporte mediante el que se envían los datos o la forma de tratamiento.

Desde la óptica española vendría a constituir todo tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

La transferencia internacional de datos son flujos de datos personales que se realizan desde un estado miembro del Espacio Económico Europeo a un tercer país no miembro del EEE u organización internacional, ya sea como comunicación de datos personales o en condición de encargado de tratamiento[16].

Varios son, a mi juicio, los elementos a examinar para poder conceptuar una transferencia internacional de datos de carácter personal:

- **Primero**: Debe tratarse de datos de carácter personal, esto es, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
- **Segundo**: Los datos de carácter personal que vayan a transmitirse vienen referidos tanto a aquellos que son tratados de forma automatizada (movimientos realizados por medios informatizados) como a los tratados de forma no automatizada (aquellos realizados por medios convencionales).
- **Tercero**: La transferencia internacional de datos se efectúa con el objeto de realizar un tratamiento de datos de carácter personal por parte del destinatario de los mismos, ya sea tanto cesión (a otro responsable) como prestación de un servicio (encargado de tratamiento).

---

15 *Vid.*, sobre la terminología a utilizar —«transmisión internacional de datos», «flujo internacional de datos», «transferencia internacional de datos», «movimiento internacional de datos», o «flujos de datos transfrontera»—, Joan Piñol i Rull, y Olga Estadella Yuste, «La regulación… *op. cit.*; Emilio Suñé Llinás, «Marco jurídico del tratamiento de datos personales en la Unión Europea y en España», en VV.AA., *La armonización legislativa de la Unión Europea, Dykinson*, Madrid, 1999, pp. 267-269; Miguel Ángel Davara Rodríguez, «La Transferencia Internacional de Datos», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid-Civitas, Madrid, 2007, pp. 23-24; y, Diana Sancho Villa, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010, p. 23.

16 *Vid.*, en sentido amplio Davara Fernández de Marcos, Elena, *Transferencias Internacionales de Datos: Pasado, Presente y Futuro*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2021, pp. 69-70.

- **Cuarto**: El traslado físico efectivo de los datos de carácter personal, de un lugar a otro, a través de las fronteras nacionales, ya sea dentro o fuera de la UE.
- **Quinto**: El lugar de destino de los datos de carácter personal debe encontrarse en un territorio distinto al de origen de los mismos.
- **Sexto**: Existirá transferencia internacional de datos personales en cualquiera de los dos casos siguientes: cuando constituya una cesión o comunicación de datos o cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable.

Con el propósito de seguir ahondando en el concepto de «transferencia internacional de datos» resulta necesario acudir a la jurisprudencia del TJUE; que ha supuesto, en cierto modo, una reformulación del concepto en la Sentencia «Lindqvist».

La STJUE «Lindqvist», de 6 de noviembre de 2003, referente a la publicación de datos personales en Internet. Asunto C-101/01-Bodil Lindqvist[17], al plantearse si la publicación de datos de carácter personal a través de una página web puede considerarse como tal[18]. En opinión del TJUE, el RGPD

17 *Vid*. Joaquín Bayo Delgado, «Derecho comunitario sobre protección de datos», en Carlos Gómez Martínez (Dir.), *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial IX-2004, Consejo General del Poder Judicial, Madrid, 2004, pp. 59-60; Pedro A. de Miguel Asensio, «Avances en la interpretación de la normativa comunitaria sobre protección de datos personales», en *La Ley Unión Europea*, núm. 5964, Madrid, 2003, pp. 1-4; Pedro A. de Miguel Asensio, «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», en http://www.uaipit.com, 2003, pp. 1-12; M.ª Carmen Guerrero Picó, *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 356-361; Manuel Heredero Higueras, «La transmisión internacional de los datos de la salud...», *op. cit.*, pp. 192-195; Manuel Pulido Quecedo, «La catequista y los riesgos de Internet», en *Actualidad Jurídica Aranzadi*, año XIII, núm. 602, 4 de diciembre de 2003, Aranzadi, Cizur Menor (Navarra), pp. 14-15; y, Pedro Serrera Cobos, *Buenas prácticas en protección de datos*, Fundación DINTEL, Madrid, 2007, pp. 28-31; y, sobre la actividad del TJUE en materia de protección de datos de carácter personal, Mónica Arenas Ramiro, «El derecho a la protección de datos personales en la jurisprudencia del TJCE», en Javier Plaza Penadés (Coord.), *Cuestiones actuales de Derecho y Tecnologías de la información y la Comunicación (TICs)*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 95-119.

18 En el Asunto C-101/01-Bodil Lindqvist la Sra. Lindqvist desempeñaba funciones de catequista en la parroquia de la localidad de Alseda, en Suecia. Hizo un curso de informática en el que, entre otras cosas, tenía que crear una página web en Internet. A finales de 1998, la Sra. Lindqvist creó, en su domicilio y con su ordenador personal, varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaran. A petición suya, el administrador del sitio Internet de la Iglesia de Suecia creó un enlace entre las citadas páginas y dicho sitio. Las páginas web de que se trata contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre completo o, en ocasiones, solo su nombre de pila. Además, la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se

no define ni en su artículo 25 ni en ningún otro precepto, ni siquiera en su artículo 2, el concepto de «transferencia a un país tercero». Para determinar si la difusión de datos personales en una página web constituye una «transferencia» de dichos datos a un país tercero en el sentido del artículo 25 de la RGPD por el mero hecho de que resultan accesibles a personas que se encuentran en un país tercero, es necesario tener en cuenta, por una parte, la naturaleza técnica de las operaciones efectuadas y, por otra, el objetivo y la organización sistemática del capítulo IV de la citada Directiva, en el que figura su artículo 25.

En consecuencia, el TJUE responde a la cuestión señalando que no existe una «transferencia a un país tercero de datos» en el sentido del artículo 25 de la RGPD cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por su proveedor de servicios de alojamiento de páginas web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en países terceros. No supone una transferencia a países terceros el hecho de que una persona divulgue datos personales en una página web, que está almacenada en un servidor en la UE, de modo que los datos personales resulten accesibles a nacionales de Estados extracomunitarios[19] —aunque sí constituye en sí mismo un tratamiento de datos conforme a la RGPD—. Para que exista transferencia internacional de datos es fundamental el hecho de que «exista un cierto movimiento de los datos de carácter

mencionaba la situación familiar o el número de teléfono de sus compañeros. Asimismo, señaló que una de sus compañeras se había lesionado un pie y se encontraba en situación de baja parcial por enfermedad. La Sra. Lindqvist no había informado a sus compañeros de la existencia de estas páginas web, no había solicitado su consentimiento, ni tampoco había comunicado su iniciativa a la Datainspektion, organismo público para la protección de los datos transmitidos por vía informática. En cuanto supo que algunos de sus compañeros no apreciaban las páginas web controvertidas, las suprimió. En todo caso, por parte del Ministerio Fiscal se inició un proceso penal contra la Sra. Lindqvist por infracción de la Ley de Protección de Datos sueca (en lo sucesivo, la PUL), solicitándose que fuera condenada por: a) haber tratado datos personales de modo automatizado sin haberlo comunicado previamente por escrito a la Datainspektion (art. 36 de la PUL); b) haber tratado sin autorización datos personales delicados, como los relativos a la lesión en un pie y a la baja parcial por enfermedad (art. 13 de la PUL); y, c) haber transferido datos de carácter personal a países terceros sin autorización (art. 33 de la PUL).

19 La transferencia de datos, internacional o no, se produciría si existiera una transferencia directa entre quien revela los datos y quien los recibe, pero no, en palabras del propio TJUE, cuando «se han transmitido con la ayuda de la infraestructura informática del proveedor de servicios de alojamiento páginas web donde está almacenada la página». Ahora bien, la transmisión del contenido de la página web al proveedor de servicios de alojamiento sí que puede implicar una transferencia internacional de datos, al haber una transferencia directa entre quien revela los datos (el titular de la página web) y quien los recibe (el proveedor de servicios en suyo servidor se aloja esa información), cuando tenga lugar a un país tercero. *Vid.* Pedro A. de Miguel Asensio, «Avances..., *op. cit.*, p. 3-4.

personal», esto es, que el emisor adopte una posición activa y transfiera los mismos; no pudiendo considerar como transferencia el hecho de que, desde un tercer Estado, desde una posición pasiva, se acceda a unos datos colgados en una web[20].

Parece evidente que el TJUE optó por la «solución más fácil»[21] al referirse a qué debemos entender por «transferencia internacional de datos», pues teniendo en cuenta el estado de desarrollo de Internet en el momento de elaboración de la RGPD y la inexistencia de criterios aplicables al uso de Internet, el legislador comunitario no tenía la intención de incluir en el concepto de «transferencia a un país tercero de datos» la difusión de datos en una página web, ni siquiera cuando estos últimos resulten accesibles a personas de países terceros[22].

Por tanto, una transferencia internacional de datos se produce cuando los datos personales que son tratados por un responsable o un encargado del tratamiento en el Espacio Económico Europeo (países de la Unión Europea, Islandia, Liechtenstein y Noruega) son enviados a un tercer país u organización internacional, fuera de dicho territorio. El RGPD no contiene entre sus definiciones la de transferencia internacional de datos, solo la de tratamiento transfronterizo. Define este último como la comunicación o envío de datos cuando se lleva a cabo de principio a fin dentro de las fronteras de la UE (= artículo 4.23) del RGPD). Aplicando el contenido de esta definición y ampliándolo con el del artículo 44 RGPD, podemos extraer que estaremos ante una

---

20 La misma solución plantea Suquet Capdevila en materia de infracciones de derecho de propiedad industrial en Internet. *Vid.* Josep Suquet Capdevila, «Internet, marcas y competencia judicial internacional: ¿O la superación de la regla forum loci delicti commissi? A propósito de la sentencia de la Cour de Cassation de 9 de diciembre de 2003», en La *Ley Unión Europea*, núm. 6073, Madrid, 2004, pp. 1-7; y Palao Moreno respecto de la consideración de la mera accesibilidad de un sitio web desde un determinado Estado como criterio para justificar la competencia de unos determinados tribunales, *vid.* Guillermo Palao Moreno, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», en Javier Plaza Penadés, *Cuestiones actuales de derecho y Tecnologías de la Información y Comunicación (TICs)*, Editorial Aranzadi, Cizur Menor (Navarra), 2006, p. 291.

21 En palabras de Davara Rodríguez, «Concluyente, pero, a nuestro entender, desilusionante». *Vid.* Miguel Ángel Davara Rodríguez, «La Transferencia Internacional…», *op. cit.*, pp. 54-56 (en particular, p. 56); y, según Poullet, «una decisión arriesgada del TJCE», *Vid.* Yves Poullet, «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», en *Revista española de Protección de Datos*, núm. 1, Agencia de Protección de Datos de la Comunidad de Madrid-CIVITAS, Madrid, 2007, pp. 106-108.

22 Como bien señala Pulido Quecedo, «una vez más, el TJUE actúa como instrumento de integración europeo, resaltando, en el presente caso, el carácter de normación completa de la Directiva, y no mínima, que puede ser desarrollada por los Estados miembros. Éstos podrán internamente regular aquellas situaciones no comprendidas en el ámbito de aplicación de esta última y cuando ninguna otra norma de Derecho comunitario se oponga a ello». *Vid.* Manuel Pulido Quecedo, «La catequista y los riesgos de Internet», en *Actualidad Jurídica Aranzadi*, año XIII, núm. 602, 4 de diciembre de 2003, Aranzadi, Cizur Menor (Navarra), p. 15.

transferencia internacional cuando los datos se envíen a terceros países y a organizaciones internacionales. Por su parte, en este contexto son «terceros países» todos aquellos que no conformen el Espacio Económico Europeo[23].

La regulación de las transferencias internacionales en el RGPD parte de un principio general de prohibición: las transferencias de datos personales a terceros países y a organismos internacionales no podrán llevarse a cabo, salvo en caso de cumplirse con las disposiciones incluidas en el RGPD, y siempre que el responsable y encargado del tratamiento cumplan con las condiciones incluidas en el mismo.

III. Sujetos de una transferencia internacional de datos de carácter personal

Analizada desde una perspectiva objetiva, qué es una «transferencia internacional de datos» y cuál es su importancia socioeconómica, ahora vamos a determinar, desde una perspectiva subjetiva, quiénes participan en una transferencia internacional de datos, para comprobar si alguno de los sujetos intervinientes se encuentra o no en una situación de desprotección: el titular de los datos, el exportador y el importador de los datos objeto de una transferencia internacional.

En primer lugar, como sujeto relevante en una transferencia internacional de datos de carácter personal contamos con la persona física titular de los datos que son objeto de una transferencia internacional de datos de carácter personal ilícita. Nos referimos al del titular del derecho fundamental a la protección de datos. Este es uno de los derechos fundamentales que se explicitan con mayor amplitud y que aparece deslindado, con claridad meridiana, de otros como el respeto de la vida privada y familiar (art. 7)[24], en el art. 8[25], de la Carta

23 *Vid.*, en sentido amplio, Ortega Giménez, Alfonso, «Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de datos de la UE», en la *Revista Española de Derecho del Trabajo*, núm. 216/2019, Editorial Aranzadi, Cizur Menor (Navarra), 2019, pp.1-48.

24 El artículo 7 señala que «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones». Los derechos garantizados en el artículo 7 corresponden a los que garantiza el artículo 8 del CEDH. A fin de tener en cuenta la evolución técnica, se ha sustituido la palabra correspondencia por la de «comunicaciones». De conformidad con lo dispuesto en el apartado 3 del artículo 52, este derecho tiene el mismo sentido y alcance que el artículo correspondiente del CEDH.

25 El artículo 8 señala que «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente». Este artículo se basa en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE, así

de los Derechos Fundamentales de la Unión Europea[26]. Así, la privacidad ha entrado en la categoría de los derechos humanos en la medida que garantiza libertades ulteriores como la de obtener trabajo, un crédito o de optar o acceder a determinados servicios: en definitiva, devuelve al individuo (persona física)[27] el control sobre su entorno y garantiza la sostenibilidad del desarrollo[28].

En segundo lugar, debemos referirnos al exportador (o promotor) de datos: persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice una transferencia de datos de carácter personal a un país tercero.

En tercer lugar, se encuentra el importador (o receptor) de datos: persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero. Cuando hablamos de exportador e importador de una transferencia internacional de datos de carácter personal nos estamos refiriendo al responsable y al encargado en el marco de tal transferencia. Se precisa con ello un poco más y «simplemente se crea un subconcepto para referirse con mayor precisión al empresario responsable establecido en la UE que promueve una transferencia internacional a un tercer Estado (que se denomina 'exportador'), dirigida a un empresario receptor establecido en ese lugar (que denominamos 'importador'), con independencia de que este último vaya a actuar como responsable o un encargado»[29].

---

como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El derecho a la protección de los datos de carácter personal se ejerce en las condiciones establecidas por la Directiva antes mencionada y puede limitarse en las condiciones establecidas por el artículo 52 de la Carta. *Vid.* M.ª Carmen Guerrero Picó, *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006, pp. 101-108; y, José Martín y Pérez de Nanclares, «Comentario al artículo 8. Protección de Datos de Carácter Personal», en *Carta de los Derechos Fundamentales de la Unión Europea*, Fundación BBVA, Madrid, 2008, pp. 223-243.

26 *DOUE C* 303, de 14 de diciembre de 2007, y C 83, de 30 de marzo de 2010.

27 Sin embargo, en determinados supuestos también las personas jurídicas, en tanto que destinatarias de las normas en materia de protección de datos, podrían ser titulares del derecho a la protección de datos. *Vid.* en el mismo sentido, José Martín y Pérez De Nanclares, «Comentario…, *op. cit.*, pp. 231-232.

28 Ya la STC 292/2000, de 30 de noviembre, indicaba el objeto y contenido propios del derecho fundamental a la privacidad —derecho fundamental que como tal es inherente a la persona e indisponible—. Protege un conjunto de datos de carácter personal, no necesariamente íntimos o incluso públicos, que, por su capacidad de ser tratados por medios informáticos, arrojan un perfil de la persona, y cuyo uso puede lesionar los derechos de los ciudadanos.

29 Diana Sancho Villa, *Negocios Internacionales de Tratamiento de Datos Personales*, Civitas, Cizur Menor (Navarra), 2010, p. 27.

Uno y otro (exportador e importador de datos) son empresarios que en su establecimiento y en nombre propio recogen, procesan y tratan datos personales que mantienen en ficheros de datos a los efectos de darles un determinado uso y con un objetivo claro: promover una transferencia internacional de datos de carácter personal.

Resulta esencial a los efectos de este estudio identificar y presentar a los diferentes protagonistas de una transferencia internacional de datos si un tratamiento de datos responde a la relación entre el responsable del fichero de datos (persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento), y el encargado de su tratamiento (persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio)[30].

Por otro lado, En toda transferencia internacional de datos las partes pueden ser responsables y/o encargados del tratamiento. Una de ellas estará establecida en el ámbito de la Unión Europea o en el territorio del Espacio Económico Europeo y la otra estará en un tercer país o será una organización internacional.

Las transferencias internacionales de datos pueden consistir tanto en una comunicación de datos personales entre dos responsables del tratamiento, de manera que cada uno de ellos decide sobre el tratamiento de los datos personales, o en el acceso a los datos personales por un encargado del tratamiento para prestar un servicio que implique o consista en el tratamiento de datos personales. Es así que una transferencia internacional de datos puede llevarse a cabo entre: a) dos responsables del tratamiento, uno establecido en el EEE y otro establecido en un tercer país o ser una organización internacional, b) un responsable y un encargado del tratamiento, estando establecido el responsable del tratamiento en el territorio del EEE y el encargado del tratamiento fuera del mismo, o c) dos encargados del tratamiento, al igual que en los casos anteriores, uno en el territorio del EEE y otro fuera del mismo[31].

Por tanto, al igual que en cualquier otro tratamiento de datos personales, aunque no implique una transferencia internacional de datos, esta última puede consistir en una comunicación de datos entre dos responsables del tratamiento o en el acceso a los datos personales por un encargado del tratamiento para prestar un servicio al responsable del tratamiento.

---

30 Ortega Giménez, Alfonso, «La Tramitación Nacional de las Transferencias Internacionales de Datos», en *Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales*, Editorial Wolters Kluwer, Madrid, 2019, pp. 81-84.

31 Doig Yolanda, Fuentes Olga, Ortega Giménez Alfonso, y Turégano Isabel, «Privacy as Data Protection: Some Critical Legal Problems», en *Socialsci Journal*, VOL 2, PURKH, India, 2018, pp. 244-264.

IV. Tipología de transferencias internacionales de datos de carácter personal

Una vez deslindado el objeto de estudio e identificados los sujetos participantes en una transferencia internacional de datos de carácter personal, debemos ocuparnos de los diferentes criterios que existen para clasificar las transferencias internacionales de datos; de forma que podamos, en última instancia, establecer el supuesto tipo a examinar: la situación de desprotección del titular del derecho a la protección de datos ante un tratamiento ilícito internacional de sus datos.

Si bien algunos autores clasifican las transferencias internacionales de datos sobre la base de tan solo un criterio diferenciador: el de los sujetos que realizan la transferencia[32], a mi modo de ver, con el fin de ahondar en la idea de la desprotección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita[33],

32 *Vid.* Sancho Villa distingue entre «transferencias internacionales entre responsables del tratamiento» y «transferencia internacional a un encargado del tratamiento». *Vid.* Diana Sancho Villa, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003, pp. 47-52; Del Peso Navarro y Ramos González, sobre la base de la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección, relativa a las normas por las que se rigen los movimientos internacionales de datos, distingue entre: 1) «transferencias al territorio de Estados que otorguen un nivel adecuado de protección» (norma cuarta); y, 2) «transferencias al territorio de otros Estados no declarados de nivel adecuado» (norma quinta). *Vid.* Emilio del Peso Navarro, y Miguel Ángel Ramos González, *La seguridad de los datos de carácter personal*, 2.ª ed., Díaz de Santos, Madrid, 2002, pp. 112-117; Davara Rodríguez se centra en el país de destino y en la finalidad con que se realiza la transferencia internacional de datos. *Vid.* Miguel Ángel Davara Rodríguez, «La Transferencia Internacional…, *op. cit.*, pp. 27-28; y, De Miguel Asensio la hace en función de si el desplazamiento de datos se realiza a países que proporcionan o no un nivel adecuado de protección. *Vid.* Pedro A. de Miguel Asensio, Nota a la «Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal», en *Anuario de Derecho internacional Privado (2001)*, T I, Iprolex, Madrid, 2001, pp. 626-627.

33 En el marco jurídico actual de la protección de datos, el RGPD se configura como la base del sistema europeo, y por lo tanto se trata de norma de fundamento para las transferencias internacionales. En la medida que el Reglamento tiene carácter de derecho material imperativo —relativo—, lo que unido al alcance espacial del instrumento (artículo 2), su aplicación está garantizada por los tribunales y Autoridades nacionales de control los Estados de la Unión en los litigios que sobre el tratamiento de datos o posibles responsabilidades por su tratamiento inadecuado —bien cuando conozcan de este tipo de demandas, bien cuando tengan que resolver sobre el eventual reconocimiento y ejecución de resoluciones extranjeras o medidas cautelares sobre esta materia—. *Vid.* Ortega Giménez, Alfonso, «Autoridades de control de un Estado miembro y tratamiento transfronterizo de datos, tras la STJUE de 15 de junio de 2021 (Asunto C-645/19)», en *Revista LA LEY Privacidad*, número 9, Editorial Wolters Kluwer, Madrid, julio-septiembre 2021, pp. 1-12.

debemos manejar no solo este sino también otros criterios diferenciadores, siendo estos los siguientes:

a) El del país de destino;

b) El del objeto;

c) El de los sujetos intervinientes; y/o

d) El de la finalidad con que se realiza la transferencia internacional de datos de carácter personal.

IV.1. Atendiendo al criterio del país de destino de la transferencia internacional de datos

Puede tener lugar 1) hacia Estados miembros de la UE o 2) hacia terceros Estados; dentro de estas últimas, hacia Estados que garantizan un «nivel de protección adecuado», hacia Estados que carecen de dicho nivel de protección de datos[34].

Las transferencias a Estados miembros de la UE quedan reguladas por el RGPD. El régimen de transferencia internacional de datos pivota sobre el concepto de «nivel de protección adecuado», que se presume tienen los Estados miembros de la UE[35]. De esta forma, serán las autoridades de los Estados miembros quienes evaluarán, en relación con la transferencia

34 Similar clasificación presenta la Instrucción 1/2000, cuando distingue entre a) «transferencias al territorio de Estados que otorguen un nivel adecuado de protección» (Norma cuarta) y b) «transferencias de datos al territorio de otros Estados» (Norma quinta); y, la LOPDGDD cuando se refiere a «transferencias a Estados que proporcionen un nivel adecuado de protección» (Tít. VI; Cap. II; arts. 67 a 69) y a «transferencias a Estados que no proporcionen un nivel adecuado de protección» (Tít. VI; Cap. III; art. 70). Por su parte, en relación con la transferencia internacional de datos relativos a la salud, Heredero Higueras, se refiere a «transferencias intracomunitarias» —dentro del marco de la UE— y a «transferencias extracomunitarias» —de un país tercero a otro o de un país tercero a un Estado miembro de la UE—. *Vid.* Marta Grande Sanz, «La transferencia internacional de datos personales: presente y futuro», en *Diario La Ley*, n.º 8808, Sección Tribuna, 21 de Julio de 2016; Ref. D-293, Editorial LA LEY; Manuel Heredero Higueras, «La transmisión internacional de los datos de la salud», en Santiago Ripoll Carulla (Ed.), Jordi Bacaria Martrus (Coord.) y otros, *Estudios de protección de datos de carácter personal en el ámbito de la salud*, Agencia Catalana de Protección de Datos, Marcial Pons, Madrid, 2006, pp. 195-211.

35 *Vid.* Ortega Giménez, Alfonso, «El Reglamento General de Protección de Datos de la UE en la empresa: novedades prácticas», en *Diario La Ley*, número 15, Sección Ciberderecho, Editorial Wolters Kluwer, Madrid, 7 de marzo de 2018, pp. 1-28.

o categoría o clase de transferencias, si un tercer Estado ofrece o no un nivel de protección adecuado sobre la base de los criterios que enumera el RGPD[36].

Las transferencias a terceros Estados que garantizan un «nivel de protección adecuado», cuya adecuación hayan sido declaradas por la Comisión Europea. Sobre la base de lo previsto en el Considerando 45 de la RGPD[37], se habilita a la Comisión, para que evalúe si un tercer Estado garantiza dicho «nivel de protección adecuado», obligando a los Estados miembros, si no es el caso, a adoptar «las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate»[38]. Hasta la fecha, solo se consideraran adecuados los regímenes de los Estados miembros del EEE[39] y los afectados por las Decisiones de la Comisión Europea que consideraron adecuado el nivel de protección de datos personales de los siguientes países: países: Suiza[40]; Canadá[41]; Argentina[42]; la Bailía de Guernesey[43]; la Isla de

36 *Vid.* Ortega Giménez, Alfonso, «El impacto de las nuevas tecnologías en el derecho a la protección de datos desde la perspectiva del Derecho Internacional Privado: Redes Sociales de Internet y Cloud Computing», en *Revista Digital Universidad Autónoma de Tabasco*, volumen 6, n.º 11, Artículo Monográfico, México, Julio - diciembre 2018.

37 Al señalar que «por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CE del Consejo».

38 Como bien señala Heredero Higueras, «este es el único contexto para el que la Directiva ha previsto una habilitación del Consejo a favor de la Comisión en materia de ejecución». *Vid.* Manuel Heredero Higueras, *La directiva...*, *op. cit.*, p. 188.

39 El EEE se constituyó por un Acuerdo firmado el 2 de mayo de 1992 (y que entró en vigor el 1 de enero de 1994) entre los Estados miembros de la UE y los seis países que formaban la Asociación Europea de Libre Comercio (AELC), excepto Suiza. Después de la entrada en la UE de tres Estados de la AELC: Austria, Finlandia y Suecia, a comienzos de 1995, e Islandia, Noruega y Liechtenstein, pueden disfrutar de los beneficios del mercado único gracias al Acuerdo de constitución del EEE.

40 Decisiones de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza (*DO* 2000 L 215/1).

41 Decisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *(Personal Information and Electronic Documents Act)* (*DO* 2002 L 2/13).

42 Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (*DO* 2003/490/CE L 168/19).

43 Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernesey (*DO* 2003/821/CE L 308/27).

Man[44]; Jersey[45]; Islas Feroe[46]; Andorra[47]; Israel[48]; Uruguay[49]; Nueva Zelanda[50]; Japón[51], Reino Unido[52], República de Corea[53] y los EE. UU[54].

A falta de decisión de adecuación, con las siguientes garantías:

- Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
- Normas corporativas vinculantes.

---

44 Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man (*DO* 2004/411/CE L 208/47; y corrección de errores en DO L 151, de 30 de abril de 2004).

45 Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey (*DO* L 138/21).

46 Decisión 2010/146/CE de la Comisión, de 5 de marzo de 2010, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre tratamiento de datos personales (*DO* C (2010) 1130).

47 Decisión 2010/625/CE de la Comisión, de 19 de octubre de 2010, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra (*DO* 2010/87/UE).

48 Decisión de la Comisión, de 31 de enero de 2011, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales (*DO* 2011/61/UE).

49 Decisión de ejecución de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental de Uruguay en lo que respecta al tratamiento automatizado d datos personales (*DOUE* 2012/484/UE).

50 Decisión de Ejecución de la Comisión, de 19 de diciembre de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda (*DOUE* núm. 28, de 30 de enero de 2013).

51 Decisión de ejecución (UE) 2019/419 de la Comisión, de 23 de enero de 2019 con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal (*DOUE* núm. L 76/1, de 19 de marzo de 2019).

52 Decisión de ejecución de la Comisión de 28 de junio de 2021, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por parte del Reino Unido.

53 Decisión de Ejecución (UE) 2022/254 de la Comisión, de 17 de diciembre de 2021, con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de la República de Corea en virtud de la Ley sobre la protección de la información personal.

54 Decisión de ejecución de la Comisión de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre UE y los EE.UU.

- Cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2.
- Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión[55] con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2[56].
- Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas. Un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.
- Mecanismos de certificación, aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

No obstante, lo anterior, tanto las normas corporativas vinculantes como las cláusulas tipo adoptadas por una autoridad de control, deben someterse al mecanismo de coherencia del artículo 63 del RGPD (artículo 46 apartado 4 del RGPD).

---

55 Con fecha 4 de junio de 2021, la Comisión Europea ha publicado el nuevo conjunto de cláusulas contractuales tipo que, además de sustituir a sus predecesoras, pretenden poder enmarcar un abanico de transferencias ya sea entre responsable y responsable, entre responsable y encargado, entre encargados o entre encargado y responsable. Las nuevas cláusulas se adaptan al RGPD incorporando los principios de «accountability» y tratan de adoptar los criterios señalados por el Tribunal de Justicia de la Unión Europea (TJUE) en la sentencia del caso *Schrems II*. No obstante, sigue siendo necesario que el exportador, en su caso ayudado por el importador, analice el impacto que la legislación del país del importador pueda tener en el nivel de protección proporcionado, de forma que sea esencialmente equivalente al que proporciona el marco europeo. Además, adicionalmente, deberán tenerse en cuenta las directrices del Comité Europeo de Protección de Datos sobre las medidas suplementarias que se considere adecuado adoptar para garantizar ese nivel de protección equivalente.
Las cláusulas contractuales de las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE quedarán derogadas a partir del 27 de septiembre de 2021. No obstante, los contratos celebrados antes de dicha fecha con arreglo a las anteriores Decisiones serán válidos hasta el 27 de septiembre de 2022, siempre que las operaciones de tratamiento permanezcan inalteradas y las cláusulas contractuales garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas. Los contratos que utilicen las cláusulas contractuales de 2001/497/CE, 2004/915/CE o la Decisión 2010/87/UE tendrán un período de 15 meses para su adaptación a las nuevas cláusulas.

56 Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (*DOUE* núm. L 199/31, de 7 de junio de 2021).

Las transferencias a terceros Estados que no garantizan un «nivel de protección adecuado», pero que bien esté amparada en alguna de las excepciones legalmente previstas, o en alguna de las Decisiones de la Comisión Europea referidas a las cláusulas contractuales tipo, bien que medie autorización de la autoridad de protección de datos del país de origen de la transferencia internacional de datos[57].

El referido Principio de «nivel de protección adecuado» puede ser obviado a tenor de ciertos intereses que deben prevalecer y protegerse. Se trata de intereses jurídicamente protegidos —públicos y privados— que configuran en su haber, y de forma desglosada, una serie de excepciones. Además, existe una excepción al tal Principio que no alude a la defensa de otros intereses jurídicamente protegidos, sino a la presentación de «garantías suficientes» por el responsable del tratamiento de datos de carácter personal.

En este último caso, lo que subyace con la flexibilización de las normas de protección de datos aplicables es la necesidad de eliminar los obstáculos en las relaciones comerciales internacionales existentes entre los Estados miembros de la UE y terceros Estados[58].

Señala la normativa española que no se permiten transferencias de datos a países que no proporcionen un nivel de protección equiparable al que ofrece la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, la LOPDGDD), salvo que el transmitente cumpla lo previsto en la LOPDGDD y el Director de la AEPD autorice la transmisión si se obtienen las garantías adecuadas[59] en esta materia, que operan cuando no existe en el Estado de destino de la transferencia el «nivel de protección adecuado.

---

57 *Vid.*, en sentido amplio, Ortega Giménez, Alfonso, y Gonzalo Doménech, Juan José, «Las transferencias internacionales de datos de carácter personal en el nuevo Reglamento General de Protección de Datos», en *Revista Economist & Jurist*, Número 217, Difusión Jurídica, Barcelona, febrero 2018, pp. 36-43.

58 Una vez que se haya efectuado la evaluación del nivel de protección adecuado del país destinatario de la transferencia de datos de carácter personal se deberá emitir una declaración de que efectivamente existe esa situación. Los instrumentos por los que se puede materializar dicha declaración del nivel de protección adecuado son variados y corresponden a distinta naturaleza: *a)* actos de carácter público —ya sean internacionales (p. ej. las Directrices de la OCDE, de la ONU o del Convenio 108/81/CE), comunitarios (p. ej. las Decisiones de la Comisión Europea) y/o estatales (p. ej. las Autorizaciones emitidas por el Director de la AEPD)—; y *b)* actos de carácter privado (p. ej. a través de los contratos-tipo o de las normas empresariales vinculantes).

59 *Vid.* José M.ª Álvarez-Cienfuegos Suárez, «Notas a la nueva regulación de la protección de datos de carácter personal», en *La Ley*, núm. 5036, 17 de abril de 2000, p. 1716.

En ausencia de decisión adecuada o de garantías adecuadas, si la transferencia cumple alguna de las siguientes condiciones:

- El interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas.
- La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado.
- La transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica.
- La transferencia sea necesaria por razones importantes de interés público.
- La transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones.
- La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.
- La transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero solo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

IV.2. Atendiendo a su objeto

Los criterios por manejar son la modalidad del fichero y la titularidad del mismo. Así, por un lado, en base a la modalidad de fichero de datos personales, existen las transferencias cuyo objeto sean ficheros no automatizados (todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica) o automatizados(todo conjunto organizado de datos de carácter personal que permita acceder a la información relativa a una persona física determinada utilizando procedimientos de búsqueda automatizados)[60], y, por otro, atendiendo a la titularidad del fichero de datos

60 Están claramente incluidos dentro de este concepto los ficheros de datos personales que

personales, podemos diferenciar aquellas referidas a ficheros de titularidad pública, ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos[61].

En este último supuesto, nos referimos a las instituciones autonómicas con funciones análogas a los mismos, en el sentido siguiente: Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público —diferenciándolas de aquellas de titularidad privada (ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos—, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

IV.3. Atendiendo a los sujetos intervinientes

Es posible distinguir entre el «exportador o transmitente» de los datos de carácter personal (persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero) y el «importador o destinatario» de los mismos (persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero). Existen también transferencias internacionales entre responsables del tratamiento de datos personales[62] o entre responsable y encargado del trata-

almacenan la información en soportes informáticos (bases de datos, archivos, carpetas, etc.) y que se encuentran organizados de manera que se pueda acceder a los datos personales utilizando cualquier tipo de aplicación o procedimiento informatizado.

61 Ortega Giménez, Alfonso, Gonzalo Doménech, Juan José «Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea», en *Revista de la Facultad de Derecho*, n.º 44, Universidad de la República, Uruguay, enero-junio 2018, pp. 1-35.

62 El responsable originario del tratamiento de los datos de carácter personal, que tiene la categoría de transmitente de los datos, transfiere dichos datos a otra persona independiente de esta, que tendrá la categoría de destinatario de los datos y que se encuentra ubicado en un Estado distinto, para que efectúe un tratamiento de los datos de carácter personal por su propia cuenta, convirtiéndose, a su vez, en responsable del tratamiento que les dé a esos datos de carácter personal.

miento de datos personales[63], aunque la cesión se realice entre empresas de un mismo grupo[64].

Además, la LOPDGDD se refiere a los supuestos en los que el responsable del tratamiento no esté establecido en territorio de la UE y utilice para el tratamiento medios situados en el territorio español[65], en cuyo caso se le exigirá la designación de un responsable en España[66].

IV.4. Atendiendo a la finalidad o marco jurídico en el que se realizan

Las transferencias internacionales pueden ser contractuales (transmisiones internacionales como consecuencia de relaciones contractuales y comerciales entre empresas con vinculación jurídica o el flujo que se mantiene con fines comerciales), cuando existe un acuerdo previo entre exportador e importador de los datos de carácter personal o no contractuales (realización de un tratamiento ilícito de datos)[67], cuando no existe tal acuerdo.

De entre todos los criterios enunciados, a los efectos del Derecho internacional privado el que nos interesa en este trabajo (la desprotección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita) es el de la finalidad o marco jurídico en el que se realiza la transferencia, lo que nos permite distinguir

63 Es decir, el tratamiento de datos de carácter personal que realiza una persona por el encargo y a cuenta del responsable del tratamiento que se lo ha encomendado.

64 Se considera «transferencia internacional de datos» aunque la cesión se realice entre empresas españolas que, una ubicada en España y otra/s en el extranjero, pero formando parte de un grupo empresarial multinacional y con ocasión de procesos de reorganización en los mismos en el ámbito internacional, pretenden efectuar transferencias de datos que en ocasiones obedecen a la centralización de procesos de gestión y en otras a simples supuestos de utilización compartida de recursos por filiales de distintos países, al hilo de las posibilidades brindadas por las nuevas tecnologías, al tratarse de entidades jurídicas diferentes y, por tanto, de responsables de ficheros de datos diferentes.

65 *Vid.*, en sentido amplio Ortega Giménez, Alfonso, «Título VI. Transferencias internacionales de datos. Arts. 40 a 43», en Ortega Giménez, Alfonso y Arenas Ramiro, Mónica (Dirs.), *Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, Editorial Jurídica Sepín, S.L., Madrid, 2019, pp. 211-216.

66 *Vid.*, en sentido amplio, Ortega Giménez Alfonso, «Título VII. Autoridades de protección de datos. Capítulo I. La Agencia Española de Protección de Datos. Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679. Art. 61», en Ortega Giménez, Alfonso y Arenas Ramiro, Mónica (Dirs.), *Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, Editorial Jurídica Sepín, Madrid, 2019, p. 283.

67 Consecuentemente, existirá daño —y, por tanto, reclamación— si se verifica que se ha producido un tratamiento ilícito de datos de carácter personal.

entre transferencias internacionales de datos contractuales (consensuales) y extracontractuales (no consensuales):

- Las primeras (transferencias internacionales de datos «contractuales») se refieren a aquellos negocios internacionales de tratamiento de datos entre el afectado y el responsable. Es frecuente que la celebración o ejecución de un determinado acuerdo entre un sujeto y un empresario (o entre este y un tercero en interés de aquel) necesite de un tratamiento de sus datos personales. En estos casos, la transferencia internacional de tales datos tiene un carácter accesorio respecto del negocio principal[68]. En otras ocasiones, la transferencia internacional de datos se desarrolla en el marco de un negocio cuyo objeto principal es precisamente esa transmisión: son transmisiones de datos que se producen con carácter principal.
- Junto a estos supuestos, son frecuentes los casos de vulneración del derecho a la protección de datos de afectados por un tratamiento ilícito de datos realizado por un empresario al margen de una relación preexistente entre las partes (transferencias internacionales de datos «extracontractuales»), donde el afectado (perjudicado) plantea una reclamación por daños y perjuicios frente al causante del daño (persona física o jurídica que ha tratado ilegalmente los datos).

Así las cosas, nuestro objeto de estudio se centra en las reclamaciones que tienen fundamento extracontractual, las cuales suelen concluir con una pretensión de satisfacción económica. Por ello se prescinde del análisis de otro tipo de situaciones relacionadas con el flujo transfronterizo de datos personales, tales como las que traen su causa de relaciones contractuales entre perjudicado e infractor, porque ya han sido estudiadas.

Por otra parte, cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en

68 Tal sería el caso, por ejemplo, de la reserva de un billete de avión en una agencia de viajes para la ejecución de un contrato de transporte entre el pasajero y la compañía aérea (que supone el envío de los datos personales del cliente por parte de la agencia a la central de tratamiento en el extranjero), en el marco de un contrato de tarjeta de crédito (pago de las facturas o de las devoluciones de efectivo a los suministradores de bienes y servicios por parte de la entidad emisora), o del supuesto en el que la persona física contrata con una empresa especializada un servicio que implica necesariamente la elaboración de un perfil de solvencia.

la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales.

El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos (artículo 49 del RGPD)[69].

V. Decisiones de aplicación de la comisión relativas a las cláusulas contractuales tipo

Las transferencias internacionales de datos constituyen una transmisión de datos personales desde nuestro país a terceros ubicados fuera del EEE. Dentro del Espacio Económico Europeo se encontrarían todos los países de la Unión Europea y se incluyen a Liechtenstein, Islandia y Noruega. Los responsables y encargados de tratamiento podrían llevar a cabo este tipo de transferencias sin necesidad de una autorización de la autoridad de control bajo los siguientes supuestos:

- Los terceros se encuentren dentro un país que haya sido declarado con un nivel de protección adecuado por la Comisión Europea.
- En caso de no encontrarse entre el listado de países anteriores, para poder transmitir datos personales a otro país deberá ofrecer las garantías adecuadas. Entenderemos como tal disponer de lo siguiente:
  - Un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.
  - Normas corporativas vinculantes.
  - Cláusulas contractuales tipo de protección de datos adoptadas por la Comisión.
  - Cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión.
  - Códigos de conducta, junto con compromisos vinculantes.
  - Mecanismos de certificación.

Respecto a los mecanismos anteriores, destacamos las normas corporativas vinculantes y las cláusulas contractuales tipo. Según el dictamen del

69 *Vid.*, en sentido amplio Ortega Giménez, Alfonso y Heredia Sánchez, Lerdys S., «Tutela Jurisdiccional ante un tratamiento ilícito internacional de datos personales relativos a la salud. Aplicación del Reglamento General de Protección de Datos de la Unión Europea (SP/DOCT/82969)», en VV.AA., *Guía práctica de Protección de Datos en el ámbito sanitario. Comentarios doctrinales, Normativa, Cuadros legislativos y comparativos, Esquemas y Formularios*, Editorial Jurídica Sepin, Madrid, 2019, pp. 123-139.

TJUE «Schrems II» no se podría transferir datos a no ser que contemos con el consentimiento explícito del interesado[70]. Ello supone que, a pesar de que existan estas nuevas cláusulas, las compañías se verán obligadas a analizar la injerencia que puede comportar la transferencia de datos a un tercer país en el que el importador de los datos no pueda garantizar el cumplimiento de las cláusulas tipo suscritas.

Atendiendo a esta inseguridad jurídica, la Comisión Europea ha aprobado dos conjuntos de Decisiones, por un lado, se ha aprobado la Decisión de ejecución relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países[71], y por otro lado, la Decisión de ejecución relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contemplados[72]. Las nuevas cláusulas contractuales tipo entraron en vigor el 27 de junio de 2021, no obstante, será posible seguir utilizando las cláusulas contractuales tipo anteriores durante un periodo transitorio de quince meses posteriores a la entrada en vigor de las nuevas cláusulas contractuales tipo, es decir, hasta el 27 de diciembre de 2022, siempre

70 Recordemos que, en julio del pasado año, el Tribunal de Justicia de la Unión Europea (TJUE) invalidó el acuerdo de protección de datos personales entre la UE y EE.UU. Este acuerdo era conocido como «Escudo de privacidad» o «Privacy Shield». Este «escudo de protección» nació a raíz de la anulación del esquema de transferencias internacionales que se mantuvo en vigor hasta 2015, conocido como «Puerto Seguro» *(Safe Harbor)*. Un mecanismo que permitía a las empresas estadounidenses certificar que cumplían con los estándares europeos en lo referente a la protección de datos personales y facilitar, así, la transferencia de datos a sus servidores y centros en EE.UU. Un acuerdo que fue anulado por el TJUE tras estimar una denuncia del austríaco Maximiliam Schrems, que acusaba a Facebook de ceder los datos de sus usuarios al gobierno y agencias de seguridad americanas sin respetar las garantías y derechos de los ciudadanos europeos. Como alternativa, la Comisión Europea decidió en 2016 aprobar el mencionado Escudo de privacidad. Este mecanismo declaraba válidas las transferencias de datos personales entre ambas potencias siempre y cuando las empresas americanas se acogiesen a este nuevo esquema. Sin embargo, fue el pasado año cuando Europa anuló también este nuevo esquema de transferencias a raíz de una nueva reclamación del austríaco (conocido como caso Schrems II). En ella, Schrems argumentaba que el acuerdo no garantizaba la seguridad y protección de los datos cuando eran transferidos a EE.UU.
Tras la anulación inmediata y sin período de gracia del Escudo de privacidad, las empresas que lo estuviesen utilizando se vieron obligadas a implementar otro sistema. Más información en: https://alcatraz.es/2021/06/08/la-comision-europea-publica-nuevas-clausulas-contractuales-tipo-cct/

71 Decisión de Ejecución (UE) 2021/914, de la Comisión de 4 de junio de 2021, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (*DOUE* núm. 199, de 7 de junio de 2021).

72 Decisión de Ejecución (UE) 2021/915, de la Comisión de 4 de junio de 2021, relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el artículo 28, apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el artículo 29, apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo (*DOUE* núm. 199, de 7 de junio de 2021).

que (i) el tratamiento sujeto a las SCCs no cambie y (ii) sea posible garantizar un nivel adecuado de protección de los datos personales.

Estas nuevas cláusulas contractuales tipo sustituirían a las anteriores de 2001 y 2010 que quedan derogadas, estas constituyeron uno de los mecanismos más comunes para garantizar un nivel adecuado de protección al realizar transferencias internacionales que estaban en proceso de revisión y actualización al ser anteriores a la entrada en vigor del Reglamento General de Protección de Datos. Este proceso de revisión se vio acelerado por la Sentencia «Schrems II» del Tribunal de Justicia de la Unión Europea, que, aunque las considerara válidas, concluía que en algunos casos podían no ser suficientes para garantizar un nivel adecuado de protección[73].

Respecto a sus antecesoras, las nuevas cláusulas contractuales tipo ofrecen un nuevo enfoque modular expandiendo su ámbito de aplicación y adaptándose a una nueva realidad. Así, se distingue los distintos módulos en función de la relación entre el responsable y el encargado de tratamiento en las transferencias:

1. De responsable a responsable.
2. De responsable a encargado.
3. De encargado a encargado.
4. De encargado a responsable.

Atendiendo al tipo de flujo de datos que nos encontramos que la Comisión enumera una serie de aspectos y medidas que deberán detallarse en los contratos. Entre ellas, por ejemplo, nos encontraríamos con las siguientes:

- Limitación de la finalidad.
- Transparencia.
- Exactitud y minimización de datos.
- Limitación del plazo de conservación.

73 Nos encontramos ante un paso más hacia la regularización de las transferencias internacionales de datos, en la que se recogen, nuevas cláusulas contractuales tipo. Las cláusulas contractuales tipo (también conocidas como CCT, por sus siglas) para las transferencias de datos a terceros países, que recogen los nuevos requisitos del Reglamento General de Protección de Datos y que abordan las realidades a las que se enfrentan las empresas. Las principales novedades de las nuevas cláusulas tipo es que se adecuan al Reglamento General de protección de datos (GDPR); incorporan una nueva estructura contractual, de forma que la plantilla o documento, permite distintas opciones en función de la transferencia objeto de regulación como ser: ransferencia de datos de responsable a responsable (Modelo 1); Transferencia de responsable a encargado (Modelo 2); Transferencia de encargado a encargado (Modelo 3);Transferencia de encargado a responsable (Modelo 4). Cada uno de los modelos se estructura siguiendo los principios generales del Reglamento, relativos a la Limitación del tratamiento, Transparencia, Exactitud y Minimización, período de conservación, la expresa mención si son objeto de transferencia datos sensibles y la existencia de sub-encargados. Más información en: https://periscopiofiscalylegal.pwc.es/un-paso-mas-hacia-la-regularizacion-de-las-transferencias-internacionales-de-datos-nuevas-clausulas-contractuales-tipo/

- Seguridad del tratamiento.
- Datos sensibles.
- Transferencias posteriores.
- Documentación y cumplimiento.

V.1. Características principales de las Decisiones relativas a las cláusulas contractuales tipo

La estructura modular de las cláusulas contractuales tipo tiene en cuenta dos escenarios que no se contemplaban con las anteriores (Encargado-Responsable y Encargado-Encargado). De esta manera, las nuevas cláusulas contractuales tipo reflejan mejor la diversidad de escenarios presente en la realidad. Así, las cláusulas contractuales tipo para todos los escenarios se dividen en cuatro secciones diferentes: (i) una primera sección introductoria con cláusulas generales sobre interpretación y jerarquía, (ii) una segunda sección con las obligaciones de las partes, (iii) una tercera sección sobre obligaciones de análisis de normas locales y acceso a datos por parte de las autoridades, y (iv) una cuarta sección con cláusulas finales como pueden ser, la cláusula de ley aplicable o la de jurisdicción.

Asimismo, los escenarios (Responsable-Responsable y Encargado-Responsable) contienen dos anexos sobre características del tratamiento y medidas técnicas y organizativas, mientras que los escenarios (Encargado-Responsable y Encargado-Encargado) contienen un anexo adicional para listar a los subencargados del tratamiento. Adicionalmente, las nuevas cláusulas contractuales tipo contienen toda la información requerida para la contratación de encargados del tratamiento. Por lo tanto, en la medida en la que se aplique, no será necesario firmar un contrato de encargo de tratamiento adicional a las cláusulas contractuales tipo.

Las nuevas cláusulas tipo aprobadas por la Comisión Europea incorporan el principio de *accountability* (responsabilidad proactiva) para adecuarse, como hemos dicho ya, al RGPD. Para ello han incorporado una nueva estructura contractual que ahora permite aplicar diferentes opciones en función de las transferencias de datos que deben regularse, como ser:

- Transferencias de datos de responsables a responsable (módulo 1 de la Directiva 2021/914).
- Transferencias de datos de responsable a encargado (módulo 2 de la Directiva 2021/914).
- Transferencia de datos de encargado a encargado (módulo 3 de la Directiva 2021/914).
- Transferencia de encargado a responsable (módulo 4 de la Directiva 2021/914).

Las Cláusulas contractuales tipo que deben incluirse, con carácter general, y expuestas en el Anexo de la Directiva 2021/914 son las 18 cláusulas relativas a ordenar este nuevo funcionamiento. Además de estas cláusulas, será obligatorio incorporar a modo de anexo de las mismas, la lista de medidas de seguridad que se aplicarán para garantizar la protección de datos personales de los interesados en los terceros países.

a) Función de las cláusulas contractuales tipo

La función de las cláusulas contractuales tipo se limita a asegurar que haya garantías adecuadas de protección de datos en las transferencias internacionales de datos. Por consiguiente, el responsable o el encargado que transfiera los datos personales a un tercer país (exportador de datos) y el responsable o encargado que reciba los datos personales (importador de datos) tienen discrecionalidad para incluir en un contrato más amplio dichas cláusulas contractuales tipo, así como para añadir otras cláusulas o garantías adicionales siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo ni perjudiquen los derechos o libertades fundamentales de los interesados. Se alienta a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas contractuales tipo.

La utilización de las cláusulas contractuales tipo debe entenderse sin perjuicio de las obligaciones contractuales que tengan el exportador y/o el importador de datos de garantizar el respeto de los privilegios e inmunidades que sean de aplicación. Las cláusulas contractuales tipo disponen reglas de responsabilidad entre las partes y con respecto a los interesados, así como reglas de indemnización entre las partes. Cuando el interesado sufra daños materiales o inmateriales como consecuencia de una vulneración de los derechos de tercero beneficiario contemplados en las cláusulas contractuales tipo, debe tener derecho a ser indemnizado. Este derecho debe entenderse sin perjuicio de cualquier responsabilidad que pueda derivarse del Reglamento (UE) 2016/679.

Se considera que las cláusulas contractuales tipo establecidas ofrecen garantías adecuadas en el sentido del artículo 46, apartado 1 y apartado 2, letra c), del Reglamento (UE) 2016/679 para la transferencia de datos personales por parte de un responsable o encargado del tratamiento sujeto a dicho Reglamento (exportador de datos) a un responsable o (sub)encargado cuyo tratamiento de datos no esté sujeto a dicho Reglamento (importador de datos). Dichas cláusulas también establecen los derechos y obligaciones de los responsables y encargados del tratamiento con respecto a las cuestiones a que se refiere el art. 28, apartados 3 y 4, del Reglamento (UE) 2016/679 en lo que respecta a la transferencia de datos personales por parte de un responsable a un encargado, o de un encargado a un subencargado.

b) Los subencargados

Estas nuevas cláusulas establecen los derechos y obligaciones de los responsables y encargados del tratamiento que intervienen en la transferencia. Por parte de un responsable a un encargado, pero también de un encargado a un subencargado para cuando así se dé el caso. En su cláusula 9, se establece como posibilidad que un encargado pueda contar con una autorización para contratar a un subencargado. De esta manera, no sería necesario que el responsable efectúe el contrato con este nuevo tercero.

En caso de transferencia a un importador de datos que actúe como encargado o subencargado, deben aplicarse requisitos específicos de conformidad con el artículo 28, apartado 3, del Reglamento (UE) 2016/679. Las cláusulas contractuales tipo deben exigir al importador de datos que proporcione toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en ellas y permitir y contribuir a las auditorías de sus actividades de tratamiento por parte del exportador de datos. Respecto a la contratación de subencargados por parte del importador de datos, de conformidad con el artículo 28, apartados 2 y 4, del Reglamento (UE) 2016/679, las cláusulas contractuales tipo deben establecer, en particular, el procedimiento de autorización general o específica por parte del exportador de datos, así como exigir que se celebre un contrato por escrito con el subencargado por el que se garantice el mismo nivel de protección que el conferido por las cláusulas.

c) Las transferencias posteriores

Adaptándose a la complejidad de este flujo de datos, se regulan las transferencias posteriores que se deriven de la principal efectuada. Sin embargo, se requiere de una diligencia activa por parte de los intervinientes para asegurar que la continuidad de la protección esté siempre garantizada. Las partes deben poder demostrar el cumplimiento de las cláusulas contractuales tipo. En particular, debe exigirse al importador de datos que conserve la documentación que corresponda para las actividades de tratamiento bajo su responsabilidad y que informe al exportador de datos con presteza en caso de que, por cualquier motivo, no pueda cumplir las cláusulas. A su vez, el exportador de datos debe suspender la transferencia y, en casos especialmente graves, estar facultado para resolver el contrato, en la medida en que se refiera al tratamiento de datos personales en virtud de cláusulas contractuales tipo, cuando el importador de datos infrinja o no pueda cumplir las cláusulas contractuales tipo. Deben aplicarse reglas específicas cuando la normativa doméstica afecte al cumplimiento de las cláusulas. Los datos personales que ya se hubieran transferido antes de la resolución del contrato y cualquier copia de los mismos deben, a elección del exportador de datos, devolverse al exportador de datos o destruirse en su totalidad.

d) Derechos de los interesados y garantías

Destaca el principio de transparencia por el que están compuestos los derechos del interesado. En su cláusula 10 se establece que los titulares de los datos tendrán derecho a solicitar, entre otros:

- Si se están tratando sus datos personales.
- Proporcionar una copia de la información incluida en las cláusulas contractuales suscritas.
- Si los datos han sido o serán transferidos posteriormente.
- Información sobre los destinatarios o categorías de destinatarios a los que se haya realizado o vaya a realizarle la transferencia posterior.
- La finalidad de las transferencias posteriores.

A fin de ofrecer garantías adecuadas, las cláusulas contractuales tipo deben asegurar que los datos personales transferidos con arreglo a ellas gocen de un nivel de protección equivalente en lo esencial al garantizado en la Unión. Con el objetivo de garantizar la transparencia del tratamiento, los interesados deben recibir una copia de las cláusulas contractuales tipo y deben ser informados, en particular, de las categorías de datos personales tratados, del derecho a recibir una copia de las cláusulas contractuales tipo y de cualquier transferencia ulterior. Las transferencias ulteriores por parte del importador de datos a un tercero en otro tercer país solo deben permitirse si dicho tercero se adhiere a las cláusulas contractuales tipo, si la continuidad de la protección está garantizada de otro modo o en situaciones específicas, como, por ejemplo, si media el consentimiento explícito y con conocimiento de causa del interesado.

e) Evaluación y diligencia

La Comisión incide en que corresponde principalmente al exportador y al importador de los datos supervisar en todo momento la transferencia o transferencias realizadas. Ambos deberán cooperar en cualquier procedimiento destinado a garantizar el cumplimiento de las cláusulas suscritas. Ante la transferencia a terceros países, las partes deberán confirmar que no exista un impedimento legal que impida al importador cumplir con sus obligaciones.

Así, las figuras que intervengan analizarán las circunstancias en las que se celebran las transferencias, las distintas leyes y prácticas que puedan afectar en dicho país, las medidas organizativas y técnicas, las medidas de seguridad aplicables, etc. De igual forma, atendiendo a un posible acceso a la información, el importador se compromete a notificar al exportador estas circunstancias. Por ejemplo, si recibe una solicitud jurídicamente vinculante de comunicación de datos personales o si tiene conocimiento que las autoridades públicas han tenido acceso directo a los datos.

f) Medidas técnicas y organizativas

Otra de las novedades es la batería de medidas técnicas y organizativas incluida en el modelo de nuevas cláusulas contractuales tipo. Las plantillas ofrecen una serie de medidas para garantizar la seguridad de los datos, entre las que se incluyen los siguientes ejemplos:

- Seudonimización y cifrado de los datos personales.
- Medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. Incluye una evaluación regular de la eficacia de las medidas.
- Identificación y autorización de usuarios.
- Protección de datos durante la transmisión y almacenamiento de los mismos.
- Medidas para garantizar la seguridad física de los lugares donde se traten los datos, el registro de incidentes y la configuración del sistema.
- De gobernanza y gestión de la informática y la seguridad informática internas.
- Para la certificación / garantía de procesos y productos.
- Medidas para garantizar: la minimización, la calidad, una retención limitada de los datos y la responsabilidad proactiva.
- Medidas para permitir la portabilidad de los datos y garantizar la supresión.

Las compañías deberán actualizar y/o adoptar a la hora de regular las transferencias internacionales de datos las presentes nuevas cláusulas contractuales y, en aquellos casos en los que las mismas pueden no ser suficientes para garantizar la ausencia de injerencia por parte de un gobierno, o el proveedor no sea capaz de garantizar que puede cumplir con las medidas recogidas en las cláusulas tipo, realizar un análisis o evaluación de impacto de la transferencia que se pretende acometer. Dicho análisis debe evaluar los riesgos de privacidad de la transferencia de datos teniendo en cuenta las leyes locales y el marco normativo en materia de protección de datos del país de destino y, en particular, las circunstancias específicas de la transferencia (como el contenido y la duración, la naturaleza de los datos a transferir, el destinatario, la finalidad del tratamiento) y cualquier salvaguarda implementada adicional a las cláusulas (incluidas las técnicas y organizativas pertinentes). Esta evaluación legal debe documentarse y podrá ser exhibida ante la autoridad de control si fuese necesario acreditar la inexistencia de riesgo.

V.2. Derecho aplicable y competencia judicial internacional relativas a las cláusulas contractuales tipo

Con determinadas excepciones y, en particular, en cuanto a determinadas obligaciones que se refieran exclusivamente a la relación entre el exportador y el importador de datos, los interesados deben poder invocar y, en su caso, hacer cumplir las cláusulas contractuales tipo como terceros beneficiarios. Por lo tanto, si bien debe permitirse a las partes elegir el Derecho de uno de los Estados miembros para que rija las cláusulas contractuales tipo, este Derecho debe admitir la existencia de derechos de los terceros beneficiarios. A fin de facilitar el derecho a reparación en casos particulares, las cláusulas contractuales tipo deben exigir al importador de datos que comunique a los interesados los datos de un punto de contacto y que tramite con presteza cualquier reclamación o solicitud. En caso de controversia entre el importador de datos y un interesado que haga valer sus derechos de tercero beneficiario, el interesado debe poder presentar una reclamación ante la autoridad de control competente o ejercitar una acción judicial ante un órgano jurisdiccional competente de la UE.

La transferencia y el tratamiento de datos personales en virtud de cláusulas contractuales tipo no deben producirse si el Derecho y las prácticas del tercer país de destino impiden que el importador de datos cumpla dichas cláusulas. A este respecto, no se considera que se opongan a las cláusulas contractuales tipo la normativa y las prácticas que respeten en lo esencial los derechos y libertades fundamentales y no excedan de lo que es necesario y proporcionado en una sociedad democrática para salvaguardar uno de los objetivos enumerados en el artículo 23, apartado 1 del RGPD. Las partes deben garantizar que, en el momento de someterse a las cláusulas contractuales tipo, no tienen motivos para creer que el Derecho y las prácticas aplicables al importador de datos no se ajustan a estos requisitos.

Con el objetivo de garantizar la eficacia de la ejecución, el importador de datos está obligado a someterse a la competencia de dicha autoridad o dicho órgano jurisdiccional y a comprometerse a acatar la resolución vinculante que se adopte con arreglo al Derecho aplicable del Estado miembro. En particular, el importador de datos se comprometerse a responder a consultas, someterse a auditorías y cumplir las medidas adoptadas por la autoridad de control y, en particular, las medidas correctivas e indemnizatorias. Además, el importador de datos debe tener la opción de brindar a los interesados la posibilidad de acudir a un organismo independiente de resolución de litigios, sin coste alguno. De conformidad con el artículo 80, apartado 1 del RGPD, debe permitirse que los interesados sean representados por asociaciones u otros organismos en litigios contra el importador de datos si así lo desean.

Las cláusulas contractuales tipo disponen reglas de responsabilidad entre las partes y con respecto a los interesados, así como reglas de indemnización

entre las partes. Cuando el interesado sufra daños materiales o inmateriales como consecuencia de una vulneración de los derechos de tercero beneficiario contemplados en las cláusulas contractuales tipo, debe tener derecho a ser indemnizado. Este derecho debe entenderse sin perjuicio de cualquier responsabilidad que pueda derivarse del RGPD.

V.3. Cambios relevantes de las cláusulas contractuales tipo

En cuanto al contenido de las nuevas cláusulas contractuales tipo, destacan las siguientes cláusulas:

- **Cláusula de adhesión**: las nuevas cláusulas contractuales tipo permiten que terceros se adhieran a las partes firmantes, sin necesidad de modificar y firmar unas nuevas cláusulas contractuales tipo. Este mecanismo facilita enormemente la utilización de este mecanismo, por ejemplo, cuando se utilice una gran cantidad de encargados para un mismo tratamiento.
- **Comunicaciones de datos**: la comunicación de los datos sujetos a las cláusulas contractuales tipo a terceros que se encuentren fuera del Espacio Económico Europeo queda prohibida, a menos que (i) se realice a un país del que la Comisión haya emitido una decisión de adecuación, (ii) se garantice un nivel adecuado de protección de los datos a través de otros mecanismos (como podrían ser suscribir las cláusulas contractuales tipo, normas corporativas vinculantes o códigos de conducta), (iii) sea necesario para la formulación, el ejercicio, o la defensa de reclamaciones, o (iv) sea necesario para proteger los interese vitales de los interesados.
- **Información**: en el caso de transferencias internacionales Responsable-Responsable, el responsable del tratamiento al que se le comuniquen los datos y que se encuentre fuera del Espacio Económico Europeo deberá informar sobre (i) su identidad y datos de contacto, (ii) las categorías de datos personales que vaya a tratar, (iii) el derecho a obtener una copia de las cláusulas contractuales tipo firmadas, y (iv) si pretende comunicar los datos a un tercero, las categorías de terceros que accederán a los datos, la finalidad de la comunicación de los datos y la habilitación contractual que le permita comunicar los datos.
- **Identificación de la autoridad competente**: la autoridad de protección de datos del Estado miembro en que tiene su establecimiento el que transfiere datos personales fuera del Espacio Económico Europeo será la competente de supervisar la transferencia. Cuando el que transfiere los datos fuera del Espacio Económico Europeo no tiene su

establecimiento en la Unión Europea, lo será la autoridad de protección de datos del Estado miembro en el que se encuentre su representante.

- **Medidas técnicas y organizativas**: a diferencia de las anteriores cláusulas contractuales tipo, las nuevas incluyen medidas técnicas y organizativas específicas para los cuatro escenarios contemplados. Las anteriores solo incluían una descripción detallada de las medidas técnicas y organizativas para transferencias Responsable-Encargado.
- **Responsabilidad solidaria**: los interesados podrán reclamar ante cualquiera de los involucrados en una transferencia internacional cualquier daño y perjuicio causado por cualquiera de los involucrados en la transferencia internacional, con independencia de que las partes involucradas repitan el daño al verdadero causante.

V.4. Obligaciones para los importadores

Sin embargo, es cierto que hay determinadas disposiciones que aplicarán sea cual sea la relación entre las transferencias, y entre ellas se incluyen los artículos destinados a lidiar con los problemas que conlleva la transferencia internacional de datos personales a países cuyas leyes permiten, sin establecer claros límites a ojos del Tribunal de Justicia, que los poderes públicos accedan a datos personales de residentes de los Estados miembros de la UE.

Uno de estos artículos es el establecido para afrontar el efecto que las leyes locales del importador puedan tener sobre la protección de los datos. Dicho artículo regula la obligación de las partes de garantizar que no tienen motivos para creer que la legislación y las prácticas del tercer país de destino aplicables al tratamiento de los datos personales incluidos los requisitos de divulgación de los datos personales o las medidas que autorizan el acceso de las autoridades públicas impiden al importador de datos cumplir sus obligaciones en virtud de las presentes cláusulas.

Para ello, a las partes se les exige que analicen ciertos elementos, como son las circunstancias específicas de la transferencia, el número de actores involucrados, las transferencias posteriores planeadas, las categorías de receptores, la categoría de datos enviados, la localización del almacenamiento y el sector económico en el que se produce la transferencia. También se les obliga a que tengan en cuenta las leyes del tercer estado, y la práctica de las autoridades públicas en el mismo, para lo cual pueden considerar diferentes elementos como parte de su evaluación, entre los que deben incluir la experiencia práctica pertinente y documentada con casos anteriores de solicitudes de divulgación por parte de las autoridades públicas, o la ausencia de dichas solicitudes, que abarquen un marco temporal suficientemente representativo, si bien no establecer criterios que permitan concretar este margen temporal. Cuando realicen este análisis, las partes deben tener en cuenta

si su experiencia práctica se ve corroborada o contradicha por información fiable, disponible al público, sobre la existencia de solicitudes en el mismo sector, así como la aplicación de la ley en la práctica, la jurisprudencia y los informes de organismos de supervisión independientes. Se obliga al importador a notificar el exportador de datos si, por algún motivo o cambio en la legislación de su país, la situación respecto a la posibilidad de que autoridades públicas accedan a esta información se ha visto incrementada, mientras está en vigor el contrato que permite la transferencia de datos.

Otro de los artículos destinado a regular esta situación, centrado en las obligaciones del importador en caso de acceso a los datos por las autoridades, impone al mismo el deber de comunicar al exportador los requerimientos legales de divulgación de datos personales que haya recibido, siempre que sea legalmente posible o, en caso de que no lo sea, a realizar todos los esfuerzos posibles por obtener una exención a esta prohibición. Además, también deberá, a la hora de recibir una solicitud de acceso a información personal por parte de una autoridad, tener en cuenta la legalidad de la solicitud y de impugnarla en caso de ser posible. Añadido a lo anterior, el importador deberá indicar las medidas técnicas y organizativas que se implementen para garantizar la seguridad de los datos. Entre ellas, se especifica la obligación del importador de conceder a su propio personal solo el acceso a los datos estrictamente necesario para la ejecución del contrato, medida que venía recogida en las recomendaciones emitidas por el Comité Europeo de Protección de Datos (CEPD).

Así mismo, estas cláusulas mantienen la obligación al importador de notificar al exportador cuando el primero dictamine su imposibilidad de cumplir con los requisitos establecidos en estas cláusulas, con la consecuente obligación del exportador de suspender la transferencia de datos, con la excepción de que el exportador establezca las medidas apropiadas (por ejemplo, medidas técnicas u organizativas para garantizar la seguridad y la confidencialidad) que se deban adoptar para hacer frente a la situación.

Por lo tanto, si bien estas nuevas cláusulas actualizan las obligaciones en materia de transferencias internacionales, ampliando las obligaciones tanto de los importadores como exportadores de datos, es cierto que no parece desprenderse de su lectura que las mismas vayan a suponer un verdadero cambio o solución para garantizar la legalidad de las transferencias de datos a los EE.UU., dado que solo recoge algunas obligaciones que ya habían sido incluidas en la recomendaciones emitidas por el CEPD, si bien muchas de ellas siguen estando ausentes en el documento, lo cual no significa que los partes no deban analizar la idoneidad de implementarlas para garantizar la seguridad de la transferencia de datos, en caso de que las partes deseen aplicar de la excepción mencionada en el párrafo anterior.

PARTE II

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL UE-EE.UU.

I. Antecedentes en la regulación de las transferencias internacionales de datos de carácter personal desde la UE a entidades ubicadas en los EE.UU.

La Directiva 95/46/CE supuso el inicio de una disputa entre la UE y los EE.UU., ya que, a los ojos de la Directiva, era posible que las exportaciones de datos de carácter personal a los EE.UU. fueran prohibidas ya que mientras el enfoque de EE.UU. en esta materia se basaba en una mezcla de legislación, reglamentación y autorregulación, la UE consideraba imprescindible la protección del derecho fundamental a la privacidad.

Tras largas negociaciones, el 29 de julio de 2000, la UE y los EE.UU. llegaron a un acuerdo, denominado *Safe Harbour Principles* (Principios de Puerto Seguro) por el que se establecía un sistema para la protección de la vida privada, una auténtica suerte de extensión de la regulación vigente en la UE en materia de protección de datos de carácter personal. Se trataba de un sistema eficaz, tanto desde el punto de vista teórico como desde el punto de vista práctico, ya que posibilita un flujo estable e ininterrumpido de información asegurando un nivel permanente de protección adecuada.

El sistema de Principios de Puerto Seguro, aunque fue criticado en algunas ocasiones, presentaba numerosas ventajas, teniendo en cuenta que: a) constituyó un marco normativo uniforme, permanente, estable y definitivo para la protección del derecho a la intimidad y para la transferencia internacional de

datos de carácter personal entre la UE y los EE.UU.; b) permitió la aprobación automática por todos los Estados miembros de la UE de las transferencias internacionales de datos de carácter personal con destino a los EE.UU.; y, c) sustituyó a las legislaciones internas de cada uno de los Estados miembros de la UE.

La razón de ser de los Principios de Puerto Seguro fue el hecho de que EE.UU. se rige, en numerosos ámbitos, por el principio de autorregulación, en virtud del cual son las propias empresas las que adoptan sus propios códigos de conducta o se acogen a códigos de conducta sectoriales, respecto de los cuales el Estado carece de facultad fiscalizadora o de control alguno. Para suplir esta laguna se crean los principios de *Safe Harbour*, un sistema que trata de conjugar la autorregulación estadounidense con el régimen jurídico comunitario en esta materia.

La empresa que se quería adherir a este Sistema debía presentar una carta de autocertificación ante el Departamento de Comercio, por la que manifestaba su adhesión a los principios y *FAQ*, así como indicando, en particular, los datos de identificación de la entidad solicitante, una descripción de su actividad en lo relativo a la información personal recibida de la UE y una descripción de su política de protección de datos de carácter personal.

El sistema de Principios de Puerto Seguro se configuró, entonces, como un programa voluntario, basado en la autocertificación y en la autoevaluación, que se ofrece a las entidades de los EE.UU. con el fin de obtener, respecto de los datos personales recibidos desde la UE una presunción de adecuación a la protección exigida en el ámbito comunitario, que permite asegurar, de manera permanente, la legitimidad de las transferencias internacionales de datos de carácter personal.

Los Principios de Puerto Seguro, que se configuraron como mínimos para cualquier política privada de protección de datos de carácter personal, fueron los siguientes:

1. **Principio de «Notificación»** ***(Notice)***: establece la obligación que tienen las entidades de informar a los particulares de los fines y utilización de sus datos de carácter personal.
2. **Principio de «Opción»** ***(Choice)***: dispone la obligación de las entidades de ofrecer a los particulares la posibilidad de decidir si sus datos de carácter personal pueden ser o no cedidos a un tercero.
3. **Principio de «Transferencia Ulterior»** ***(Onward Transfer)***: señala que para revelar información a terceros que no participen en el sistema de Puerto Seguro, las entidades deberán aplicar los Principios de notificación y de opción.
4. **Principio de «Seguridad»** ***(Security)***: establece que las entidades que se encargan de la recogida de datos de carácter personal deberán tomar todas las precauciones que estimen oportunas con el fin de evitar su pérdida, modificación o destrucción.

5. **Principio de «Integridad de los datos»** ***(Data Integrity)***: señala que los datos de carácter personal deben ser pertinentes con respecto a los fines con los que se utiliza.
6. **Principio de «Acceso»** ***(Access)***: recoge el derecho de los particulares al conocimiento de sus datos de carácter personal que las entidades tengan sobre ellos y poder corregirla, modificarla o suprimirla en caso de que sea inexacta.
7. **Principio de «Aplicación»** ***(Enforcement)***: dispone la necesidad de incluir una vía de recurso para los interesados que se vean afectados por el incumplimiento de la normativa sobre transferencia internacional de datos de carácter personal entre los EE.UU. y la UE.

Aunque existían toda una serie de excepciones a estos Principios del sistema de Puerto Seguro, cuando era necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley, cuando una disposición legal o resolución jurisdiccional así lo estableciera y/o cuando la Directiva 95/46/CE o cualquier norma de los Estados miembros de la UE lo permitiera; en cumplimiento de la Directiva 95/46/CE, las entidades estadounidenses podían adoptar cualquiera de las siguientes posturas: a) adherirse al sistema de Principios de Puerto Seguro; b) acudir a fórmulas que exonerasen del requisito de la protección adecuada, que recoge el artículo 26 de la Directiva 95/46/CE; o, c) no recibir datos de carácter personal de la UE.

Ante el incumplimiento por parte de las entidades estadounidenses del sistema de Puerto Seguro, cabían dos posibilidades: a) la suspensión de las transferencias de datos de carácter personal hacia una entidad que haya autocertificado su adhesión a los Principios y su aplicación de conformidad con las *FAQ*, con el fin de proteger a los particulares de un «tratamiento fraudulento» de sus datos de carácter personal, o la adopción de cualquier otra medida dentro de sus competencias con el fin de evitar ese «tratamiento fraudulento» de los datos de carácter personal de los particulares; o, b) si se demostrara que un organismo encargado del cumplimiento de los Principios de Puerto Seguro en los EE.UU. no está ejerciendo su función, la Comisión Europea le notificaría al *US Department of Commerce* que tenía intención de adoptar toda una serie de medidas con el objeto de anular, suspender o restringir la transferencia internacional de datos de carácter personal entre los EE.UU. y la UE.

El denominado *Safe Harbour* (Puerto Seguro) por el que se establecía el sistema de Principios de Puerto Seguro para la protección de la vida privada, basado en la voluntaria y libre autocertificación y autoevaluación de las entidades de los EE.UU., tenía como finalidad obtener, respecto de los datos personales recibidos desde la UE una presunción de adecuación a la protección exigida en el ámbito comunitario, que permitiera asegurar, de manera permanente, la legitimidad de las transferencias.

En cuanto al ámbito del Acuerdo UE-EE.UU., es preciso especificar varios extremos: a) si se excluían algunos sectores del ámbito del mecanismo de puerto seguro en virtud de disposiciones especiales (por ejemplo, el sector público) o por la inexistencia de un organismo público de supervisión con responsabilidad para ocuparse de la cuestión; b) si la entidad podría, cuando notificara su adhesión al puerto seguro, excluir algunos sectores de su propia actividad (por ejemplo, los servicios en línea) y cómo se haría pública y se pondría tal exclusión en conocimiento de las autoridades nacionales de control; c) respecto de las transferencias de datos de trabajadores, reforzar el nivel general de protección que brindan los principios o excluir dichos datos del ámbito de aplicación de los acuerdos para proporcionarles mayor protección, en vista asimismo de la inexistencia de un organismo público independiente capaz de ocuparse de este tipo de datos; d) no introducir excepciones a la aplicación de los principios recurriendo a la regulación y sin tomar en la debida cuenta los intereses de la protección de la intimidad.

II. Los principios de *Safe Harbour* o la apuesta por restaurar la confianza en las transferencias internacionales entre los EE.UU. y la UE.: «Scherems I»

Así las cosas, a finales de septiembre de 2013, *Safe Harbour* contaba con 3246 empresas adheridas; un aumento muy significativo si lo comparamos con las 400 empresas que habían en el año 2004. No obstante, la radiografía era inquietante: había una falta de confianza en las transferencias internacionales de datos entre los EE.UU. y la UE. Razones de seguridad nacional no debían poner en tela de juicio el cumplimiento de los Principios de Puerto Seguro. El funcionamiento de los Principios de Puerto Seguro debió seguir basándose en los compromisos y la autocertificación de las empresas que se han adherido. Los Principios de Puerto Seguro debían seguir actuando como un conducto para la transferencia de los datos personales de los ciudadanos de la UE a los EE.UU. y de las empresas estadounidenses a la UE, en vez de transferirlos a las agencias de inteligencia de EE.UU., en virtud de los programas de vigilancia de los EE.UU.

Pero, no fue así: el TJUE declaró inválida la Decisión 2000/520/CE que consideraba que los principios de Puerto Seguro garantizaban un nivel adecuado de protección de los datos transferidos desde la UE a empresas norteamericanas[74]. La sentencia de 6/10/2015 resuelve sobre una cuestión prejudicial

74 *Vid.* Francisca María Roselló Rubert «La transferencia de datos personales entre PYMEs españolas y proveedores norteamericanos de *Cloud Computing* tras la reciente anulación del Acuerdo Safe Harbor por el Tribunal de Justicia de la Unión Europea», en *Diario La Ley*, n.º 8725, Sección Doctrina, 18 de Marzo de 2016; Ref. D-115, Editorial LA LEY.

planteada por la Corte Suprema irlandesa a raíz de un recurso (caso «Scherems I»- *Maximilliam Schrems vs.* Comisionado de Protección de Datos) interpuesto por un nacional austríaco que entendía que la autoridad de control irlandesa debía prohibir a Facebook Ireland transferir los datos personales de sus usuarios a su matriz estadounidense, Facebook, Inc., debido a que el derecho y las prácticas en vigor de los EE.UU. no garantizaban protección suficiente de los datos personales conservados en su territorio contra l vigilancia practicada en él por las autoridades públicas, haciendo referencia a las revelaciones efectuadas por Snowden sobre las prácticas de la Agencia Nacional de Seguridad.

No obstante, el 2 de febrero de 2016, la Comisión Europea y el Gobierno de los EE.UU. alcanzaron un acuerdo político sobre un nuevo marco para los intercambios transatlánticos de datos personales con fines comerciales: el Escudo de la privacidad UE-EE. UU (IP/16/216). La Comisión presentó los textos del proyecto de decisión el 29 de febrero de 2016. Tras el dictamen del Grupo de Trabajo del Artículo 29 (autoridades de protección de datos) de 13 de abril y la Resolución del Parlamento Europeo de 26 de mayo, la Comisión culminó el procedimiento de adopción el 12 de julio de 2016.

El Escudo de la privacidad UE-EE.UU. reflejaba los requisitos establecidos por el TJUE, en su sentencia de 6 de octubre de 2015, en la que declaraba inválido el antiguo marco de «puerto seguro». El Escudo de la privacidad se basaba en los siguientes principios: a) Obligaciones rigurosas para las empresas que trabajan con datos: al amparo del nuevo sistema, el Departamento de Comercio de los EE.UU. llevará a cabo actualizaciones y revisiones periódicas de las empresas participantes, con el fin de garantizar que sigan las normas que ellas mismas han suscrito. Si las empresas no cumplen en la práctica, se enfrentan a sanciones y a ser retiradas de la lista. El endurecimiento de las condiciones para las transferencias ulteriores de datos a terceros garantizará el mismo nivel de protección en caso de transferencia desde una empresa adherida al Escudo de la privacidad; b) Obligaciones en materia de transparencia y salvaguardias claras para el acceso de la administración estadounidense: los EE.UU. han dado a la UE garantías de que el acceso de las autoridades públicas a efectos de aplicación de la ley y de seguridad nacional está sujeto a limitaciones, salvaguardias y mecanismos de supervisión claros. También por primera vez, cualquier persona en la UE tendrá a su disposición vías de recurso en la materia. Los EE.UU. han descartado una vigilancia masiva indiscriminada de los datos personales transferidos hacia ese país en el marco del acuerdo del Escudo de la privacidad UE-EE UU. La Oficina del Director de Inteligencia Nacional explica además que la recopilación en bloque de datos solo podrá utilizarse en condiciones específicas predeterminadas y tiene que ser lo más concreta y precisa posible. Detalla las salvaguardias existentes para la utilización de los datos en esas circunstancias excepcionales. El secretario de Estado estadounidense ha establecido un mecanismo de recurso en el ámbito de la inteligencia nacio-

nal para los europeos a través de la figura del Defensor del Pueblo dentro del Departamento de Estado; c) Protección eficaz de los derechos individuales: cualquier ciudadano que considere que sus datos se han utilizado de forma indebida en el nuevo sistema del Escudo de la privacidad se beneficiarán de varios mecanismos de resolución de litigios accesibles y asequibles. Lo ideal es que las reclamaciones las resuelva la propia empresa; o se ofrecerán gratuitamente mecanismos de resolución alternativa de litigios. Los particulares también podrán dirigirse a sus autoridades nacionales de protección de datos, que colaborarán con la Comisión Federal de Comercio para garantizar que las reclamaciones de los ciudadanos de la UE se investiguen y resuelvan. Si un asunto no se resuelve por un medio u otro, estará previsto, en última instancia, un mecanismo de arbitraje. El mecanismo de recurso en el ámbito de la seguridad nacional para los ciudadanos de la UE será gestionado por un Defensor del pueblo independiente de los servicios de inteligencia de los EE.UU.; y d) Mecanismo de revisión conjunta anual: el mecanismo hará un seguimiento del funcionamiento del Escudo de la privacidad, incluidos los compromisos y garantías en lo que se refiere al acceso a los datos a efectos de aplicación de la ley o de seguridad nacional. La Comisión Europea y el Departamento de Comercio de los EE.UU. llevarán a cabo el examen y asociarán al mismo a expertos nacionales de inteligencia de los EE.UU. y a las autoridades europeas de protección de datos. La Comisión se basará en todas las demás fuentes de información disponibles y presentará un informe público al Parlamento Europeo y al Consejo.

En cuanto a los pronunciamientos contenidos en la STJUE «Schrems I» resulta pertinente la realización de un breve análisis de los antecedentes fácticos y jurídicos que nos llevan a la Sentencia objeto de estudio, constituyendo el punto de partida la reclamación que el Sr. Schrems presentó, en fecha 25 de junio de 2013, ante el Comisario, en la que le solicitaba, en esencia, que prohibiera a Facebook Ireland transferir sus datos personales a los EE.UU., alegando el reclamante que el Derecho y las prácticas en vigor en dicho país no garantizaban una protección suficiente de los datos personales conservados en su territorio frente a las actividades de vigilancia llevadas a cabo, en dicho país, por las autoridades públicas. Esta reclamación fue desestimada basándose en que, en particular, la Comisión había declarado, en su Decisión 2000/520/CE de «Puerto Seguro»[75], que los EE.UU. ofrecían un nivel adecuado de protección.

La High Court (Tribunal Superior, Irlanda), ante la que el Sr. Schrems había interpuesto un recurso contra la desestimación de su reclamación, planteó

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

al TJUE una petición de decisión prejudicial relativa a la interpretación y a la validez de la Decisión 2000/520/CE, que dio lugar a la Sentencia de 6 de octubre de 2015, que se denominará como «Schrems I», en la que el TJUE declaró inválida la referida Decisión[76].Como consecuencia de dicha Sentencia, el órgano jurisdiccional remitente anuló la desestimación de la reclamación del Sr. Schrems, devolviendo la misma al Comisario.

Cabe señalar que, en el marco de la investigación abierta por este último, Facebook Ireland alegó que una gran parte de los datos personales se transfería a Facebook Inc. basándose en cláusulas tipo de protección de datos recogidas en el anexo de la Decisión 2010/87/UE[77], por lo que, teniendo en cuenta todos estos elementos, el Comisario instó al Sr. Schrems a modificar su reclamación.

Atendiendo el requerimiento del Comisario, el Sr. Schrems presentó, el 1 de diciembre de 2015, su reclamación modificada en base a la nuevas circunstancias acaecidas (Sentencia «Schrems I» y alegaciones de Facebook Inc. ante la Comisión, acerca de su actuación conforme a la Decisión 2010/87/UE), alegando, principalmente, que el Derecho estadounidense obliga a Facebook Inc. a poner los datos personales que se le transfieren a disposición de las autoridades estadounidenses, como la National Security Agency (NSA) y la Federal Bureau of Investigation (FBI). La reclamación modificada afirmaba, además, que, al utilizarse esos datos en el marco de diferentes programas de vigilancia, de una manera incompatible con los artículos 7, 8 y 47 de la Carta[78] (que reconocen, respectivamente, el derecho a la vida privada y fami-

76 Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Schrems, C-362/14.

77 2010/87/UE: Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

78 *Carta de los Derechos Fundamentales de la Unión Europea*. Artículo 7: «Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.» Artículo 8: «Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente» Artículo 47: «Derecho a la tutela judicial efectiva y a un juez imparcial. 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 el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia».

liar, el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva, y a un juez imparcial para la obtención de la tutela de los derechos y libertades reconocidos en el marco de la Unión Europea), la Decisión 2010/87/UE no puede justificar la transferencia de esos datos a los EE.UU. en base a las cláusulas tipo de protección de datos que se recogen en la misma. Teniendo en cuenta estos argumentos, el Sr. Schrems solicitó al Comisario que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.

Con posterioridad a la presentación de la reclamación modificada por el Sr. Schrems, el 24 de mayo de 2016, el Comisario publicó un «proyecto de decisión» en el que se resumían las conclusiones provisionales de su investigación. En dicho proyecto, consideró con carácter provisional que los datos personales de ciudadanos de la Unión Europea transferidos a EE.UU. corrían el riesgo de ser consultados y tratados por las autoridades estadounidenses de una manera incompatible con los artículos 7 y 8 de la Carta y que el Derecho estadounidense no ofrece a esos ciudadanos vías de recurso compatibles con el artículo 47 de la Carta. El Comisario estimó que las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT no subsanan esa deficiencia, en la medida en que solo confieren a los interesados derechos contractuales contra el exportador o el importador de los datos, sin vincular a las autoridades estadounidenses.

De esta forma, al considerar que, en esas circunstancias, la reclamación modificada del Sr. Schrems planteaba la cuestión de la validez de la Decisión 2010/87/UE relativa a cláusulas contractuales tipo, el 31 de mayo de 2016, el Comisario inició un procedimiento ante la High Court (Tribunal Superior), apoyándose en la jurisprudencia resultante de la sentencia «Schrems I», de 6 de octubre de 2015, apartado 65, a efectos de que esta última pregunte al TJUE acerca de esta cuestión. Mediante resolución de 4 de mayo de 2018, la High Court (Tribunal Superior) planteó la petición de decisión prejudicial ante el TJUE que, finalmente, se resuelve por la Sentencia «Schrems II».

Es conveniente resaltar que, durante todo este *iter* procedimental se producen dos hechos que constituyen antecedentes a tener en cuenta. La primera de las circunstancias ocurridas durante toda la tramitación someramente reproducida es que, con posterioridad a la declaración de invalidez de la Decisión «Puerto seguro», por la Sentencia «Schrems I», la Comisión adoptó la Decisión «Escudo de Privacidad»[79] que tenía como vocación ocupar el vacío dejado por la declaración de invalidez contenida en la referida Sentencia, constituyendo su validez, como se verá, uno de los puntos fundamentales de la Sentencia que es objeto de análisis en el presente estudio. La segunda de estas circunstancias con cierta relevancia para el análisis de

79 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 Privacidad UE-EE.UU. (*DO* 2016, L 207, p. 1).

la cuestión objeto del presente trabajo, es la entrada en vigor del RGPD, que sustituyó a la Directiva 95/46/CE, manteniendo, no obstante, en lo sustancial, la regulación contenida en esta sobre la transferencia de datos personales a terceros países extracomunitarios.

Con respecto a esta última circunstancia, considera el Tribunal que aunque las cuestiones prejudiciales planteadas se refieren a las disposiciones de la Directiva 95/46/CE, deberán responderse en base al RGPD, ya que el Comisario aún no había adoptado una decisión final sobre esa reclamación cuando la Directiva fue derogada y sustituida por el RGPD, con efecto a partir del 25 de mayo de 2018, por lo que es esta norma, y no la Directiva derogada, la que toma en consideración el Tribunal para la resolución de las cuestiones prejudiciales planteadas.

III. Un nuevo esfuerzo (baldío) por restaurar la confianza en las transferencias internacionales entre los EE.UU. y la UE.: «Scherems II»

La STJUE, de 16 de julio de 2020, dictada en el Asunto C-311/18, (en adelante, Sentencia «Schrems II») constituye un hito esencial en una sucesión de hechos relacionados con una de las cuestiones que mayor debate ha generado en los últimos años en materia de protección de datos, como es la transferencia de datos personales protegidos por el Derecho de la Unión a terceros países extracomunitarios, especialmente, a los EE.UU. de América.

Se trata de una cuestión cuya suma importancia resulta comprensible en un mundo en el que la globalización alcanza su máximo exponente en el campo de los datos personales protegidos, principalmente, debido a la existencia de redes sociales u otras plataformas digitales que operan a nivel mundial tratando datos personales protegidos de sus usuarios que, en muchos casos, se refieren a la esfera más íntima de su privacidad.

Esta situación es de enorme importancia por cuanto que, de no establecerse los adecuados criterios de control del respeto a la normativa comunitaria en materia de protección de datos de carácter personal, en este tipo de transferencias a terceros países extracomunitarios, nos encontraríamos con que la protección de datos de carácter personal quedarían limitados a un ámbito territorial relativamente reducido, con lo que los ciudadanos de la Unión Europea estarían desprotegidos en multitud de ocasiones en los que sus datos personales serán tratados en países ajenos al territorio comunitario.

Es por ello por lo que, la normativa comunitaria de protección de datos de carácter personal, representada en la actualidad por el RGPD establece unos criterios reguladores de dichas transferencias a países extracomunitarios, con la evidente finalidad de mantener, aún en estos casos, el debido nivel de protección de los datos de carácter personal de los ciudadanos de la Unión.

De esta forma, a grandes rasgos, el RGPD establece un mecanismo de protección que se configura en tres niveles, debiendo considerarse, en primer lugar, lo establecido en su artículo 45[80], que regula la emisión de Decisiones

80 Artículo 45 del RGPD: «Transferencias basadas en una decisión de adecuación. 1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica. 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales. 3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2. 4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE. 5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2. Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a

de Adecuación por parte de la Comisión; en segundo lugar, lo dispuesto por su artículo 46, que establece un sistema de garantías sostenido, principalmente, por las normas corporativas vinculantes y las cláusulas tipo de protección de datos. Por último, lo dispuesto en su artículo 49 que, en defecto de los mecanismos dispuestos en los anteriores preceptos, establece una serie de supuestos relacionados taxativamente, en los que pueden realizarse transferencias de datos a terceros países comunitarios, que descansan, en general, en el expreso consentimiento del interesado, previa advertencia de los riesgos de la transferencia de sus datos, así como en razones de interés general que, en cualquier caso, deberán respetar las garantías del derecho Comunitario.

Teniendo en cuenta lo anterior, la Sentencia «Schrems II» es de enorme importancia por cuanto que, a pesar de referirse a las transferencias de datos personales protegidos a los EE.UU., establece con nitidez los parámetros que deberán ser tenidos en cuenta para las transferencias de datos a terceros países extracomunitarios, definiendo con claridad conceptos esenciales como es el nivel de protección adecuado de los datos personales que ha de ser tomado en consideración, o las obligaciones y facultades, tanto de las autoridades públicas de control, como de todos los sujetos implicados en la transferencia y tratamiento de datos personales protegidos con destino a terceros países extracomunitarios.

Por esta razón, a pesar de que el objeto y alcance de la Sentencia «Schrems II» puede parecer limitado al caso de los EE.UU., lo cierto es que la misma ha marcado un antes y un después en las transferencias extracomunitarias de datos de carácter personal al definir elementos esenciales para garantizar que los derechos de los ciudadanos de la Unión Europea, afectados por estas transferencias, no quedan desprotegidos.

Estamos ante una cuestión enormemente importante, que hará correr ríos de tinta, por lo que, es evidente que, no llegaremos a alcanzar, en el presente trabajo, todas las implicaciones y matices que tiene la Sentencia. Sin perjuicio de ello, no cabe duda del interés jurídico del presente estudio, en el que

---

que se refiere el artículo 93, apartado 3. 6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5. 7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49. 8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado. 9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo».

se partirá de un breve relato de los antecedentes que nos han conducido a este hito, concretando el objeto de la cuestión prejudicial planteada, para llegar al concreto análisis de la decisión que, el TJUE, ha alcanzado con respecto a cada una de estas cuestiones controvertidas.

Aunque el órgano judicial nacional formula un total de once cuestiones prejudiciales, el Tribunal agrupa sistemáticamente las mismas de manera que el objeto de decisión se reduce a cinco cuestiones que se relacionarán a continuación.

La primera cuestión prejudicial, tiene como objeto la determinación de la inclusión dentro del ámbito de aplicación del RGPD de las transferencias de datos personales realizada por un operador económico establecido en un Estado miembro, a otro operador económico establecido en un país tercero cuando, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades de ese país tercero con fines de seguridad nacional, defensa y seguridad del Estado.

El segundo grupo sistemático de la reclamación prejudicial formulada, en el que el Tribunal incluye las cuestiones prejudiciales segunda, tercera y sexta, es de suma importancia, por cuanto que se traduce en la delimitación de los elementos que han de tomarse en consideración a efectos de determinar si ese nivel de protección está garantizado en el contexto de una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos.

En tercer lugar, el TJUE se pronuncia sobre la cuestión prejudicial octava, que se refiere a la determinación de las facultades de las autoridades de control competentes y, concretamente, a si estas están obligadas a suspender o prohibir una transferencia de datos personales a un país tercero, que esté basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando por parte de la correspondiente autoridad de control se considera que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero.

El cuarto grupo sistemático objeto de resolución por la STJUE «Schrems II» comprende las cuestiones prejudiciales séptima y undécima, concretándose en el análisis de la validez de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo, bajo el prisma de la Carta de Derechos Fundamentales de la UE.

En quinto y último lugar, se valoran por el Tribunal, de forma conjunta, las cuestiones prejudiciales cuarta, quinta, novena y décima que, en suma, se refieren a una cuestión de vital importancia como es la validez de la Decisión «Escudo de Privacidad», así como el grado de garantía de la tutela judicial efectiva que, para los ciudadanos de la UE, ofrece la figura del Defensor del Pueblo mencionado en el Anexo III de la referida Decisión.

IV. La sentencia «Schrems II»

IV.1. Sobre el ámbito de aplicación del RGPD

Como se ha expuesto, el objeto de la primera cuestión prejudicial se concreta en la inclusión, dentro del ámbito de aplicación del RGPD de una transferencia de datos personales realizada por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero cuando, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades de ese país tercero con fines de seguridad nacional, defensa y seguridad del Estado.

El Tribunal resuelve esta cuestión considerando que este tipo de transferencias se encuentran dentro del ámbito de aplicación del RGPD, tras un acertado análisis del ámbito de aplicación del mismo, conforme a lo dispuesto en su artículo 2, apartado 1, que establece que el RGPD se aplica al tratamiento total, o parcialmente automatizado, de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Toma en consideración, también, el Tribunal la definición que el artículo 4, punto 2 del RGPD, realiza del concepto de «tratamiento» como «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no», así como los ejemplos que, de dicho concepto, se citan en el referido precepto, como es la «comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso», debiendo tenerse en cuenta, además, a juicio del Tribunal, que el referido RGPD aplica, a las transferencias de datos personales a países terceros, normas particulares recogidas en su capítulo V, titulado «Transferencias de datos personales a terceros países u organizaciones internacionales», y confiere a las autoridades de control poderes específicos a ese efecto, que se recogen en el artículo 58[81], apartado 2, letra j), del RGPD.

No existiendo dudas con respecto a que el RGPD se aplica a las transferencias de datos personales a países terceros extracomunitarios, pasa el Tribunal a analizar si, el supuesto de hecho de la cuestión prejudicial planteada resulta incardinable a alguna de las excepciones que establece el Reglamento en cuanto a su ámbito de aplicación establecidas en el artículo 2[82],

81 Artículo 58, apartado 2, letra j) del RGPD: «Poderes. Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional».

82 Artículo 2, apartado 2 del RGPD: «Ámbito de aplicación material 2. El presente Reglamento no se aplica al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio

apartado 2 del RGPD que, como recuerda el TJUE, deben interpretarse en sentido estricto[83].

Así las cosas, el Tribunal concluye que, en el caso de autos, al haber sido realizada la transferencia de datos personales que es objeto del litigio principal, por Facebook Ireland hacia Facebook Inc., es decir, entre dos personas jurídicas, dicha transferencia no está comprendida dentro del ámbito del artículo 2, apartado 2, letra c) del RGPD, que tiene por objeto el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. A la referida transferencia tampoco pueden aplicársele las excepciones recogidas en el artículo 2[84], apartado 2, letras a), b) y d), del antedicho Reglamento, ya que las actividades que allí se enumeran a título de ejemplo son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares.

Por todo ello concluye el Tribunal, con respecto a la primera de las cuestiones prejudiciales planteadas, que la posibilidad de que los datos personales transferidos entre dos operadores económicos con fines comerciales sean objeto, en el transcurso de la transferencia o tras ella, de un tratamiento con fines de seguridad pública, defensa o seguridad del Estado por parte de las autoridades del país tercero de que se trate, no puede excluir a la referida transferencia del ámbito de aplicación del RGPD.

IV.2. Sobre el nivel de protección adecuado para la transferencia de datos a terceros países

Como se ha avanzado, el segundo grupo de cuestiones analizadas por el TJUE, se centra en la delimitación de los elementos que han de tomarse en consideración a efectos de determinar si ese nivel de protección está garan-

---

de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención».

83 *Vid.* en lo que se refiere al artículo 3, apartado 2, de la Directiva 95/46/CE, la sentencia de 10 de julio de 2018, Jehovan todistajat, C 25/17, EU:C:2018:551, apartado 37 y jurisprudencia citada).

84 Artículo 2, apartado 2, letras a), b) y d) del RGPD: «Ámbito de aplicación material: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención».

tizado en el contexto de una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos.

En relación con esta cuestión, analiza el TJUE, en primer lugar, lo dispuesto por el artículo 46[85], apartados 1 y 2, letra c) del RGPD, tras una lectura conjunta de esas disposiciones, concluyendo que, cuando no existe una decisión de adecuación adoptada en virtud del artículo 45[86], apartado 3, del referido Reglamento, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país si hubiera ofrecido «garantías adecuadas», siempre que se cumpla la condición de que los interesados cuenten «con derechos exigibles y acciones legales efectivas», pudiendo proporcionarse esas garantías adecuadas, en particular, mediante cláusulas tipo de protección de datos adoptadas por la Comisión.

Afirma el Tribunal que el artículo 45[87], apartado 1, primera frase del RGPD establece que podrá autorizarse una transferencia de datos personales a un tercer país mediante una decisión adoptada por la Comisión, conforme a la cual se atestigua que ese tercer país, un territorio o uno o varios sectores específicos de ese tercer país garantizan un nivel de protección adecuado. A este respecto, sin exigir que el país tercero de que se trate garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión Europea, debe entenderse que la expresión «nivel de protección adecuado»,

---

85 Artículo 46, apartados 1 y 2, letra c) del RGPD: «Transferencias mediante garantías adecuadas 1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. 2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por: c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2».

86 Artículo 45, apartado 3 del RGPD: «Transferencias basadas en una decisión de adecuación. 3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2».

87 Artículo 45, apartado 1 del RGPD: «Transferencias basadas en una decisión de adecuación 1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica».

tal como queda confirmado en el considerando 104 del referido Reglamento, exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y de los derechos fundamentales sustancialmente equivalente al garantizado en la Unión Europea en virtud del antedicho Reglamento, interpretado a la luz de la Carta. En efecto, a falta de esa exigencia, el objetivo mencionado en el anterior apartado se frustraría[88].

En este sentido, concluye el Tribunal que las garantías adecuadas deben asegurar que las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gocen, como en el marco de una transferencia basada en una decisión de adecuación, de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión.

En relación con el marco sobre el que ha de interpretarse el alcance del nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea, analiza el Tribunal si el análisis del nivel de protección debía determinarse a la luz del Derecho de la Unión, en particular, de los derechos garantizados por la Carta y/o a la luz de los derechos fundamentales reconocidos en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, o también a la luz del Derecho nacional de los Estados miembros. Con respecto a esta cuestión, concluye el Tribunal que el nivel de protección de los derechos fundamentales exigido en el artículo 46, apartado 1, del antedicho Reglamento debe determinarse sobre la base de las disposiciones del mismo Reglamento, interpretadas a la luz de los derechos fundamentales garantizados por la Carta.

Por último, determina el Tribunal los elementos que han de tomarse en consideración para determinar la adecuación del nivel de protección en el contexto de una transferencia de datos personales a un país tercero sobre la base de las cláusulas tipo de protección de datos adoptadas en virtud del artículo 46, apartado 2, letra c) del RGPD, respondiendo el Tribunal que han de tenerse en cuenta, por una parte, las estipulaciones contractuales objeto de acuerdo entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate y, por otra parte, en lo que respecta al hipotético acceso de las autoridades públicas del país tercero, a los datos personales transferidos, se han de tener en cuenta los elementos mencionados, de modo no exhaustivo, en el artículo 45, apartado 2 del RGPD, que precisa que los interesados deben gozar de garantías adecuadas y contar con derechos exigibles y acciones legales efectivas.

88 *Vid.*, en lo que respecta al artículo 25, apartado 6, de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C 362/14, EU:C:2015:650, apartado 73.

Por tanto, teniendo en cuenta todo lo anterior, el Tribunal interpreta el nivel de protección adecuado para la transferencia de datos a terceros países en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45[89], apartado 2 del RGPD.

IV.3. Sobre las obligaciones de control de las autoridades

Como se ha visto, el TJUE analiza, de forma independiente, la cuestión prejudicial octava, que se refiere a la determinación de las facultades de las autoridades de control competentes y, concretamente, a si estas están obligadas a suspender o prohibir una transferencia de datos personales a un

89 Artículo 45, apartado 2 del RGPD: «Transferencias basadas en una decisión de adecuación. 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales».

país tercero, basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando por parte de la correspondiente autoridad de control se considera que dichas cláusulas no se respetan, o no pueden respetarse en ese país tercero, así como que la protección de los datos transferidos exigida por el Derecho de la Unión Europea, en particular, por los artículos 45 y 46 del RGPD y por la Carta, no puede garantizarse, o si, por el contrario, el ejercicio de esas facultades de suspensión o prohibición de las transferencias están limitadas a supuestos excepcionales[90].

Esta cuestión prejudicial es resuelta por el mencionado Tribunal en el sentido de considerar dos escenarios diferentes dependiendo de la existencia o no de una decisión de adecuación dictada por la Comisión. En el caso de que exista una decisión de adecuación, y mientras que la misma no haya sido objeto de invalidación por el TJUE, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciará con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado ni, por consiguiente, suspender o prohibir transferencias de datos personales a ese tercer país.

No obstante, aclara el Tribunal que incluso habiendo adoptado la Comisión una decisión de adecuación, la autoridad nacional de control competente, a la que una persona haya presentado una reclamación para proteger sus derechos y libertades frente al tratamiento de datos personales que la conciernen, debe poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por el RGPD y, en su caso, interponer un recurso ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de adecuación, planteen al TJUE una cuestión prejudicial sobre esta validez[91].

Por el contrario, en el caso de que no exista una decisión de adecuación emitida por la Comisión, el Tribunal resuelve que la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando esa autoridad de control considera, a la luz de todas las circunstancias específicas de la referida transferencia, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión Europea,

90 *Vid.*, en relación con la traslación de la responsabilidad hacia el responsable del tratamiento, Rodríguez Ayuso, Juan Francisco, «Anulación del Privacy Shield en las transferecnias internacionales de datos: ¿presenciamos un desplazamiento fáctico de la responsabilidad?», en *Revista Boliviana de Derecho*, n.º 31, enero 2021, pp. 426-503.

91 *Vid.*, en lo que respecta al artículo 25, apartado 6, y al artículo 28 de la Directiva 95/46/CE, la sentencia de 6 de octubre de 2015, Schrems, C 362/14, EU:C:2015:650, apartado 57 y 65.

en particular, por los artículos 45 y 46[92] del RGPD y por la Carta, no puede garantizarse mediante otros medios, en especial si el responsable o el encargado del tratamiento establecidos en la Unión Europea no han suspendido la transferencia o puesto fin a esta por sí mismos.

IV.4. Sobre la validez de la Decisión 2010/87/UE

Como se ha señalado, el cuarto grupo sistemático objeto de resolución por la Sentencia «Schrems II» comprende las cuestiones prejudiciales séptima y undécima que, en esencia, tratan sobre el análisis de la validez de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo bajo el prisma de la Carta de Derechos Fundamentales de la Unión Europea.

El TJUE hace depender la validez de la Decisión 2010/87/UE a si, de conformidad con la exigencia resultante de los artículos 46, apartado 1 y 2, letra

92 Artículo 46 del RGPD: «Transferencias mediante garantías adecuadas. 1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. 2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por: a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; b) normas corporativas vinculantes de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2; e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados. 3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante: a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. 4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo. 5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo».

c), del RGPD, interpretados a la luz de los artículos 7, 8 y 47 de la Carta[93], tal decisión incluye mecanismos efectivos que permitan, en la práctica, garantizar que el nivel de protección exigido por el Derecho de la Unión Europea sea respetado, así como que las transferencias de datos personales basadas en esas cláusulas sean suspendidas o prohibidas en caso de violación de dichas cláusulas, o de que resulte imposible su cumplimiento.

El referido Tribunal analiza los concretos mecanismos efectivos de protección de datos que se recogen en el anexo de la Decisión 2010/87/UE concluyendo que, de las cláusulas 4, letras a) y b), 5, letra a), 9 y 11, apartado 1, de dicho anexo se desprende que el responsable del tratamiento establecido en la Unión Europea, el destinatario de la transferencia de datos personales y el eventual encargado de este último, se comprometen mutuamente a que el tratamiento de esos datos, incluida su transferencia, ha sido efectuado y seguirá efectuándose de conformidad con la legislación de protección de datos aplicable, que, conforme al artículo 3, letra f) de la antedicha Decisión se corresponde con la legislación que protege los derechos y libertades fundamentales de las personas y, en particular, su derecho a la vida privada respecto del tratamiento de los datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos.

Asimismo, se analizan por el TJUE las obligaciones del destinatario de la transferencia de datos personales establecido en un país tercero, que se concretan en una información inmediata, al responsable del tratamiento establecido en la Unión Europea, de su eventual incapacidad para cumplir con las obligaciones que le incumben con arreglo al contrato celebrado, teniendo la posibilidad, en este caso, el responsable del tratamiento establecido de suspender la transferencia de los datos o rescindir el contrato interpretando el TJUE que esta facultad es obligatoria para el responsable del tratamiento

93 *Carta de los Derechos Fundamentales de la Unión Europea*. Artículo 7: «Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.» Artículo 8: «Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente» Artículo 47: «Derecho a la tutela judicial efectiva y a un juez imparcial. 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 el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia».

cuando el destinatario de la transferencia establecido en un país extracomunitario no cumple, o ya no puede cumplir, las cláusulas tipo de protección de datos, por lo que, más que una facultad, se convierte en una obligación del responsable de tratamiento establecido en la Unión Europea.

Por tanto, concluye el TJUE que la interpretación de los mecanismos incluidos en la Decisión 2010/87/UE, obligan al responsable del tratamiento establecido en la Unión Europea y al destinatario de la transferencia de datos personales a asegurarse de que la legislación del país tercero de destino permita al antedicho destinatario cumplir con las cláusulas tipo de protección de datos recogidas en la propia Decisión 2010/87/UE, antes de llevar a cabo una transferencia de datos personales a ese país tercero.

En lo que se refiere al alcance de dicha comprobación a efectuar por los sujetos intervinientes en la transferencia de datos, o lo que es lo mismo, cuando debe considerarse por estos que la legislación del país extracomunitario es incompatible con las cláusulas, señala el TJUE que, las obligaciones impuestas por esa legislación que no vayan más allá de las restricciones necesarias en una sociedad democrática para la salvaguardia, en particular, de la seguridad del Estado, la defensa y la seguridad pública no están en contradicción con las cláusulas tipo de protección de datos, por lo que, *sensu* contrario, el hecho de acatar una obligación dictada por el Derecho del país tercero de destino que vaya más allá de lo necesario para la consecución de tales fines debe considerarse una violación de las antedichas cláusulas.

Conforme a lo establecido en el anexo de la Decisión 2010/87/UE, el responsable del tratamiento establecido en la Unión Europea está obligado, cuando el destinatario de la transferencia de datos personales le notifica, que la legislación que le es de aplicación ha sido objeto de una modificación que puede tener un importante efecto negativo sobre las garantías ofrecidas y las obligaciones impuestas por las cláusulas tipo de protección de datos, a enviar esa notificación a la autoridad de control competente en caso de que, a pesar de dicha notificación por parte del destinatario establecido en el país extracomunitario, el responsable de tratamiento establecido en la Unión Europea, decida proseguir la transferencia, o levantar una suspensión previamente acordada. El envío de la referida notificación a la autoridad de control competente, y la facultad de esta de auditar al destinatario de la transferencia de datos personales, permiten a la mencionada autoridad de control comprobar si es preciso proceder a la suspensión o la prohibición de la transferencia prevista para garantizar un nivel de protección adecuado.

Por lo tanto, advierte el Tribunal que, incluso teniendo en cuenta las obligaciones de notificación e información del destinatario extracomunitario, y la obligación de suspensión o finalización de la transferencia de datos por parte del responsable del tratamiento las partes, en el caso de que este decida no suspender o no finalizar la transferencia, tiene una obligación de notificación a la autoridad de control competente que podrá suspender o prohibir, en su

caso, una transferencia de datos personales a un país tercero basada en las cláusulas tipo de protección de datos recogidas en el anexo de dicha Decisión 2010/87/UE, debiendo la autoridad de control ejercer las facultades que le corresponden conforme a lo resuelto en la propia Sentencia «Schrems II».

Por todo lo expuesto, concluye el TJUE que la Decisión 2010/87/UE prevé mecanismos efectivos que permiten, en la práctica, garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas, incluyendo la posibilidad de control por las autoridades en el caso de que por el responsable del tratamiento no se suspenda o prohíba la transferencia, por lo que entiende que no se presenta ningún elemento que pueda afectar a la validez de dicha Decisión.

IV.5. Sobre la validez de la Decisión «Escudo de Privacidad»

Por último, el TJUE entra a valorar la validez de la Decisión «Escudo de Privacidad», atendiendo a si el Derecho de los EE.UU. garantiza efectivamente el nivel de protección adecuado exigido en el artículo 45 del RGPD, interpretado a la luz de los derechos fundamentales garantizados en los artículos 7, 8 y 47 de la Carta teniendo en cuenta que, el órgano jurisdiccional que plantea la cuestión prejudicial considera que el Derecho de los EE.UU. no prevé las limitaciones y garantías necesarias con respecto a las injerencias autorizadas por su normativa nacional, así como que tampoco garantiza una tutela judicial efectiva a los interesados, contra tales injerencias, sin que el mecanismo del Defensor del Pueblo previsto ofrezca la debida protección a la tutela judicial efectiva.

Partiendo de este planteamiento se analiza por parte del TJUE la validez de la Decisión «Escudo de Privacidad» teniendo en cuenta, por una parte, la incidencia que las injerencias de las autoridades de EE.UU., conforme al Derecho de aquel país, tiene en el nivel de protección adecuado y, por otra, la validez de la figura de Defensor del Pueblo regulado por la Decisión «Escudo de Privacidad» para garantizar la tutela judicial efectiva de los ciudadanos comunitarios en defensa de sus datos personales protegidos.

Con respecto a la primera de las cuestiones, considera el Tribunal que las injerencias resultantes de los programas de vigilancia basados en la FISA[94] y en la E.O. 12333[95] no están sujetas a exigencias que garanticen, un nivel de

94 Foreign Intelligence Surveillance Act of 1978 (Ley de Vigilancia de la Inteligencia Extranjera) (Pub.L. 95-511, 92 Stat. 1783, 50 U.S.C. cap. 36).

95 Executive Order 12333.

protección sustancial, considerando el TJUE que las limitaciones que establecen las referidas normas de los EE.UU. no respetan el principio de proporcionalidad, que establece básicamente que las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario.

En este sentido, añade el TJUE que la comunicación de datos de carácter personal a un tercero, como una autoridad pública, constituye una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta (derecho al respeto a la vida privada y familiar, así como derecho a la protección de datos personales), cualquiera que sea la utilización posterior de la información comunicada, considerando una injerencia similar la conservación de los datos de carácter personal y del acceso a esos datos con vistas a su utilización por parte de las autoridades públicas, con independencia de que la información relativa a la vida privada de que se trate tenga o no carácter sensible o de que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia[96].

Aunque el TJUE pone de manifiesto que los anteriores derechos no gozan de carácter absoluto, incide en que cualquier limitación de los mismos, derivada del tratamiento de datos de carácter personal, debe realizarse para fines concretos, sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto en la Ley, que deberá definir con absoluta claridad el alcance de la limitación prevista en los derechos y libertades, estableciendo reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario ya que, de lo contrario, no se respetaría el citado principio de proporcionalidad.

En el caso objeto de la Sentencia «Schrems II», el TJUE advierte que las injerencias resultantes de los programas de vigilancia basados en la FISA y en la E.O. 12333 exceden de los límites impuestos por la normativa europea de protección de datos de carácter personal, principalmente debido a que los programas de vigilancia autorizados por la normativa de los EE.UU. no se fundamentan en una vigilancia individual sino en programas de vigilancia masivos e indiscriminados y, en definitiva, ilimitados, basados en sistemas

96 Se remite el Tribunal de Justicia de la Unión Europea, en este punto a las sentencias de 20 de mayo de 2003, Österreichischer Rundfunk y otros, C 465/00, C 138/01 y C 139/01, EU:C:2003:294, apartados 74 y 75; de 8 de abril de 2014, Digital Rights Ireland y otros, C 293/12 y C 594/12, EU:C:2014:238, apartados 33 a 36, y el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126.

de recopilación «en bloque» de los datos personales protegidos que, evidentemente, exceden notablemente de las exigencias de concreción y determinación del alcance de la limitación de los derechos y libertades que derivan del principio de proporcionalidad, por lo que, concluye el Tribunal, que no puede considerarse que los programas de vigilancia basados en esas disposiciones se limiten a lo estrictamente necesario.

Con respecto a la segunda de las cuestiones, es decir, sobre la debida garantía del derecho a la tutela judicial efectiva de los interesados, y sobre si la figura del Defensor del Pueblo a la que se refiere la Decisión «Escudo de Privacidad» garantiza este derecho, el TJUE recuerda que el primer párrafo del referido artículo 47 de la Carta requiere que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión Europea hayan sido violados tenga derecho a la tutela judicial efectiva respetando las condiciones establecidas en el mencionado artículo. A tenor del párrafo segundo del antedicho artículo, toda persona tiene derecho a que su causa sea oída por un juez independiente e imparcial, lo que hace necesaria, en todo caso, la existencia de recursos administrativos y acciones judiciales que sean efectivos y accesibles para las personas cuyos datos personales son objeto de tratamiento.

En el caso de autos, la constatación contenida en la Decisión «Escudo de Privacidad», según la cual los EE.UU. garantizan un nivel de protección sustancialmente equivalente al previsto en el artículo 47 de la Carta, fue puesta en entredicho basándose, en particular, en que la creación del Defensor del Pueblo en el ámbito del «Escudo de Privacidad» no puede subsanar las lagunas en lo que respecta a la tutela judicial de las personas cuyos datos personales son transferidos a ese país tercero, considerando el TJUE que esta exigencia no se cumple en este caso, por cuanto la normativa de los EE.UU., en especial en los casos de programas de vigilancia basados en la E.O. 12333, no ofrecen ninguna vía de recurso, por lo que no garantizan la debida tutela judicial efectiva para los ciudadanos cuyos datos son objeto de tratamiento.

Entiende el TJUE que la existencia del mecanismo del Defensor del Pueblo no subsana las limitaciones al derecho a la tutela judicial efectiva, poniendo en entredicho la independencia del Defensor del Pueblo con respecto al poder ejecutivo de los EE.UU. y su facultad para emitir decisiones vinculantes para las autoridades estadounidenses sin que, además, constata que no existe ninguna garantía legal que pueda ser invocada por los ciudadanos ante dicho Defensor del Pueblo, por lo que no se cumple con la exigencia de una vía de recurso efectivo garante del derecho a la tutela judicial efectiva en materia de protección de datos.

Por lo tanto, concluye el TJUE que la Comisión, al declarar, en el artículo 1, apartado 1, de la Decisión «Escudo de Privacidad», que los EE.UU. garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a entidades establecidas en ese país tercero en el marco del Escudo de la Privacidad UE EE.UU., no tuvo en cuenta las exigen-

cias resultantes del artículo 45, apartado 1, del RGPD, interpretado a la luz de los artículos 7, 8 y 47 de la Carta por lo que declara la invalidez de dicha Decisión.

Por último, se pronuncia el TJUE sobre si es preciso mantener los efectos de la antedicha Decisión «Escudo de Privacidad» para evitar la creación de un vacío legal, concluyendo que en este caso no se produce tal vacío legal por cuanto que teniendo en cuenta el artículo 49 del RGPD, que establece, de manera precisa, las condiciones en las que pueden tener lugar transferencias de datos personales a países terceros en ausencia de una decisión de adecuación en virtud del artículo 45, apartado 3, del referido Reglamento o de garantías adecuadas con arreglo al artículo 46 del mismo Reglamento.

V. ¿Y a la tercera va la vencida?: el nuevo marco transatlántico de privacidad de datos

V.1. Contexto

El nuevo Marco de Privacidad de Datos UE-EE.UU. introduce nuevas garantías vinculantes al objeto de dar respuesta a cada uno de los motivos de inquietud puestos de manifiesto, en su día, por el TJUE. Entre estas garantías se encuentran la limitación del acceso por parte de los servicios de inteligencia estadounidenses a los datos de la UE (a lo necesario y proporcionado), y el establecimiento de un Tribunal de Recurso en Materia de Protección de Datos, al que los ciudadanos de la UE tendrán acceso. El nuevo marco introduce mejoras importantes respecto al mecanismo que existía en virtud del *Safe Harbour* o del Escudo de la privacidad. Por ejemplo, si el Tribunal de Recurso en Materia de Protección de Datos concluye que se han recogido datos en contravención de las nuevas garantías, podrá requerir la supresión de los mismos.

Las empresas estadounidenses podrán adherirse al Marco de Privacidad de Datos UE-EE.UU. si se comprometen a cumplir una serie de obligaciones detalladas de privacidad; por ejemplo, el requisito de borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida, y a garantizar la continuidad de la protección en caso de compartir los datos de carácter personal con terceros. Y, en caso de tratamiento indebido de sus datos por parte de las empresas estadounidenses, los ciudadanos de la UE se beneficiarán de varias vías de reparación, entre ellos mecanismos de resolución independiente y gratuita de controversias, y un tribunal arbitral. Además, el marco jurídico estadounidense establece una serie de *garantías relativas al acceso por parte de las administraciones públicas estadounidenses* a los datos transferidos al amparo del marco se limita a lo estrictamente necesario: en particular, a efectos penales y de seguridad nacional y solo en aras a proteger la seguridad nacional.

En cuestiones relacionadas con la recogida y el uso de sus datos por parte de los servicios de inteligencia estadounidenses, los ciudadanos de la UE tendrán acceso a unos órganos independientes e imparciales de impugnación, entre ellos, como hemos señalado, el nuevo Tribunal de Recurso en Materia de Protección de Datos, que investigará y resolverá las reclamaciones de forma independiente y podrá imponer medidas reparatorias de fuerza vinculante.

Un elemento esencial del marco jurídico estadounidense que consagra estas garantías es el Decreto Presidencial de los EE.UU. titulado «Refuerzo de las garantías en las actividades de inteligencia de señales de los EE.UU.», que da respuesta a las reservas manifestadas por el TJUE en su sentencia «Schrems II»[97].

A pesar de que no existe legislación federal en materia de privacidad y protección de datos en los EE.UU., son notables los esfuerzos realizados por los EE.UU. en el Decreto n.º 14086, introduce definiciones de conceptos fundamentales de la protección de datos, como los principios de necesidad y proporcionalidad, y supone un importante paso adelante con respecto a mecanismos de transferencia anteriores, para fijar límites a las actividades de inteligencia de señales de los EE.UU. haciendo que los principios de proporcionalidad y necesidad sean aplicables al marco jurídico estadounidense en materia de inteligencia de señales e incorporando una lista de objetivos legítimos para dichas actividades.

Si bien el citado Decreto prevé importantes mejoras destinadas a garantizar que estos principios sean sustancialmente equivalentes a los contemplados en el Derecho de la UE, estos principios son desde hace tiempo elementos clave del régimen de protección de datos de la UE y sus definiciones sustantivas recogidas en el Decreto n.º 14086 no están en consonancia con su definición en el Derecho de la UE y su interpretación por parte del TJUE.

En la medida en que el Decreto n.º 14086 permite en algunos casos la recopilación masiva de datos (incluido el contenido de las comunicaciones) mediante inteligencia de señales; si bien el Decreto n.º 14086 contiene varias garantías en caso de recogida masiva, no prevé una autorización previa independiente para la recogida masiva; y ya, en la sentencia «Schrems II», el TJUE explicó que la vigilancia de los EE.UU. no cumplía el Derecho de la UE porque no exigía un «criterio objetivo» que permitiese justificar la injerencia del Gobierno en la privacidad.

Las garantías establecidas por los EE.UU. también facilitarán la circulación transatlántica de datos de forma más general, ya que también serán de

97 *Vid.* Ortega Giménez, Alfonso, «"A la tercera va la vencida": el nuevo Marco Trasatlántico de Privacidad de Datos EE.UU.-EU (Privay Shield 2.0)», en *LA LEY Privacidad*, Número 14, Editorial Wolters Kluwer, Las Rozas (Madrid), octubre-diciembre 2022, pp. 1-7.

aplicación a la transferencia de datos mediante otras herramientas como las cláusulas contractuales tipo[98] o las *Binding Corporate Rules*.

V.2. Rasgos característicos

Este nuevo Marco de Privacidad de Datos UE-EE.UU. responde a los siguientes 5 principios:

1. **Transferencias legítimas y seguras**: con base en el nuevo marco de privacidad, los datos personales podrán transferirse de forma legítima y segura entre la UE y las compañías estadounidenses que se encuentren adheridas a dicho Marco.
2. **Acceso a los datos estrictamente necesarios por parte de las Agencias de Inteligencia**: establecimiento de un nuevo conjunto de normas y garantías vinculantes con el fin de limitar el acceso a los datos por parte de las autoridades de inteligencia estadounidenses a lo necesario y respetando el principio de proporcionalidad para proteger la seguridad nacional. En este sentido, dichas agencias de inteligencia adoptarán procedimientos con el fin de garantizar una supervisión eficaz de los nuevos estándares de privacidad y libertades civiles.
3. **Posibilidad de recurso para los titulares de los datos**: articulación de un nuevo procedimiento de recurso al alcance de los interesados en dos niveles, para investigar y resolver las reclamaciones de los titulares europeos sobre el acceso a sus datos por parte de las autoridades de inteligencia estadounidenses, que incluye el establecimiento de un Tribunal de revisión de protección de datos.
4. **Necesidad de adhesión por las compañías estadounidenses**: fijación de obligaciones estrictas para las empresas estadounidenses que tratan datos personales transferidos desde la Unión Europea, incluyendo el requisito de «auto-certificar» su adhesión a los principios de este nuevo acuerdo.
5. **Mecanismos de control y revisión**: se establecerán mecanismos específicos de control y revisión del marco de privacidad. La Comisión Europea, junto con representantes de las autoridades de protección de datos europeas y de las autoridades competentes estadounidenses, se ha comprometido a realizar una revisión periódica del funcionamiento del Marco de Privacidad de Datos UE-EE.UU. Y la primera revisión se llevará a cabo antes de que se cumpla un año de la entrada

98 *Vid.* Ortega Giménez, Alfonso, «Decisiones relativas a las cláusulas contractuales tipo para las transferencias internacionales de datos personales a terceros países y entre los responsables y encargados del tratamiento», en *Revista LA LEY Privacidad*, número 9, Editorial Wolters Kluwer, Madrid, julio-septiembre 2021, pp. 1-12.

en vigor de la decisión de adecuación (esto es, antes del 10 de julio de 2024), con objeto de verificar si todos los elementos pertinentes se han implantado plenamente y funcionan eficazmente en la práctica. Y el Departamento de Comercio estadounidense será el responsable de la administración y la supervisión del Marco. La Comisión Federal de Comercio de los EE.UU. se encargará de hacer cumplir por parte de las empresas estadounidenses.

El pasado 10 de julio de 2023, la Comisión Europea publicó su decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE.UU. Se convierte en la tercera decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE. UU[99].

Los puntos clave de esta decisión son los siguientes:

a) Los servicios de inteligencia estadounidenses deberán limitar su acceso a los datos de la UE que sean necesarios y proporcionados a la protección de la seguridad nacional en el seno de una investigación realizada de acuerdo con la normativa de inteligencia exterior de los EE.UU.

b) Los ciudadanos de la UE podrán acudir al nuevo *Data Protection Review Court* para impugnar las acciones y decisiones de las autoridades de inteligencia y para proteger sus derechos.

c) Si el *Data Protection Review Court* concluye que se han recogido datos incumpliendo las nuevas garantías, podrá requerir la supresión de los mismos.

d) Las nuevas garantías en materia de acceso a los datos por los servicios de inteligencia complementarán las obligaciones que las empresas estadounidenses que importen datos de la UE tendrán que asumir.

e) Las empresas estadounidenses podrán adherirse al Marco de Privacidad de Datos UE-EE.UU. si se comprometen a cumplir una serie de obligaciones detalladas de privacidad y obtienen la aprobación del *US Department of Commerce*, que se encargará de revisar y monitorizar si dichas empresas cumplen los requisitos.

f) Entre los requisitos a cumplir destaca la obligación de borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida;

g) También destaca la obligación de garantizar la continuidad de la protección si se comparten los datos de carácter personal con terceros.

h) En caso de tratamiento indebido de los datos por parte de las empresas estadounidenses, los ciudadanos de la UE dispondrán de varias

99 Decisión de ejecución de la Comisión de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre UE y los EE.UU.

vías de reparación entre las que destacan los mecanismos de resolución independiente y gratuita de controversias y un tribunal arbitral.

i) Serán también aplicables las cláusulas contractuales tipo y las normas corporativas vinculantes. Como consecuencia de estas nuevas garantías, los datos personales transferidos por las empresas europeas a empresas estadounidenses al amparo del nuevo marco no necesitarán de establecer garantías adicionales de protección de datos[100].

Con la aprobación de este nuevo Acuerdo, la Comisión Europea espera, por un lado, dar carpetazo de una vez por todas, a la falta de garantías señalada por el TJUE y que provocó la invalidez de los dos marcos de privacidad anteriores *(Safe Harbor y Privacy Shield)*; y, por otro lado, establecer un nuevo marco seguro y duradero, mediante el que se puedan realizar las transferencias de datos personales necesarias desde la UE a EE.UU.

Este es un acuerdo importante y necesario para facilitar el actual flujo de datos UE-EE.UU. y las relaciones comerciales con clientes, socios y proveedores de servicios en dicho país. No obstante, existen todavía muchas dudas en relación con este nuevo marco jurídico trasatlántico y si el mismo podrá realmente conseguir los objetivos que se propone. En especial, los retos que la legislación estadounidense relativa a vigilancia y espionaje *(FISA y EO 12333)* suponen para ofrecer unas garantías similares a las establecidas por la normativa de protección de datos personales vigente en la UE.

El nuevo marco introduce mejoras significativas en comparación con el mecanismo que existía bajo el Escudo de Privacidad. Por ejemplo, si el Tribunal de Revisión de Protección de Datos determina que los datos se recopilaron en violación de las nuevas salvaguardas, podrá ordenar la eliminación de los datos. Las nuevas salvaguardas en el ámbito del acceso gubernamental a los datos complementarán las obligaciones que tendrán que suscribir las empresas estadounidenses que importen datos de la UE.

Las empresas estadounidenses podrán unirse al nuevo Marco de Privacidad Unión Europea-EE.UU. comprometiéndose a cumplir con un conjunto detallado de obligaciones de privacidad, por ejemplo, el requisito de eliminar datos personales cuando ya no sean necesarios para el propósito para el que fueron recopilados, y garantizar la continuidad de la protección cuando los datos personales se comparten con terceros.

Las personas de la UE se beneficiarán de varias vías de reparación en caso de que las empresas estadounidenses manejen incorrectamente sus datos. Esto incluye mecanismos de resolución de disputas independientes y gratuitos y un panel de arbitraje.

---

100 *Vid.*, en sentido amplio, https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf

La clave va a estar en la capacidad de las autoridades americanas de controlar posibles abusos en la gestión de datos, sobre todo por las instituciones de inteligencia de EE.UU. Y los principales cambios de este nuevo acuerdo van en esa línea para dotar de seguridad jurídica este tipo de transferencias internacionales de datos. De esta forma se establecen procedimientos e instituciones para ese control de la actividad amparada por la normativa americana se alinee con los principios del RGPD, a nivel de proporcionalidad y minimización de los datos.

El funcionamiento de estas medidas va a radicar en la transparencia que existe en estos procesos de control. Es importante que el ciudadano tenga visibilidad sobre en qué se concretan esas medidas y si van a tener el efecto que se esperan. Sin lugar a dudas, las principales obligaciones son las de respetar los principios básicos que reconoce el Marco de Privacidad (muy similares a los que reconoce el RGPD). Sobre el proceso de certificación, para adherirse al Marco de Privacidad deberá demostrarse el cumplimiento con los anteriores principios tanto al momento de inscribirse por primera vez como con cada recertificación (obligatoriamente, las entidades deberán revalidar su certificación con carácter anual). Al mismo tiempo se reconocen modalidades de certificación vía (i) *self assessment* o (ii) por comprobación externa[101].

Al examinar el nivel de protección ofrecido por un tercer país, la Comisión está obligada a evaluar el contenido de las normas aplicables en ese país derivadas de su legislación nacional o de sus compromisos internacionales, así como la práctica destinada a garantizar el cumplimiento de dichas normas; que, en caso de que dicha evaluación se considere insatisfactoria en términos de adecuación y equivalencia, la Comisión estará obligada a suspender la adecuación cuando deje de existir equivalencia.

Es evidente que la capacidad de transferir datos personales a través de las fronteras puede ser un motor fundamental de innovación, productividad y competitividad económica, siempre y cuando se ofrezcan unas garantías adecuadas; que estas transferencias deben realizarse con pleno respeto del derecho a la protección de los datos personales y el derecho a la privacidad; y que uno de los fines de la UE es la protección de los derechos fundamentales consagrados en la Carta de derechos Fundamentales de la UE (en particular, el respeto de la vida privada y familiar y la protección de los datos personales).

Si bien el RGPD se aplica a todas las empresas que tratan datos personales de interesados en la UE cuando las actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la UE o con

101 *Vid.*, en sentido amplio, https://www.economistjurist.es/actualidad-juridica/eeuu-y-la-ue-llegan-a-un-nuevo-acuerdo-sobre-transferencias-internacionales-de-datos-que-blinda-la-privacidad-que-reclamaba-el-tjue/

el seguimiento de su comportamiento en la medida en que este tenga lugar dentro de la UE, la recopilación indiscriminada de datos sin salvaguardias que limiten la intrusión en la privacidad de las personas por agentes estatales merma la confianza de los ciudadanos, las empresas y los Gobiernos europeos en los servicios digitales; y, por ende, en la economía digital; y, aunque a las agencias estadounidenses les está prohibida la recopilación masiva de datos sobre los ciudadanos estadounidenses que viven en ese país, dicha prohibición no se aplica en el caso de los ciudadanos de la UE; y esa vigilancia masiva por parte de agentes estatales es ilegal y afecta negativamente a la confianza de los ciudadanos y las empresas de la UE en los servicios digitales y, por ende, en la economía digital.

V.3. Especial atención a las reservas del Comité Europeo de Protección de Datos al nuevo Marco transatlántico de privacidad de datos

Hemos tenido que esperar casi 2 años desde la STJUE «Schrems II» para el restablecimiento del flujo de datos de carácter personal entre las empresas europeas y estadounidenses[102]. Tras la invalidación de la decisión de adecuación anterior sobre el Escudo de privacidad la UE-EE.UU. por parte del Tribunal de Justicia de la UE, la Comisión Europea y el Gobierno estadounidense se sentaron a negociar un nuevo marco que resolviera los problemas puestos de manifiesto por el propio TJUE[103].

El pasado 25 de marzo de 2022 se publicó una Declaración conjunta de la Comisión Europea y los EE.UU. sobre el marco transatlántico de privacidad de datos. Dicha Declaración constituye un nuevo Marco Trasatlántico de Privacidad de Datos, que pretende fomentar los flujos de datos transatlánticos y abordará las preocupaciones planteadas por «Schrems II». El nuevo Marco fijaba un compromiso sin precedentes por parte de EE.UU. para implementar reformas que fortalecerán las protecciones de privacidad y libertades civiles aplicables a las actividades de inteligencia de señales de EE.UU. Bajo el Marco Transatlántico de Privacidad de Datos, EE.UU. implementará nuevas salvaguardas para garantizar que las actividades de vigilancia de señales sean necesarias y proporcionadas en la búsqueda de objetivos definidos de seguridad nacional, establecerá un mecanismo de reparación independiente de dos niveles con autoridad vinculante para medidas correctivas directas y

102 *Vid.* Ortega Giménez, Alfonso y García Escobar, Encarnación, «Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 ("Schrems II")», en *LA LEY Privacidad*, número 6, Editorial Wolters Kluwer, Madrid, octubre-diciembre 2020, pp. 1-22.

103 *Vid.*, en sentido amplio, https://www.tendencias.kpmg.es/2022/03/claves-acuerdo-principios-ue-ee-uu-marco-transatlantico-privacidad-datos

mejorar la supervisión rigurosa y en capas de las actividades de inteligencia de señales para garantizar el cumplimiento de las limitaciones en las actividades de vigilancia.

Se señalaba, entonces, que sería el Comité Europeo de Protección de datos (CEPD) quien debía analizar el documento antes de que se adoptase una decisión en firme, tal y como recoge el RGPD. El CEPD recordó que, de momento, el anuncio no constituía un marco legal, por lo que los exportadores de datos tendrían/tienen que seguir cumpliendo con las medidas impuestas por el TJUE y a partir de la sentencia «Schrems II». Y, así las cosas, el CEPD, en su reunión plenaria del pasado 28 de febrero de 2023, emitió un dictamen sobre el Proyecto de Decisión de Adecuación, publicado por la Comisión Europea el 13 de diciembre de 2022, sobre el nuevo Marco para los intercambios transatlánticos de datos personales entre la UE y los EE. UU[104].

El Dictamen del CEPD[105] reconoce los aspectos positivos incorporados tras la negociación, al tiempo que señala determinadas deficiencias que no han sido resueltas, representando riesgos desde la óptica de la protección de datos personales. Dichas deficiencias afectan tanto a la parte comercial de dicho marco, es decir, a las transferencias de datos desde las empresas en Europa a las empresas en EE.UU., como al acceso que desde las autoridades de seguridad gubernamentales de EE.UU. se prevé a los datos personales que se transfieran a EE.UU. El CEPD ha presentado su dictamen al Parlamento Europeo, dando así continuidad al proceso de tramitación de dicho Acuerdo en la UE hasta su posible aprobación definitiva.

En su Dictamen 5/2023, el CEPD acoge con satisfacción mejoras sustanciales introducidas en relación con el marco anterior regulado por el Acuerdo *Privacy Shield*, tales como la introducción de los principios de necesidad y proporcionalidad para la recogida de datos por los servicios de inteligencia de EE.UU. y el nuevo mecanismo de recurso para los interesados de la UE; pero, al mismo tiempo, expresa su preocupación y solicita aclaraciones sobre varios puntos incluidos en la nueva propuesta.

Se señala que el marco de privacidad propuesto es una mejora respecto el anterior, pero no suficiente como para justificar una decisión de adecuación sobre las transferencias de datos personales, por lo que se oponen a este.

Argumentan que la Comisión Europea no debería otorgar a los EE.UU. una decisión de adecuación que considere que su nivel de protección de datos personales sea esencialmente equivalente al de la UE y permita la transferencia de datos personales entre la UE y EE.UU. Recalcando que se continúa

104 *Vid.* https://diariolaley.laleynext.es/dll/2023/03/06/el-comite-europeo-de-proteccion-de-datos-emite-un-dictamen-favorable-con-reservas-al-nuevo-marco-de-transferencia-de-datos-a-los-estados-unidos

105 Puede accederse al contenido completo del Dictamen 5/2023 a través del enlace: https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf

permitiendo la recopilación masiva de datos y que, a pesar de la creación de un Tribunal de Revisión de Protección de Datos, destinado a proporcionar a los interesados de la UE reparación en caso de vulneración de derechos, se trata de un tribunal que lleva a cabo decisiones secretas y que vulnera el derecho de los ciudadanos a acceder y rectificar los datos sobre ellos, además, de no tener plena independencia.

Concluyen indicando que se presenta un marco de privacidad que no se encuentra preparado para el futuro y que la evaluación de la adecuación debe basarse en la aplicación práctica de las normas. Por esto, entienden que la Comisión Europea no debería otorgar una decisión de adecuación basada en el régimen actual, sino que debería negociar nuevamente un nuevo acuerdo que mejore los puntos expuestos.

Y mientras todo esto ocurre, un nuevo terremoto en material de transferencias internacionales de datos de carácter personal se ha producido: hemos tenido conocimiento de la multa récord de 1200 millones de euros impuesta a Meta por parte del regulador irlandés por violar las normas europeas de protección de datos con su red social Facebook.

Meta, que pretende apelar, es condenada por haber continuado transfiriendo datos personales de usuarios de la UE a los EE.UU. violando las normas europeas en la materia, indicó en su decisión la Comisión Irlandesa de Protección de Datos. (DPC), que actúa en nombre de la UE.

Meta también debe suspender cualquier transferencia de datos personales a los EE.UU. en los próximos cinco meses tras la notificación de esta decisión y debe cumplir con la protección de datos en los próximos seis meses. Esta sanción, la más alta impuesta por un regulador de protección de datos en la UE, es el resultado de una investigación iniciada en 2020, y tiene su fundamentación jurídica en la vulneración del artículo 46 del RGPD, que señala que «el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas».

Esta es la tercera multa impuesta a Meta desde principios de año en la UE y la cuarta en seis meses. En enero, la Comisión Irlandesa de Protección de Datos. (DPC) había sancionado duramente al grupo con casi 400 millones de euros por delitos sobre el uso de datos personales con fines publicitarios dirigidos a sus aplicaciones de Facebook, Instagram y WhatsApp, luego, en marzo, con 5,5 millones de euros por violar la protección de datos con su mensaje de WhatsApp. Desde entonces, Meta se comprometió a cambiar sus términos de uso en Europa para poder continuar recopilando y procesando los datos personales de sus usuarios europeos. Estas sanciones se dan en un contexto de refuerzo de los controles y procedimientos judiciales en la UE, pero también en EE.UU., contra GAFA (Google, Amazon, Facebook y Apple), y las medidas tomadas recientemente contra el gigante chino

TikTok. En 2021, Amazon recibió una multa de 746 millones de euros en Luxemburgo por incumplimiento de la normativa de protección de datos.

V.4. Valoración crítica

Al examinar el nivel de protección ofrecido por un tercer país, la Comisión está obligada a evaluar el contenido de las normas aplicables en ese país derivadas de su legislación nacional o de sus compromisos internacionales, así como la práctica destinada a garantizar el cumplimiento de dichas normas; que, en caso de que dicha evaluación se considere insatisfactoria en términos de adecuación y equivalencia, la Comisión debe abstenerse de adoptar una decisión de adecuación, ya que está supeditada a la aplicación de las garantías pertinentes; que la Comisión está obligada a suspender la adecuación cuando deje de existir equivalencia; que el RGPD exige que la evaluación pertinente sea un proceso continuo que tenga en cuenta los cambios en las normas y prácticas aplicables.

Sin ninguna duda la capacidad de transferir datos personales a través de las fronteras puede ser un motor fundamental de innovación, productividad y competitividad económica, siempre y cuando se ofrezcan unas garantías adecuadas; que estas transferencias deben realizarse con pleno respeto del derecho a la protección de los datos personales y el derecho a la privacidad; y que uno de los fines de la UE es la protección de los derechos fundamentales consagrados en la Carta (en particular, el respeto de la vida privada y familiar y la protección de los datos personales).

Si bien el RGPD se aplica a todas las empresas que tratan datos personales de interesados en la Unión cuando las actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión o con el seguimiento de su comportamiento en la medida en que este tenga lugar dentro de la UE, la recopilación indiscriminada de datos sin salvaguardias que limiten la intrusión en la privacidad de las personas por agentes estatales merma la confianza de los ciudadanos, las empresas y los Gobiernos europeos en los servicios digitales y, por ende, en la economía digital; y, aunque a las agencias estadounidenses les está prohibida la recopilación masiva de datos sobre los ciudadanos estadounidenses que viven en ese país, dicha prohibición no se aplica en el caso de los ciudadanos de la UE; y esa vigilancia masiva por parte de agentes estatales es ilegal y afecta negativamente a la confianza de los ciudadanos y las empresas de la UE en los servicios digitales y, por ende, en la economía digital.

A pesar de que no existe legislación federal en materia de privacidad y protección de datos en los EE.UU., son notables los esfuerzos realizados por los EE.UU. en el Decreto n.º 14086, introduce definiciones de conceptos fundamentales de la protección de datos, como los principios de necesidad y proporcionalidad, y supone un importante paso adelante con respecto a

mecanismos de transferencia anteriores, para fijar límites a las actividades de inteligencia de señales de los EE.UU. haciendo que los principios de proporcionalidad y necesidad sean aplicables al marco jurídico estadounidense en materia de inteligencia de señales e incorporando una lista de objetivos legítimos para dichas actividades.

Si bien el citado Decreto prevé importantes mejoras destinadas a garantizar que estos principios sean sustancialmente equivalentes a los contemplados en el Derecho de la UE, estos principios son desde hace tiempo elementos clave del régimen de protección de datos de la UE y sus definiciones sustantivas recogidas en el Decreto n.º 14086 no están en consonancia con su definición en el Derecho de la UE y su interpretación por parte del TJUE.

En la medida en que el Decreto n.º 14086 permite en algunos casos la recopilación masiva de datos (incluido el contenido de las comunicaciones) mediante inteligencia de señales; si bien el Decreto n.º 14086 contiene varias garantías en caso de recogida masiva, no prevé una autorización previa independiente para la recogida masiva; y ya en la sentencia «Schrems II», el TJUE explicó que la vigilancia de los EE.UU. no cumplía el Derecho de la UE porque no exigía un «criterio objetivo» que permitiese justificar la injerencia del Gobierno en la privacidad.

Se deben compartir las preocupaciones del CEPD en la medida en que el Decreto n.º 14086 no proporcione garantías suficientes respecto a la recopilación masiva de datos al no prever una autorización previa independiente, carecer de normas claras y estrictas sobre la conservación de los datos, permitir una recopilación masiva «temporal» y no establecer exigencias más estrictas en relación con la difusión de los datos recopilados de forma masiva; señala, en particular, la preocupación específica de que, si no se aplican restricciones adicionales a la transmisión a las autoridades estadounidenses, los servicios de seguridad podrían acceder a datos a los que, de otro modo, se les habría prohibido acceder; recuerda que las transferencias ulteriores multiplican de hecho los riesgos para la protección de datos.

El Decreto n.º 14086 introduce algunas garantías para velar por la independencia de los jueces del TRPD, como también reconoce el CEPD; el TRPD forma parte del poder ejecutivo y no del poder judicial y que sus jueces son nombrados para un mandato fijo de cuatro años; el presidente de los EE.UU. puede revocar las decisiones del TRPD e incluso hacerlo en secreto; señala que, aunque el nuevo mecanismo de recurso no permite al fiscal general de los EE.UU. destituir y supervisar a los jueces del TRPD, no afecta a las facultades correspondientes del presidente de los EE.UU.; subraya que, mientras el presidente de los EE.UU. pueda destituir a los jueces del TRPD durante su mandato, la independencia de estos no estará garantizada; en caso de adopción, la Comisión debería seguir de cerca la aplicación de salvaguardas que garanticen la independencia en la práctica; señala que los demandantes estarían representados por un «abogado especial» designado por el TRPD y no sujeto a requisitos de independencia; pide a la Comisión que, en caso de

que se adopte una decisión de adecuación, vele por que se introduzca un requisito de independencia; concluye que, a día de hoy, el TRPD no cumple las normas de independencia e imparcialidad establecidas en el artículo 47 de la Carta; y, si bien la Junta de supervisión de la intimidad y las libertades civiles examinaría de forma independiente el funcionamiento del nuevo proceso de recurso, el alcance de este examen sería limitado.

Si bien los EE.UU. han previsto un nuevo mecanismo de recurso para las cuestiones relacionadas con el acceso de las autoridades públicas a los datos, siguen existiendo dudas sobre la efectividad de las vías de recurso disponibles en materia comercial, respecto a las cuales la decisión de adecuación no introduce cambios; observa que los mecanismos para resolver estas cuestiones se dejan en gran medida a la discreción de las empresas, que pueden elegir vías alternativas de solución, como los mecanismos de resolución de litigios o el uso de los programas de privacidad de las empresas; pide a la Comisión que, en caso de que se adopte una decisión de adecuación, supervise de cerca la eficacia de estos mecanismos de recurso.

A diferencia de todos los demás terceros países que han recibido una decisión de adecuación en virtud del RGPD, los EE.UU. no cuentan con una ley federal de protección de datos. La aplicación del Decreto n.° 14086 no es clara, precisa ni previsible, ya que puede ser modificado en cualquier momento por el presidente de los EE.UU., quien también está facultado para emitir decretos secretos; observa que la revisión de la decisión de adecuación tendría lugar transcurrido un año a partir de la fecha de notificación de la decisión de adecuación a los Estados miembros y, posteriormente, al menos cada cuatro años.

Las preocupaciones expresadas por el CEPD en relación con los derechos de los interesados, la ausencia de definiciones fundamentales y de normas específicas sobre la toma de decisiones automatizada y sobre la elaboración de perfiles, la falta de claridad sobre la aplicación de los principios del marco de privacidad a los encargados del tratamiento y la necesidad de evitar que las transferencias ulteriores socaven el nivel de protección son compartidas.

Las decisiones de adecuación, que deben ser adoptadas sobre la base de la legislación y las prácticas vigentes, no solo en cuanto al fondo, sino también en la práctica, tal como se establece en la STJUE «Schrems I», en la STJUE «Schrems II» y en el propio RGPD (Considerando 104), deben incluir mecanismos claros y estrictos de seguimiento y revisión a fin de garantizar que las decisiones estén preparadas para el futuro o que puedan revocarse o modificarse según proceda, y que se garantice en todo momento el derecho fundamental de los ciudadanos de la UE a la protección de datos y el Marco Transatlántico de Privacidad de Datos debería estar sujeto a una revisión permanente en función de la evolución jurídica y práctica en los EE. UU[106].

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

V.5. Perspectivas de futuro

Así las cosas, ¿podríamos decir que «a la tercera va la vencida?» ...pues la verdad es que no lo tenemos muy claro. A la misma vez que se anunciaba la puesta de largo del nuevo Marco de Privacidad de Datos UE-EE.UU. Edward Snowden se pronunciaba: este nuevo marco jurídico es en gran medida una copia del «Escudo de Privacidad». El tercer intento de la Comisión Europea de conseguir un acuerdo estable sobre las transferencias de datos entre la UE y EE.UU. volverá probablemente al TJUE en cuestión de meses. El «nuevo» Marco Transatlántico de Privacidad de Datos es en gran medida una copia del fracasado «Escudo de Privacidad». A pesar de los esfuerzos de relaciones públicas de la Comisión Europea, hay pocos cambios en la legislación estadounidense o en el enfoque adoptado por la UE. EE.UU. no se abordó el problema fundamental de la ley FISA 702, ya que sigue considerando que solo las personas estadounidenses son merecedoras de derechos constitucionales[107].

En 2013 Edward Snowden reveló que el Gobierno de EE.UU. utilizaba empresas de «grandes tecnologías» y programas como «PRISM» o «Upstream» al amparo de la FISA 702 y la OE 12.333 para espiar al resto del mundo sin necesidad de causa probable ni aprobación judicial. Esto no se limitaba a la delincuencia o el terrorismo, sino que también incluía el espionaje a «socios» de EE.UU. Desde una ley de la UE de 1995, en general no se pueden enviar datos personales fuera de la UE a menos que exista una protección «esencialmente equivalente» en el país de destino. La industria estadounidense se basó en gran medida en una Decisión de la Comisión Europea llamada «Safe Harbor» (Puerto Seguro) que declaró a EE.UU. «esencialmente equivalente» en 2000. El TJUE anuló la Decisión de la Comisión en el asunto C-362/14 («Schrems I») en 2015, dadas las leyes de vigilancia de EE.UU. En 2016, la Comisión Europea ha aprobado en gran medida la misma Decisión sobre transferencias de datos UE-EE.UU. de nuevo, bajo el nuevo nombre de «Escudo de Privacidad», que fue invalidado por el TJUE en C-311/18 («Schrems II») en 2020 en gran medida por los mismos motivos.

Tras la anulación del «Escudo de la privacidad», las negociaciones entre la UE y EE.UU. apenas avanzaron. EE.UU. insistió en que los datos de la UE seguirían sujetos a la vigilancia masiva estadounidense y que las personas «*no* estadounidenses» no tendrían las mismas protecciones que las estadounidenses. Tras más de año y medio sin apenas movimiento, EE.UU. habría utilizado la guerra de Ucrania para presionar a la UE sobre el intercambio de datos personales. Poco después, Joe Biden y Ursula von der Leyen se reunieron el 25 de marzo de 2022. Ese mismo día, los dos han «resuelto» de repente lo que los abogados eran incapaces de resolver y han presentado un «acuerdo de principio», un pagaré que en esencia contenía

107 *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu

dos «trucos» que deberían calmar a la opinión pública: *a) en primer lugar*, el TJUE consideró que la vigilancia masiva FISA 702 no era «proporcionada» en el sentido del artículo 52 de la Carta de los Derechos Fundamentales de la UE (CFR). La «nueva» Orden Ejecutiva 14086 de EE.UU. (que equivale en gran medida a la PPD-28 de 2014) incluiría ahora la palabra «proporcionada». El «truco» aquí: EE.UU. atribuirá otro significado a la palabra «proporcionado» que el TJUE. La OE 14086 declara que la vigilancia masiva FISA 702 es «proporcionada» en virtud de una «interpretación estadounidense» no revelada de la palabra y contraria a las dos conclusiones del TJUE. De este modo, la UE y EE.UU. pudieron afirmar que estaban de acuerdo en la misma palabra («proporcionada»), incluso cuando no hay acuerdo sobre el significado de la palabra; y, *b) en segundo lugar*, el TJUE determinó que la compensación a través del «Defensor del Pueblo» del Escudo de Privacidad no cumplía ni remotamente con el artículo 47 del MCR, incluso cuando el Defensor del Pueblo fue aclamado por las relaciones públicas de la Comisión en 2016 como una forma «independiente» de «compensación en el ámbito de la seguridad nacional». El «truco» de la reparación: el mecanismo del Defensor del Pueblo fue renombrado y dividido en un Oficial de Protección de las Libertades Civiles (CLPO) y un llamado «Tribunal» (que no es un tribunal, sino un órgano ejecutivo parcialmente independiente). Aunque hay algunas mejoras menores con respecto al Defensor del Pueblo, el individuo no tendrá ninguna interacción directa con los nuevos organismos (tendrá que enviar una queja a una autoridad de protección de datos de la UE y no será escuchado por EE.UU.) y darán exactamente la misma respuesta que el anterior «Defensor del Pueblo». Según la OE 14086, el CLPO y el Tribunal deberán responder en cualquier caso diciendo: «*Sin confirmar ni negar que el denunciante estuviera sometido a actividades de inteligencia de señales de EE.UU., la revisión o bien no identificó ninguna violación cubierta o bien el Tribunal de Revisión de Protección de Datos emitió una resolución que exigía una reparación adecuada*» (ver aquí). Por lo tanto, la «sentencia» de este «Tribunal» se conoce incluso antes de que se presente un caso. Hay muchos problemas adicionales con el mecanismo, que garantizarán en gran medida que las denuncias ni siquiera sean admitidas. Parece impensable que el Tribunal de Justicia acepte esto como «recurso judicial» en virtud del artículo 47 del MCR.

EE.UU. se ha negado a reformar la FISA 702 para ofrecer a las personas no estadounidenses una protección razonable de la intimidad. Hay acuerdo a ambos lados del Atlántico en que la FISA 702 y la OE 12.333 violan derechos fundamentales en virtud de la 4.ª Enmienda en EE.UU. y de los artículos 7, 8 y 47 del CFR en la UE, pero EE.UU. sigue insistiendo en que las personas no estadounidenses no tienen derechos constitucionales en EE.UU., por lo que una violación de su derecho a la intimidad no está cubierta por la 4.ª Enmienda. FISA 702 tendrá que prorrogarse a finales de 2023, dado que existe una «cláusula de extinción» en la legislación estadounidense. Esta

habría sido la oportunidad perfecta para mejorar la ley estadounidense, pero dado el nuevo acuerdo con la UE, habrá pocas razones para que EE.UU. reforme la FISA 702[108].

En general, el nuevo «Marco Transatlántico de Privacidad de Datos» es una copia de *Privacy Shield* (de 2016), que a su vez era una copia de *Safe Harbour* (de 2000). Dado que este enfoque ya ha fracasado dos veces, no había base jurídica para el cambio de rumbo: la única lógica de llegar a un acuerdo era política.

Cualquier persona cuyos datos personales vayan a ser transferidos en virtud del nuevo acuerdo puede presentar un recurso ante las autoridades de protección de datos o los tribunales. *noyb* ha preparado varias opciones procesales para llevar el nuevo acuerdo ante el TJUE. Esperamos que el nuevo sistema sea aplicado por las primeras empresas en los próximos meses, lo que abrirá la vía a la impugnación por parte de una persona cuyos datos se transfieran en virtud del nuevo instrumento. No es improbable que una impugnación llegue al TJUE a finales de 2023 o principios de 2024. El TJUE tendría entonces incluso la opción de suspender el «Marco» durante el tiempo que dure el procedimiento. Una decisión final del TJUE sería probable para 2024 o 2025. Independientemente de que la impugnación prospere, esto aportará claridad al «Marco Transatlántico de Privacidad de Datos» dentro de unos dos años[109].

Este tercer intento de aprobar en gran medida la misma decisión ilegal también plantea interrogantes sobre el papel más amplio de la Comisión

---

108 Señala Max Schrems, presidente de Noyb: «dicen que la definición de locura es hacer lo mismo una y otra vez y esperar un resultado diferente. Al igual que el "Escudo de la privacidad", el último acuerdo no se basa en cambios materiales, sino en intereses políticos. Una vez más, la actual Comisión parece pensar que el lío será problema de la próxima Comisión. La FISA 702 debe ser prorrogada por EE.UU. este año, pero con el anuncio del nuevo acuerdo la UE ha perdido todo poder para conseguir una reforma de la FISA 702». Es más, «ahora tenemos "Puertos", "Paraguas", "Escudos" y "Marcos", pero ningún cambio sustancial en la legislación estadounidense sobre vigilancia. Las declaraciones de prensa de hoy son casi una copia literal de las de hace 23 años. El mero anuncio de que algo es "nuevo", "sólido" o "eficaz" no basta ante el Tribunal de Justicia. Necesitaríamos cambios en la legislación estadounidense sobre vigilancia para que esto funcionara, y sencillamente no los tenemos» *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu

109 Max Schrems: «Tenemos varias opciones de impugnación ya en el cajón, aunque estamos hartos de este ping-pong jurídico. Actualmente esperamos que esto vuelva al Tribunal de Justicia a principios del año que viene. El Tribunal de Justicia podría incluso suspender el nuevo acuerdo mientras revisa su contenido. En aras de la seguridad jurídica y el Estado de Derecho, entonces sabremos si las pequeñas mejoras de la Comisión han sido suficientes o no. Durante los últimos 23 años, todos los acuerdos entre la UE y EE.UU. han sido declarados inválidos con carácter retroactivo, haciendo ilegales todas las transferencias de datos realizadas por las empresas en el pasado; parece que ahora vamos a añadir otros dos años de este ping-pong». *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu

Europea como guardiana de los tratados de la UE. En lugar de defender el «Estado de derecho», la Comisión se limita a aprobar una decisión inválida una y otra vez, a pesar de las claras sentencias del TJUE. A pesar de la gran indignación tras las revelaciones de Snowden en la UE y de los repetidos llamamientos del Parlamento Europeo a tomar medidas, la Comisión parece dar prioridad a las relaciones diplomáticas con EE.UU. y a la presión empresarial a ambos lados del Atlántico sobre los derechos de los europeos y los requisitos de la legislación de la UE[110].

110 Max Schrems: «se supone que la Comisión es la 'guardiana de los tratados' y la defensora del 'Estado de Derecho'. Le encanta ese papel cuando se trata de que los Estados miembros violen la legislación de la UE. Ahora la propia Comisión simplemente ignora al Tribunal de Justicia por tercera vez». *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu

CONCLUSIONES

PRIMERA. El imparable (y peligroso) aumento de las transferencias internacionales de datos de carácter personal. El acceso y uso de la información por parte de empresas, administraciones e individuos se ha convertido en un precioso bien intangible, causa y efecto a la vez de la progresiva integración económica y social. Junto a la dimensión económica, la protección de los datos personales y de la intimidad supone afrontar por vez primera la difícil tarea de compatibilizar los derechos fundamentales con el comercio internacional; y todo ello en cada una de las distintas esferas jurídicas implicadas. La búsqueda de una solución que ampare ambos intereses en las transferencias internacionales de datos en un contexto global no es fácil, debido, sobre todo, a las diferencias entre los distintos niveles de protección de los derechos y libertades de las personas y su intimidad existentes entre distintos estados. En este sentido, la búsqueda de soluciones uniformes ha de superar las distintas calificaciones en las categorías de datos personales y los distintos intereses económicos en juego, dada la original vinculación de los datos con el desarrollo del comercio internacional. Las acciones concertadas permitirían, además de un aumento de la eficacia y la seguridad jurídicas, la consecución de economías sobre los costes de circulación internacional de la información, impidiendo la constitución de los comentados «paraísos de datos» y la deslocalización de actividades informáticas.

La especial volatilidad de las transferencias internacionales de datos complica extraordinariamente la definición del derecho sustantivo aplicable. Las características de los flujos de información y el carácter abierto de las redes posibilitan el acceso a los datos, así como su recopilación y tratamientos desde varios países de manera simultánea, por lo que distintos estados tendrán competencia normativa para definir los términos y las condiciones de las prácticas apropiadas en el ámbito de la información.

SEGUNDA. Diferente enfoque acerca de la protección del derecho fundamental a la protección de datos de carácter personal entre la UE y los EE.UU. en tres actos. El fracaso de los *Safe Harbour* tuvo una razón de ser clara: ya que, a los ojos de la Directiva, era posible que las exportaciones de datos de carácter personal a los EE.UU. fueran prohibidas ya que mientras el enfoque de EE.UU. en esta materia se basaba en una mezcla de legislación, reglamentación y autorregulación, la UE consideraba imprescindible la protección del derecho fundamental a la privacidad.

Gráficamente podemos reseñar ese diferente enfoque en dos actos:

- Acto Primero: STJUE «Schrems I»:

  Varios fueron los interrogantes (sin respuesta) que las condiciones de aplicación e imposición del Acuerdo UE-EE.UU. nos planteó: ¿Qué repercusión tendrá en la función de las autoridades nacionales de control la elección de una sociedad estadounidense con quejas incursas ante un organismo específico?; en el ámbito europeo, cuando se tramiten las quejas, ¿cuáles serán las competencias respectivas de las autoridades nacionales de control y de la UE?; en el caso de procedimientos que tengan lugar en EE.UU. y en la UE de manera simultánea o sucesiva y que resulten en posturas contrarias respecto de una misma queja, ¿cómo se resolverán las diferencias?

  Y, sobre el contenido de los Principios de *Safe Harbour*, se debió poner la atención, en particular, en alguno de ellos: por un lado, hubiera sido aconsejable reforzar el Principio de «Opción», ya que los principios de puerto seguro no regulaban la legitimidad de los criterios de tratamiento; y, por otro lado, respecto del principio de «Acceso», pensamos que las excepciones que contenían las FAQ eran demasiado generales, era preciso abarcar los datos públicos; y, c) que los datos cuyo tratamiento vulnerase los principios habrían de corregirse o suprimirse. Quizás estos interrogantes precipitaron el resultado de sobra conocido por todos: el TJUE declaró inválida la Decisión 2000/520/CE que consideraba que los principios de Puerto Seguro garantizaban un nivel adecuado de protección de los datos transferidos desde la UE a empresas norteamericanas —(STJUE «Scherems I»)—.

- Acto Segundo: STJUE «Schrems II»:

  La STJUE «Schrems II» resolvió un total de once cuestiones prejudiciales planteadas por la High Court (Tribunal Superior, Irlanda), que el TJUE agrupó, para su resolución, en cinco cuestiones que se referían a la aplicabilidad del RGPD a las transferencia de datos a terceros países extracomunitarios, cuando en dichos países los datos pueden ser tratados por las autoridades con fines de seguridad nacional, defensa y seguridad del Estado; a los elementos integrantes del nivel de protección adecuado en terceros países; a las competencias y facultades de las autoridades de control en dichas transferencias; así como a la

validez tanto de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo bajo el prisma de la Carta de Derechos Fundamentales de la UE, como de la Decisión «Escudo de Privacidad», así como el grado de garantía de la tutela judicial efectiva que, para los ciudadanos de la Unión Europea, ofrece la figura del Defensor del Pueblo mencionado en esta última Decisión.

El TJUE interpretó el nivel de protección adecuado para la transferencia de datos a terceros países en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas las disposiciones normativas de los terceros países deben garantizar que los derechos de las personas cuyos datos personales se transfieren a dicho país, sobre la base de cláusulas tipo de protección de datos, gozan de un nivel de protección, sustancialmente, equivalente al garantizado dentro de la Unión Europea por el RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

En cuanto a las facultades de las autoridades de control competentes en el caso de transferencias de datos protegidos a terceros países extracomunitarios, diferencia el TJUE entre si existe o no de una decisión de adecuación dictada por la Comisión. En el caso de que exista una decisión de adecuación, y mientras que la misma no haya sido objeto de invalidación por el TJUE, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden adoptar medidas contrarias a esa decisión, aunque tienen la potestad de interponer recurso ante los tribunales nacionales para que estos formulen una cuestión prejudicial, ante el TJUE, sobre la validez de la decisión de adecuación. Por el contrario, en el caso de que no exista una decisión de adecuación emitida por la Comisión, el Tribunal resuelve que la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando esa autoridad de control considera, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero.

El TJUE, en la Sentencia «Schrems II», declaró la validez de la Decisión 2010/87/UE por cuanto que esta prevé mecanismos efectivos que permiten en la práctica garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas, incluyendo la posibilidad de control por las autoridades en el caso de que por el responsable del tratamiento no se suspenda o prohíba la transferencia.

> En consecuencia, el TJUE declaró la invalidez de la Decisión «Escudo de Privacidad» teniendo en cuenta, por una parte, que las injerencias resultantes de los programas de vigilancia basados en la normativa de los EE.UU. no ofrecen un nivel de protección, sustancialmente, equivalente al garantizado dentro de la Unión Europea por el RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea y, por otra parte, que el mecanismo del Defensor del Pueblo previsto en la Decisión «Escudo de Privacidad», no subsana las limitaciones al derecho a la tutela judicial efectiva, poniendo en entredicho la independencia del Defensor del Pueblo con respecto al poder ejecutivo de los EE.UU., poniendo de manifiesto, además, que no existe ninguna garantía legal que pueda ser invocada por los ciudadanos ante dicho Defensor del Pueblo, por lo que no se cumple con la exigencia de una vía de recurso efectivo garante del derecho a la tutela judicial efectiva en materia de protección de datos.

TERCERA. Hacia la restauración de la confianza y la estabilidad en los flujos de datos trasatlánticos. Las transferencias internacionales de datos de carácter personal UE-EE.UU. siguen al orden del día con el nuevo Acuerdo UE-EE.UU. flujos de datos transatlánticos.

El pasado 10 de julio de 2023 la Comisión Europea publicó su decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE.UU. Se convierte en la tercera decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE.UU. Los puntos clave de esta decisión son los siguientes: a) Los servicios de inteligencia estadounidenses deberán limitar su acceso a los datos de la UE que sean necesarios y proporcionados a la protección de la seguridad nacional en el seno de una investigación realizada de acuerdo con la normativa de inteligencia exterior de los EE.UU.; b) Los ciudadanos de la UE podrán acudir al nuevo Data Protection Review Court para impugnar las acciones y decisiones de las autoridades de inteligencia y para proteger sus derecho; c) Si el Data Protection Review Court concluye que se han recogido datos incumpliendo las nuevas garantías, podrá requerir la supresión de los mismos; d) Las nuevas garantías en materia de acceso a los datos por los servicios de inteligencia complementarán las obligaciones que las empresas estadounidenses que importen datos de la UE tendrán que asumir; e) Las empresas estadounidenses podrán adherirse al Marco de Privacidad de Datos UE-EE.UU. si se comprometen a cumplir una serie de obligaciones detalladas de privacidad y obtienen la aprobación del US Department of Commerce, que se encargará de revisar y monitorizar si dichas empresas cumplen los requisitos; f) Entre los requisitos a cumplir destaca la obligación de borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida; g) También destaca la obligación de garantizar la continuidad de la protección si se comparten los datos de carácter personal con terceros; h) En caso de tratamiento indebido de los datos por

parte de las empresas estadounidenses, los ciudadanos de la UE dispondrán de varias vías de reparación entre las que destacan los mecanismos de resolución independiente y gratuita de controversias y un tribunal arbitral; y, finalmente, i) Serán también aplicables las cláusulas contractuales tipo y las normas corporativas vinculantes. Como consecuencia de estas nuevas garantías, los datos personales transferidos por las empresas europeas a empresas estadounidenses al amparo del nuevo marco no necesitarán de establecer garantías adicionales de protección de datos[111].

En definitiva, este nuevo Marco de Privacidad de Datos UE-EE.UU. no da lugar a una equivalencia sustancial en el nivel de protección; se debería crear un mecanismo que garantice dicha equivalencia y que proporcionase el nivel adecuado de protección exigido por la legislación de la UE en materia de protección de datos y la Carta de Derechos Fundamentales de la UE, según la interpretación del TJUE y todas las recomendaciones formuladas, en su día, por el Parlamento Europeo y por el CEPD. Así las cosas, en un horizonte no muy lejano, se vislumbra un «Schrems III» … ¡Ojalá nos equivoquemos!

111 *Vid.* https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf

BIBLIOGRAFÍA BÁSICA CONSULTADA Y RECOMENDADA

Aced Félez, Emilio (2005). «Transferencias internacionales de datos», en Piñar Mañas, José Luis (Dir.) (2005), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua- Guatemala, 2-6 de junio de 2003)*, pp. 123-125. Valencia: Tirant lo blanch.

Arribas Luque, J. M. (2002), «Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: el sistema de principios de puerto seguro», en *La Ley*, núm. 5497, 7 de marzo de 2002.

González Vaqué, Luis (2006), «El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EE.UU. para la transmisión de los datos sobre los pasajeros por las compañías aéreas», en *Civitas. Revista Española de Derecho Europeo*, n.º 20, pp. 557-576.

Guasch Portas, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, 2014.

Hance, Oliver (1996), «Privacy and the Internet: Intrusion, Surveillance and Personal Data», en *International Review of Law Computers & Technology*, PP. 219-234. vol. 10, n.º 2.

López Álvarez, Luis Felipe, *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, Madrid, 2016.

López Carballo, Daniel, «A vueltas con las transferencias internacionales de datos: actualidad y seguridad jurídica», *Actualidad Jurídica Aranzadi*, núm. 922/2016, Aranzadi, Cizur Menor (Navarra), 2016.

Ortega Giménez, Alfonso, *Código Universitario de Derecho Internacional Privado. Tomos I y II*, Boletín Oficial del Estado, Madrid, 2023.

Ortega Giménez, **Alfonso**, «A la tercera no va la vencida: reservas del Comité Europeo de Protección de Datos al nuevo marco transatlántico de privacidad de datos», en *La Ley Privacidad*, n.º 16, julio 2023.

Ortega Giménez, **Alfonso**, *El intercambio de datos de carácter personal como paradigma de desarrollo de una economía global. Desde la óptica del Derecho internacional privado*, Monografía, Editorial Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2022.

Ortega Giménez, **Alfonso** y **García Escobar**, **Encarnación**, «Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 ("Schrems II")», en *La Ley Privacidad*, número 6, Editorial Wolters Kluwer, Madrid, 2020, pp. 1-22.

Ortega Giménez, **Alfonso**, «Tutela jurisdiccional ante un tratamiento ilícito internacional de datos personales y el nuevo Reglamento General de Protección de Datos de la Unión Europea», en *Revista Acta Judicial*, número 6, Ilustre Colegio Nacional de Letrados de la Administración de Justicia, Madrid, 2020, pp. 2-23

Ortega Giménez, **Alfonso**, «Hacia la "libre circulación de datos de carácter personal": el nuevo Reglamento General de Protección de Datos de la UE», en Ruda González, Albert y Jerez Delgado, Carmen (Directores), *Estudios sobre la Jurisprudencia Europea. Materiales del III Encuentro anual del Centro español European Law Institute*, volumen II, Editorial Jurídica Sepin, Madrid, 2020, pp. 1065-1075.

Ortega Giménez, **Alfonso**, «Tratamiento ilícito internacional de datos personales, reglamento general de protección de datos y derecho internacional privado: cuestiones de competencia judicial internacional y de determinación de la ley aplicable», Parte 3 -Capítulo I, La protección de datos en la era digital, en Fuentes Soriano, Olga (Directora), Arrabal Platero, Paloma; Doig Díaz, Yolanda; Ortega Giménez, Alfonso; Turégano Mansilla, Isabel (Coordinadores), *Era Digital, Sociedad y Derecho*, Tirant lo Blanch, Valencia, 2020, pp. 521-545.

Ortega Giménez, **Alfonso**, «El impacto del Reglamento General de Protección de Datos de la Unión Europea y de la LOPDGDD en el régimen jurídico de las transferencias internacionales de datos de carácter personal», en *El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de datos y garantía de los derechos digitales*, Editorial Tirant lo Blach, Valencia 2019, pp. 393-417.

Ortega Giménez, **Alfonso**, y **Gonzalo Domenech**, **Juan José**, «Las transferencias internacionales de datos de carácter personal en el nuevo Reglamento General de Protección de Datos», en *Revista Economist & Jurist*, Número 217, Difusión Jurídica, Barcelona, febrero 2018, pp. 36-43.

Ortega Giménez, **Alfonso**, «Impacto del nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea: del "safe harbour" al "privacy shield"», en *Revista Digital Administrativo*, Editorial jurídica Sepin, n.º 24, SP/DOCT/73156, Artículo Monográfico. Enero 2018.

Ortega Giménez, **Alfonso**, *El nuevo régimen jurídico de la Unión Europea para las empresas en materia de protección de datos de carácter personal*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017.

Ortega Giménez, **Alfonso**, *Transferencias Internacionales de Datos de Carácter Personal Ilícitas*, Thomson Reuters Aranzadi, Cizur Menor, Navarra, 2017.

Rodríguez Ayuso, **Juan Francisco**, «Anulación del Privacy Shield en las transferencias internacionales de datos: ¿presenciamos un desplazamiento fáctico de la responsabilidad?», en *Revista Boliviana de Derecho*, n.º 31, enero 2021, pp. 426-503.

Sancho Villa, **Diana**, *Negocios internacionales de tratamiento de datos personales*, Navarra, Civitas, 2010.

Sancho Villa, **Diana**, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003.

ANEXO

DECISIÓN DE EJECUCIÓN DE LA COMISIÓN de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre UE y los EE.UU.



Bruselas, 10.7.2023
C(2023) 4745 final

DECISIÓN DE EJECUCIÓN DE LA COMISIÓN de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre UE y los EE.UU.

(Texto pertinente a efectos del EEE)

DECISIÓN DE EJECUCIÓN DE LA COMISIÓN de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre UE y los EE.UU.

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

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

Considerando que:

1. INTRODUCCIÓN

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

---

1 DO L 119 de 4.5.2016, p. 1.

2 Para facilitar la consulta, en el Anexo VIII figura una lista de las abreviaturas utilizadas en la presente Decisión.

3 Véase el considerando 101 del Reglamento (UE) 2016/679.

(2) De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, la Comisión puede decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país garantizan un nivel de protección adecuado. Bajo esta condición, las transferencias de datos personales a un tercer país pueden tener lugar sin necesidad de obtener ninguna otra autorización, tal como se establece en el artículo 45, apartado 1, y en el considerando 103 del Reglamento (UE) 2016/679.

(3) Como se especifica en el artículo 45, apartado 2, del Reglamento (UE) 2016/679, la adopción de una decisión de adecuación debe basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, que abarque tanto las normas aplicables a los importadores de datos como las limitaciones y salvaguardias en lo que respecta al acceso a los datos personales por parte de las autoridades públicas. En su evaluación, la Comisión tiene que determinar si el tercer país en cuestión garantiza un nivel de protección "esencialmente equivalente" al garantizado en la Unión (considerando 104 del Reglamento (UE) 2016/679). Si este es el caso debe evaluarse con arreglo a la legislación de la Unión, en particular el Reglamento (UE) 2016/679, así como a la jurisprudencia del Tribunal de Justicia de la Unión Europea (el Tribunal de Justicia)[4] .

(4) Como aclaró el Tribunal de Justicia en su sentencia de 6 de octubre de 2015 en el asunto C- 362/14, *Maximillian Schrems/Comisario de Protección de Datos*[5] *(Schrems)*, ello no exige constatar un nivel de protección idéntico. En particular, los medios a los que recurre el tercer país en cuestión para proteger los datos personales pueden diferir de los empleados en la Unión, siempre que resulten, en la práctica, eficaces para garantizar un nivel de protección adecuado[6] . Por tanto, la norma de adecuación no exige una réplica punto por punto de las normas de la Unión. Más bien, la prueba consiste en determinar si, a través del contenido de los derechos a la intimidad y de su aplicación, supervisión y cumplimiento efectivos, el sistema extranjero en su conjunto ofrece el nivel de protección requerido[7]. Además, según dicha sentencia, al aplicar este criterio, la Comisión debe apreciar, en particular, si el marco jurídico del tercer país de que se trate prevé normas destinadas a limitar las injerencias en los derechos fundamentales de las personas cuyos datos se transfieren desde la Unión, que las entidades estatales de ese país estarían autorizadas a realizar cuando persiguen objetivos legítimos, como la seguridad nacional, y ofrece una protección jurídica eficaz contra las injerencias de ese tipo[8]. El "Referencial de Adecuación" del Consejo Europeo de Protección de Datos, que trata de aclarar aún más esta norma, también ofrece orientaciones a este respecto[9].

---

4 Véase, más recientemente, el asunto C-311/18, Facebook Ireland y *Schrems* (*Schrems II*) ECLI:EU:C:2020:559.

5 Caso C-362/14, *Maximilian Schrems v. Data Protección de datos Comisario (Schrems)*, ECLI:EU:C:2015:650, apartado 73.

6 *Schrems*, apartado 74.

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

8 *Schrems*, párrafo 88-89.

9 Consejo Europeo de Protección de Datos, Referencial de Adecuación, WP 254 rev. 01.disponible en el siguiente enlace: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

(5) La norma aplicable con respecto a dicha injerencia en los derechos fundamentales a la intimidad y a la protección de datos fue aclarada de nuevo por el Tribunal de Justicia en su sentencia de 16 de julio de 2020 en el asunto C-311/18, *Comisario de Protección de Datos contra Facebook Ireland Limited y Maximillian Schrems (Schrems II)*, que invalidó la Decisión de Ejecución (UE) 2016/1250 de la Comisión[10] sobre un marco anterior de flujo de datos transatlántico, el Escudo de Privacidad UE-EE.UU. (Privacy Shield). El Tribunal de Justicia consideró que las limitaciones a la protección de datos personales derivadas de El Derecho interno de Estados Unidos sobre el acceso y la utilización por las autoridades públicas de ese país de datos transferidos de la Unión a Estados Unidos con fines de seguridad nacional no se circunscribía de modo que cumpliera requisitos esencialmente equivalentes a los del Derecho de la Unión, en lo que respecta a la necesidad y proporcionalidad de tales injerencias en el derecho a la protección de datos[11] . El Tribunal de Justicia consideró asimismo que no existía ninguna vía de recurso ante un organismo que ofreciera a las personas cuyos datos fueron transferidos a Estados Unidos garantías esencialmente equivalentes a las exigidas por el artículo 47 de la Carta sobre el derecho a la tutela judicial efectiva[12].

(6) A raíz de la sentencia *Schrems II*, la Comisión entabló conversaciones con el Gobierno de Estados Unidos con vistas a una posible nueva decisión de adecuación que cumpliera los requisitos del artículo 45, apartado 2, del Reglamento (UE) 2016/679, según la interpretación del Tribunal de Justicia. Como resultado de estos debates, los Estados Unidos adoptaron el 7 de octubre de 2022 la Orden Ejecutiva 14086 "Mejora de las salvaguardias para las actividades de inteligencia de señales de los Estados Unidos" (OE 14086), que se complementa con un Reglamento sobre el Tribunal de Revisión de Protección de Datos emitido por el Fiscal General de los Estados Unidos (Reglamento AG)[13]. Además, se ha actualizado el marco que se aplica a las entidades comerciales que tratan datos transferidos desde la Unión en virtud de la presente Decisión: el "Marco de protección de datos UE-EE.UU." (EU-U.S. DPF o DPF).

(7) La Comisión ha analizado detenidamente la legislación y la práctica de los Estados Unidos, incluidas la OE 14086 y el Reglamento AG. Sobre la base de las constataciones expuestas en los considerandos 9 a 200, la Comisión concluye que los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos en virtud del DPF UE-EE.UU. desde un responsable o un encargado del tratamiento de la Unión[14] a organizaciones certificadas de los Estados Unidos.

---

10 Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección conferida por la UE-. Escudo de privacidad de Estados Unidos (DO L 207 de 1.8.2016, p. 1).

11 *Schrems II*, apartado 185.

12 *Schrems II*, apartado 197.

13 28 CFR Parte 302.

14 La presente Decisión es pertinente a efectos del EEE. El Acuerdo sobre el Espacio Económico Europeo (Acuerdo EEE) prevé la ampliación del mercado interior de la Unión Europea a los tres Estados del EEE: Islandia, Liechtenstein y Noruega. La Decisión del Comité Mixto por la que se incorpora el Reglamento (UE) 2016/679 al anexo XI del Acuerdo EEE fue adoptada por el Comité Mixto del EEE el 6 de julio de 2018 y entró en vigor el 20 de

(8) La presente Decisión tiene por efecto que las transferencias de datos personales de los responsables y encargados del tratamiento de la Unión[15] a organizaciones certificadas de los Estados Unidos puedan tener lugar sin necesidad de obtener ninguna otra autorización. No afecta a la aplicación directa del Reglamento (UE) 2016/679 a dichas organizaciones cuando se cumplan las condiciones relativas al ámbito de aplicación territorial de dicho Reglamento, establecidas en su artículo 3.

2. EL MARCO DE PROTECCIÓN DE DATOS UE-EE.UU.

2.1. Ámbito personal y material

2.1.1. Organizaciones certificadas

(9) El DPF UE-EE.UU. se basa en un sistema de certificación por el que las organizaciones estadounidenses se comprometen a respetar una serie de principios de protección de la intimidad -los "Principios del Marco de Protección de la Intimidad de los Datos UE-EE.UU.", incluidos los Principios Complementarios (en lo sucesivo, "los Principios")- publicados por el Departamento de Comercio de EE.UU. (DoC) y recogidos en el anexo I de la presente Decisión[16]. Para poder optar a la certificación con arreglo al DPF UE-EE.UU., una organización debe estar sujeta a los poderes de investigación y ejecución de la Comisión Federal de Comercio (FTC) o del Departamento de Transporte (DoT) de EE.UU.[17]. Los principios excepciones, por ejemplo, con respecto a los bancos, las compañías aéreas, el negocio de los seguros y las actividades de transporte común de los proveedores de servicios de telecomunicaciones (aunque la decisión del Tribunal de Apelación de los Estados Unidos para el Noveno Circuito, de 26 de febrero de 2018, en el caso FTC c. AT&T, ha confirmado que la FTC tiene jurisdicción sobre los servicios no se aplican inmediatamente después de la certificación. Como se explica con más detalle en los considerandos 48 a 52, las organizaciones de DPF de la UE y EE.UU. deben volver a certificar anualmente su adhesión a los Principios[18].

julio de 2018. Por lo tanto, el Reglamento está cubierto por dicho Acuerdo. A efectos de la Decisión, debe entenderse, por tanto, que las referencias a la UE y a los Estados miembros de la UE abarcan también a los Estados del EEE.

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

16 Véase a este respecto *Schrems*, apartado 81, en el que el Tribunal de Justicia confirmó que un sistema de autocertificación puede garantizar un nivel de protección adecuado.

17 Anexo I, sección I.2. La FTC tiene una amplia jurisdicción sobre las actividades comerciales, con algunas actividades de transporte común de dichas entidades). Véase también el anexo IV, nota 2. El DoT es competente para exigir el cumplimiento por parte de las compañías aéreas y los agentes de venta de billetes (para el transporte aéreo), véase el anexo V, apartado A.

18 Anexo I, sección III.6.

2.1.2. Definición de datos personales y conceptos de responsable del tratamiento y "agente"

(10) La protección que ofrece el DPF UE-EE.UU. se aplica a cualquier dato personal transferido desde la Unión a organizaciones de EE.UU. que hayan certificado su adhesión a los Principios ante la DdC, con la excepción de los datos que se recojan para la publicación, emisión u otras formas de comunicación pública de material periodístico e información en material previamente publicado difundido desde archivos de medios de comunicación[19]. Por lo tanto, dicha información no puede transferirse sobre la base de los Principios de la UE- DPF ESTADOUNIDENSE.

(11) Los Principios definen los datos personales/la información personal del mismo modo que el Reglamento (UE) 2016/679, es decir, como "datos sobre una persona física identificada o identificable que entran en el ámbito de aplicación del RGPD recibidos por una organización en Estados Unidos procedentes de la UE, y registrados en cualquier forma[20]. En consecuencia, también cubren los datos de investigación seudonimizados (o "codificados con clave") (incluso cuando la clave no se comparte con la organización estadounidense receptora)[21]. Del mismo modo, el concepto de tratamiento se define como "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación o difusión, así como su supresión o destrucción"[22].

(12) El DPF UE-EE.UU. se aplica a las organizaciones de EE.UU. que reúnen las condiciones de responsables del tratamiento (es decir, como persona u organización que, sola o junto con otras, determina los fines y medios del tratamiento de datos personales)[23] o encargados del tratamiento (es decir, agentes que actúan en nombre de un responsable del tratamiento)[24]. Los encargados del tratamiento estadounidenses deben estar obligados contractualmente a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la UE y a ayudar a este último a responder a las personas que ejerzan sus derechos en virtud de los Principios[25]. Además, en caso de subtratamiento, el encargado del tratamiento debe celebrar un contrato con el subencargado del tratamiento que garantice el mismo nivel de protección que el previsto en los Principios y adoptar medidas para garantizar su correcta aplicación[26].

---

19 Anexo I, sección III.2.

20 Anexo I, sección I.8.a.

21 Anexo I, sección III.14.g.

22 Anexo I, sección I.8.b.

23 Anexo I, sección I.8.c.

24 Véase, por ejemplo, el anexo I, sección II.2.b y secciones II.3.b y 7.d, que dejan claro que los agentes actúan en nombre de un responsable del tratamiento, sujetos a las instrucciones de este último y bajo obligaciones contractuales específicas.

25 Anexo I, sección III.10.a. Véanse también las orientaciones elaboradas por el DoC, en consulta con el Consejo Europeo de Protección de Datos, en el marco del Escudo de la privacidad, que aclaran las obligaciones de los encargados del tratamiento estadounidenses que reciben datos personales de la Unión en virtud de dicho marco. Dado que estas normas no han cambiado, estas orientaciones/FAQ sigue siendo pertinentes en el sitio UE-EE.UU. DPF (https://www.privacyshield.gov/article?id=Processing-FAQs).

26 Anexo I, sección II.3.b.

(13) Los datos personales deben tratarse de forma lícita y leal. Deben recogerse con un fin específico y utilizarse posteriormente sólo en la medida en que ello no sea incompatible con la finalidad del tratamiento.

2.2. Principios del marco de privacidad de datos UE-EE.UU.

2.2.1. Limitación de la finalidad y elección

(14) En virtud del DPF UE-EE.UU., esto se garantiza a través de diferentes Principios. En primer lugar, en virtud del *Principio de integridad de los datos y limitación de la finalidad*, de manera similar a lo dispuesto en el artículo 5, apartado 1, letra b), del Reglamento (UE) 2016/679, una organización no podrá tratar datos personales de manera incompatible con la finalidad para la que fueron recogidos originalmente o para la que fueron autorizados posteriormente por el interesado[27].

(15) En segundo lugar, antes de utilizar los datos personales para una finalidad nueva (modificada) que sea materialmente diferente pero aún compatible con la finalidad original, o de divulgarlos a un tercero, la organización debe ofrecer a los interesados la oportunidad de oponerse (opt-out), de conformidad con el Principio de *Elección*[28], a través de un mecanismo claro, visible y fácilmente dis-

27 Anexo I, sección II.5.a. Los fines compatibles pueden incluir la auditoría, la prevención del fraude u otros fines coherentes con las expectativas de una persona razonable dado el contexto de la recogida (véase el anexo I, nota 6).

28 Esto no se aplica cuando una organización proporciona datos personales a un encargado del tratamiento que actúa en su nombre y bajo sus instrucciones (anexo I, sección II.2.b). Dicho esto, en este caso la organización debe tener un contrato en vigor y garantizar el cumplimiento del Principio de *responsabilidad en las transferencias ulteriores*, tal como se describe con más detalle en el considerando 43. Además, el Principio de Elección no se aplica cuando una organización proporciona datos personales a un encargado del tratamiento que actúa en su nombre y bajo sus instrucciones. Además, el Principio de *Elección* (así como el Principio de *Notificación*) puede restringirse cuando los datos personales se tratan en el contexto de la diligencia debida (como parte de una posible fusión o adquisición) o de auditorías, en la medida y durante el tiempo que sea necesario para cumplir requisitos legales o de interés público, o en la medida y durante el tiempo que la aplicación de estos Principios perjudique los intereses legítimos de la organización en el contexto específico de las investigaciones de diligencia debida o auditorías (Anexo I, Sección III.4). El Principio Suplementario 15 (Anexo I, Sección
III.15.a y b) también prevé una excepción al Principio de Elección (así como a los Principios de *Notificación y Responsabilidad en las Transferencias Ulteriores*) para los datos personales procedentes de fuentes accesibles al público (a menos que el exportador de datos de la UE indique que la información está sujeta a restricciones que requieren la aplicación de dichos principios) o los datos personales recogidos de registros abiertos a la consulta del público en general (siempre que no se combinen con información de registros no públicos y se respeten las condiciones de consulta). Del mismo modo, el Principio Suplementario 14 (Anexo I, Sección III.14.f prevé una excepción al Principio de Elección (así como a los Principios de *Notificación y de Responsabilidad en las Transferencias Ulteriores*) para el tratamiento de datos personales por parte de una empresa farmacéutica o de productos sanitarios para actividades de seguimiento de la seguridad y eficacia de los productos, en la medida en que la adhesión a los Principios interfiera con el cumplimiento de los requisitos reglamentarios.

ponible. Es importante señalar que este principio no sustituye a la prohibición expresa de tratamiento incompatible[29].

2.2.2. Tratamiento de categorías especiales de datos personales

(16) Deben existir salvaguardias específicas cuando se traten "categorías especiales" de datos.

(17) De acuerdo con el *Principio de Elección*, se aplican salvaguardias específicas al tratamiento de "información sensible", e s decir, datos personales que especifican condiciones médicas o de salud, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, información sobre la vida sexual de la persona o cualquier otra información recibida de un tercero que sea identificada y tratada por éste como sensible[30]. Esto significa que cualquier dato que se considere sensible con arreglo a la legislación de protección de datos de la Unión (incluidos los datos sobre orientación sexual, datos genéticos y datos biométricos) será tratado como sensible con arreglo al DPF UE- EE.UU. por las organizaciones certificadas.

(18) Como norma general, las organizaciones deben obtener el consentimiento afirmativo y expreso (es decir, el consentimiento expreso) de las personas para utilizar información sensible con fines distintos de aquellos para los que se recogió originalmente o para los que la persona la autorizó posteriormente (mediante el consentimiento expreso), o para divulgarla a terceros[31].

(19) No es necesario obtener dicho consentimiento en circunstancias limitadas similares a excepciones comparables previstas en la legislación de protección de datos de la Unión, por ejemplo, cuando el tratamiento de datos sensibles redunde en el interés vital de una persona; sea necesario para el establecimiento de reclamaciones legales; o se requiera para proporcionar atención médica o diagnóstico[32].

---

29 Esto se aplica a todas las transferencias de datos con arreglo al DPF UE-EE.UU., incluso cuando se refieren a datos recogidos en el contexto de la relación laboral. Por lo tanto, aunque una organización estadounidense certificada puede, en principio, utilizar datos de recursos humanos para fines diferentes no relacionados con el empleo (por ejemplo, determinadas comunicaciones de marketing), debe respetar la prohibición de tratamiento incompatible y, además, sólo puede hacerlo de conformidad con los principios de *notificación y elección*. Excepcionalmente, una organización puede utilizar datos personales para un fin compatible adicional sin proporcionar notificación y opción, pero sólo en la medida y durante el período necesarios para evitar perjudicar la capacidad de la organización a la hora de tomar promociones, nombramientos u otras decisiones de empleo similares (véase el anexo I, sección III.9.b.(iv)). La prohibición de que la organización estadounidense adopte cualquier medida punitiva contra el empleado por ejercer dicha elección, incluida cualquier restricción de las oportunidades de empleo, garantizará que, a pesar de la relación de subordinación y dependencia inherente, el empleado estará libre de presiones y, por tanto, podrá ejercer una auténtica libre elección. Véase el anexo I, sección III.9.b.(i).

30 Anexo I, Sección II,2.c.

31 Anexo I, sección II.2.c.

32 Anexo I, sección III.1.

2.2.3. Precisión, minimización y seguridad de los datos

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

(21) En virtud *del principio de integridad de los datos y limitación de su finalidad*[33], los datos personales deben limitarse a lo que sea pertinente para los fines del tratamiento. Además, las organizaciones deben, en la medida necesaria para los fines del tratamiento, adoptar medidas razonables para garantizar que los datos personales sean fiables para el uso previsto, exactos, completos y actuales.

(22) Además, la información personal sólo podrá conservarse en una forma que identifique o haga identificable a una persona (y, por tanto, en forma de datos personales)[34] durante el tiempo en que sirva a los fines para los que fue inicialmente recogida o posteriormente autorizada por la persona de conformidad con el *Principio de Elección*. Esta obligación no impide que las organizaciones sigan tratando información personal durante períodos más largos, pero sólo durante el tiempo y en la medida en que dicho tratamiento sirva razonablemente a uno de los siguientes fines específicos, similares a excepciones comparables previstas en la legislación de la Unión en materia de protección de datos: archivo en interés público, periodismo, literatura y arte, investigación científica e histórica y análisis estadístico[35]. Cuando los datos personales se conserven para uno de estos fines, su tratamiento estará sujeto a las garantías previstas en los Principios[36].

(23) Los datos personales también deben tratarse de forma que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida accidental, destrucción o daños. A tal fin, los responsables y encargados del tratamiento deben adoptar las medidas técnicas u organizativas adecuadas para proteger los datos personales de posibles amenazas. Estas medidas deben evaluarse teniendo en cuenta el estado de la técnica, los costes correspondientes y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos de las personas.

(24) En virtud del DPF UE-EE.UU., esto se garantiza mediante el *Principio de Seguridad*, que exige, de forma similar al artículo 32 del Reglamento (UE) 2016/679, adoptar medidas de seguridad razonables y apropiadas, teniendo en cuenta los riesgos que entraña el tratamiento y la naturaleza de los datos[37].

---

33 Anexo I, sección II.5.

34 Véase el anexo I, nota 7, que aclara que una persona se considera "identificable" siempre que una organización o un tercero pueda identificarla razonablemente, teniendo en cuenta los medios de identificación que sea razonablemente probable que se utilicen (considerando, entre otras cosas, el coste y el tiempo necesarios para la identificación y la tecnología disponible en el momento del tratamiento).

35 Anexo I, sección II.5.b.

36 *Ibid*.

37 Anexo I, Sección II.4.a. Además, en lo que respecta a los datos de recursos humanos, la DPF UE- EE.UU. exige a los empresarios que se adapten a las preferencias de privacidad de los empleados restringiendo el acceso a los datos personales, anonimizando determi-

2.2.4. Transparencia

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

(26) Esto se garantiza a través del *Principio de Notificación*[38], que, de forma similar a los requisitos de transparencia en virtud del Reglamento (UE) 2016/679, exige a las organizaciones que informen a los interesados, entre otras cosas, sobre (i) la participación de la organización en el DPF, (ii) el tipo de datos recopilados, (iii) la finalidad del tratamiento, (iv) el tipo o la identidad de los terceros a los que se pueden revelar los datos personales y los fines para hacerlo, (v) sus derechos individuales, (vi) cómo ponerse en contacto con la organización y (vii) las vías de recurso disponibles.

(27) Este aviso debe facilitarse en un lenguaje claro y visible cuando s e pida por primera vez a los individuos que proporcionen los datos personales o tan pronto como sea posible después, pero en cualquier caso antes de que los datos se utilicen para un fin materialmente diferente (pero compatible) de aquel para el que se recogieron, o antes de que se revelen a un tercero[39].

(28) Además, las organizaciones deben hacer públicas sus políticas de privacidad que reflejen los Principios (o, en el caso de los datos de recursos humanos, ponerlas a disposición de las personas afectadas) y proporcionar enlaces al sitio web de la DdC (con más detalles sobre la certificación, los derechos de los interesados y los mecanismos de recurso disponibles), la Lista del Marco de Privacidad de Datos (Lista DPF) de organizaciones participantes y el sitio web de un proveedor alternativo de resolución de litigios adecuado[40].

---

nados datos o asignando códigos o seudónimos (Anexo I, Sección III.9.b.(iii).

38 Anexo I, sección II.1.

39 Anexo I, Sección II.1.b. El Principio Complementario 14 (Anexo I, Sección III.14.b y c) establece disposiciones específicas para el tratamiento de datos personales en el contexto de la investigación sanitaria y los ensayos clínicos. En concreto, este Principio permite a las organizaciones tratar datos de ensayos clínicos incluso después de que una persona se retire del ensayo, si así se dejó claro en el aviso que se le facilitó cuando aceptó participar. Del mismo modo, cuando una organización de DPF de la UE recibe datos personales con fines de investigación sanitaria, sólo puede utilizarlos para una nueva actividad de investigación de conformidad con los principios de *notificación y elección*. En este caso, la notificación a la persona deberá, en principio, proporcionar información sobre cualquier futuro uso específico de los datos (por ejemplo, estudios relacionados). Cuando no sea posible incluir desde el principio todos los usos futuros de los datos (porque pueda surgir un nuevo uso de investigación a partir de nuevos conocimientos o avances médicos o de investigación), deberá incluirse una explicación de que los datos pueden utilizarse en futuras actividades imprevistas de investigación médica y farmacéutica. Si ese nuevo uso no es coherente con los fines generales de investigación para los que se recogieron los datos (es decir, si los nuevos fines son materialmente diferentes, pero siguen siendo compatibles con el fin original, véanse los considerandos 14-15), deberá obtenerse un nuevo consentimiento (es decir, consentimiento previo). Véanse además las restricciones/excepciones específicas al principio de *notificación* descritas en la nota 28.

40 Anexo I, sección III.6.d.

2.2.5. Derechos individuales

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

(30) *El principio de acceso*[41] del DPF UE-EE.UU. otorga a las personas tales derechos. En concreto, los interesados tienen derecho, sin necesidad de justificación, a obtener de una organización confirmación de si está tratando datos personales relacionados con ellos; a que se les comuniquen los datos; y a obtener información sobre la finalidad del tratamiento, las categorías de datos personales que se tratan y los destinatarios (o categorías de destinatarios) a los que se comunican los datos[42]. Las organizaciones están obligadas a responder a las solicitudes de acceso en un plazo razonable[43]. Una organización podrá establecer límites razonables al número de veces dentro de un período determinado que se atenderán las solicitudes de acceso de una persona concreta y podrá cobrar una tasa que no sea excesiva, por ejemplo, cuando las solicitudes sean manifiestamente excesivas, en particular debido a su carácter repetitivo[44].

(31) El derecho de acceso sólo podrá restringirse en circunstancias excepcionales similares a las previstas en la legislación de protección de datos de la Unión, en particular cuando se vulneren los derechos legítimos de terceros; cuando la carga o el coste de facilitar el acceso sean desproporcionados en relación con los riesgos para la intimidad de la persona en las circunstancias del caso (aunque el coste y la carga no son factores determinantes para determinar si facilitar el acceso es razonable); en la medida en que sea probable que la divulgación interfiera con la salvaguardia de intereses públicos compensatorios importantes, como la seguridad nacional, la seguridad pública o la defensa; la información contenga información comercial confidencial; o la información se procese únicamente con fines de investigación o estadísticos[45]. Cualquier denegación o limitación de un derecho debe ser necesaria y estar debidamente justificada, y la entidad debe demostrar que se cumplen estos requisitos[46]. Al llevar a cabo dicha evaluación, la organización deberá tener especialmente en cuenta los intereses de la persona[47]. Cuando sea posible separar la información de otros datos a los que se aplique una restricción, la entidad deberá suprimir la información protegida y divulgar el resto de la información[48].

(32) Además, los interesados tienen derecho a obtener la rectificación o modificación de los datos inexactos y a obtener la supresión de los datos que se hayan

---

41 Véase también el Principio Complementario sobre "Acceso" (Anexo I, Sección III.8).

42 Anexo I, sección III.8.a.(i)-(ii).

43 Anexo I, sección III.8.i.

44 Anexo I, sección III.8.f.(i)-(ii) y g.

45 Anexo I, sección III.4; 8.b, c, e; 14.e, f y 15.d.

46 Anexo I, sección III . 8.e.(ii). La organización debe informar a la persona de los motivos de la denegación/restricción y proporcionar un punto de contacto para cualquier consulta adicional, Sección III.8.a.(iii).

47 Anexo I. Sección III.8.a.(ii)-(iii).

48 Anexo I, sección III.8.a.(i).

tratado infringiendo los Principios[49]. Además, como se explica en el considerando 15, las personas tienen derecho a oponerse al tratamiento de sus datos para fines materialmente distintos (pero compatibles) de aquellos para los que se recogieron los datos y a la divulgación de sus datos a terceros. Cuando los datos personales se utilicen con fines de venta directa, las personas tienen derecho a oponerse al tratamiento en cualquier momento[50].

(33) Los Principios no abordan específicamente la cuestión de las decisiones que afectan al interesado basadas únicamente en el tratamiento automatizado de datos personales. Sin embargo, como por lo que respecta a los datos personales que se han recogido en la Unión, cualquier decisión basada en el tratamiento automatizado será tomada normalmente por el responsable del tratamiento en la Unión (que tiene una relación directa con el interesado en cuestión) y, por lo tanto, está directamente sujeta al Reglamento (UE) 2016/679[51]. Esto incluye los supuestos de transferencia en los que el tratamiento es llevado a cabo por un operador comercial extranjero (por ejemplo, de Estados Unidos) que actúa como agente (encargado del tratamiento) en nombre del responsable del tratamiento en la Unión (o como subencargado del tratamiento que actúa en nombre del responsable del tratamiento en la Unión habiendo recibido los datos de un responsable del tratamiento en la Unión que los recogió) que, sobre esta base, toma la decisión.

(34) Esto fue confirmado por un estudio encargado por la Comisión en 2018 en el contexto de la segunda revisión anual del funcionamiento del Escudo de Privacidad[52], que concluyó que, en ese momento, no había pruebas que sugirieran que las organizaciones del Escudo de Privacidad estuvieran llevando a cabo normalmente la toma de decisiones automatizada sobre la base de los datos personales transferidos en virtud del Escudo de Privacidad.

(35) En cualquier caso, en los ámbitos en los que es más probable que las empresas recurran al tratamiento automatizado de datos personales para tomar decisiones que afectan al individuo (por ejemplo, concesión de créditos, ofertas de hipotecas, empleo, vivienda y seguros), la legislación estadounidense ofrece protecciones específicas contra las decisiones adversas[53]. Estas leyes suelen establecer

---

49 Anexo I, sección II.6 y III.8.a.(i).

50 Anexo I, sección III.8.12.

51 Por el contrario, en el caso excepcional de que la organización estadounidense tenga una relación directa con el interesado de la Unión, esto será normalmente consecuencia de que se haya dirigido a la persona en la Unión ofreciéndole bienes o servicios o supervisando su comportamiento. En este supuesto, la propia organización estadounidense entrará en el ámbito de aplicación del Reglamento (UE) 2016/679 (artículo 3, apartado 2) y, por tanto, deberá cumplir directamente la legislación de la Unión en materia de protección de datos.

52 SWD(2018)497 final, sección 4.1.5. El estudio se centró en: i) la medida en que las organizaciones del Escudo de la privacidad en los Estados Unidos toman decisiones que afectan a las personas basándose en el tratamiento automatizado de datos personales transferidos desde empresas de la UE en el marco del Escudo de la privacidad; y ii) las salvaguardias para las personas que la legislación federal estadounidense prevé para este tipo de situaciones y las condiciones para que se apliquen dichas salvaguardias.

53 Véanse, por ejemplo, la Ley de igualdad de oportunidades de crédito (15 U.S.C. 1691 y ss.), la Ley de informes de crédito justos (15 USC § 1681 y siguientes), o la Ley de Vivienda Justa (42 U.S.C. 3601 y siguientes). Además, Estados Unidos ha suscrito los Principios

que las personas tienen derecho a ser informadas de las razones específicas que subyacen a la decisión (por ejemplo, la denegación de un crédito), a impugnar la información incompleta o inexacta (así como la confianza en factores ilícitos) y a solicitar reparación. En el ámbito del crédito al consumo, la Fair Credit Reporting Act (FCRA) y la Equal Credit Opportunity Act (ECOA) contienen salvaguardias que proporcionan a los consumidores algún tipo de derecho a recibir explicaciones y a impugnar la decisión. Estas leyes son pertinentes en una amplia gama de ámbitos, como el crédito, el empleo, la vivienda y los seguros. Además, algunas leyes antidiscriminatorias, como el Título VII de la Ley de Derechos Civiles y la Ley de Vivienda Justa, protegen a las personas frente a los modelos utilizados en la toma de decisiones automatizada que podrían dar lugar a discriminación por determinadas características, y conceden a las personas el derecho a impugnar tales decisiones, incluidas las automatizadas. Con respecto a la información sanitaria, la Ley de Portabilidad y Responsabilidad de los Seguros de Salud (HIPAA) crea ciertos derechos que son similares a los del Reglamento (UE) 2016/679 con respecto al acceso a la información sanitaria personal. Además, las orientaciones de las autoridades estadounidenses exigen que los proveedores médicos reciban información que les permitan informar a las personas de los sistemas automatizados de toma de decisiones utilizados en el sector médico[54].

(36) Por lo tanto, estas normas ofrecen protecciones similares a las previstas en la legislación de protección de datos de la Unión en la improbable situación de que las decisiones automatizadas sean tomadas por la propia organización DPF UE-EE.UU.

2.2.6. Restricciones a las transferencias ulteriores

(37) El nivel de protección concedido a los datos personales transferidos desde la Unión a organizaciones de Estados Unidos no debe verse menoscabado por la posterior transferencia de dichos datos a un destinatario de Estados Unidos o de otro tercer país.

(38) En virtud *del principio de responsabilidad por las transferencias ulteriores*[55], se aplican normas especiales a las denominadas "transferencias ulteriores", es decir, las transferencias de datos personales de una organización de DPF de la UE y Estados Unidos a un tercero responsable o encargado del tratamiento, independientemente de que este último esté situado en Estados Unidos o en un tercer país fuera de Estados Unidos (y de la Unión). Cualquier transferencia ulterior sólo puede tener lugar (i) para fines limitados y especificados, (ii) sobre la base de un contrato entre la organización de DPF UE-EE.UU. y el tercero[56] (o

---

de Inteligencia Artificial de la Organización de Cooperación y Desarrollo Económicos, que incluyen, entre otros, principios sobre transparencia, capacidad de explicación, seguridad y responsabilidad.

54 Véanse, por ejemplo, las orientaciones disponibles en 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

55 Véase el anexo I, sección II.3 y el principio complementario "Contratos obligatorios para transferencias ulteriores" (anexo I, sección III.10).

56 Como excepción a este principio general, una organización puede transferir datos personales de un pequeño número de empleados sin celebrar un contrato con el destinatario para necesidades operativas ocasionales relacionadas con el empleo, por ejemplo, la

un acuerdo comparable dentro de un grupo empresarial[57]) y (iii) sólo si dicho contrato exige que el tercero proporcione el mismo nivel de protección que el garantizado por los Principios.

(39) Esta obligación de proporcionar el mismo nivel de protección que garantizan los Principios, leída en combinación con el *Principio de Integridad de los Datos y Limitación de la Finalidad*, significa en particular que el tercero sólo podrá tratar la información personal que se le transmita para fines que no sean incompatibles con los fines para los que fue recogida o posteriormente autorizados por la persona (de conformidad con el Principio de Elección).

(40) El *principio de responsabilidad de la transferencia* ulterior también debe leerse en conjunción con el *principio de notificación* y, en el caso de una transferencia ulterior a un tercero responsable del tratamiento[58], con el principio de elección, según el cual los interesados deben ser informados (entre otras cosas) sobre el tipo/identidad de cualquier tercero destinatario, la finalidad de la transferencia ulterior y la opción ofrecida, y pueden oponerse (opt out) o, en el caso de datos sensibles, tienen que dar su "consentimiento afirmativo expreso" (opt in) para la transferencia ulterior.

(41) La obligación de proporcionar el mismo nivel de protección que exigen los Principios se aplica a todos y cada uno de los terceros implicados en el tratamiento de los datos así transferidos, con independencia de su ubicación (en EE.UU. o en otro tercer país), así como cuando el propio tercero destinatario original transfiere esos datos a otro tercero destinatario, por ejemplo con fines de subtratamiento.

(42) En todos los casos, el contrato con el tercero destinatario debe estipular que éste notificará a la organización DPF UE-EE.UU. si determina que ya no puede cumplir con su obligación. Cuando se llegue a tal determinación, el tratamiento por parte del tercero deberá cesar o deberán tomarse otras medidas razonables y apropiadas para remediar la situación[59].

---

reserva de un vuelo, una habitación de hotel o la cobertura de un seguro. Sin embargo, también en este caso, la organización debe cumplir los principios de *notificación y elección* (véase el anexo I, sección III.9.e).

57 Véase el principio complementario "Contratos obligatorios para transferencias ulteriores" (anexo I, sección III.10.b). Aunque este principio permite las transferencias basadas también en instrumentos no contractuales (por ejemplo, programas de cumplimiento y control intragrupo), el texto deja claro que estos instrumentos deben siempre "garantizar la continuidad de la protección de la información personal con arreglo a los Principios". Además, dado que la organización estadounidense certificada seguirá siendo responsable del cumplimiento de los Principios, tendrá un fuerte incentivo para utilizar instrumentos que sean realmente eficaces en la práctica.

58 Las personas no tendrán derecho de exclusión voluntaria cuando los datos personales se transfieran a un tercero que actúe como agente para realizar tareas en nombre y bajo las instrucciones de la organización estadounidense. Sin embargo, esto requiere un contrato con el agente y la organización estadounidense tendrá la responsabilidad de garantizar las protecciones previstas en los Principios mediante el ejercicio de sus poderes de instrucción.

59 La situación es diferente según que el tercero sea un responsable del tratamiento o un encargado del tratamiento (agente). En el primer caso, el contrato con el tercero debe prever que éste cese el tratamiento o adopte otras medidas razonables y adecuadas para remediar la situación. En el segundo supuesto, corresponde a la UE La organización esta-

(43) Se aplican protecciones adicionales en caso de transferencia ulterior a un agente tercero (es decir, un encargado del tratamiento). En tal caso, la organización estadounidense debe asegurarse de que el agente sólo actúe siguiendo sus instrucciones y tome las medidas razonables y apropiadas (i) para garantizar que el agente procese efectivamente la información personal transferida de forma coherente con las obligaciones de la organización en virtud de los Principios y, (ii) para detener y remediar el procesamiento no autorizado, previa notificación[60]. La DdC podrá exigir a la organización que facilite una copia resumida o representativa de las disposiciones sobre privacidad del contrato[61] . Cuando surjan problemas de cumplimiento en una cadena de (sub)tratamiento, la organización que actúe como responsable del tratamiento de los datos personales se enfrentará en principio a la responsabilidad, tal como se especifica en el *Principio de recurso, ejecución y responsabilidad*, excepto si demuestra que no es responsable del hecho que dio lugar al daño[62].

2.2.7. Rendición de cuentas

(44) En virtud del principio de responsabilidad, las entidades que tratan datos están obligadas a establecer medidas técnicas y organizativas adecuadas para cumplir efectivamente sus obligaciones en materia de protección de datos y poder demostrar dicho cumplimiento, en particular ante la autoridad de control competente.

(45) Una vez que una organización ha decidido voluntariamente certificar[63] con arreglo al DPF UE-EE.UU., su cumplimiento efectivo de los Principios es obligatorio y exigible. En virtud *del principio de recurso, ejecución y responsabilidad*[64], las organizaciones del DPF UE-EE.UU. deben proporcionar mecanismos eficaces para garantizar el cumplimiento de los Principios. Las organizaciones también deben tomar medidas para verificar[65] que sus políticas de privacidad se ajustan a los Principios y que de hecho se cumplen. Esto puede hacerse bien mediante un sistema de autoevaluación, que debe incluir procedimientos internos que garanticen que los empleados reciben formación sobre la aplicación de las políticas de privacidad de la organización y que el cumplimiento se revisa periódicamente de forma objetiva, o bien mediante revisiones externas del cumplimiento, cuyos métodos pueden incluir auditorías, controles aleatorios o el uso de herramientas tecnológicas.

(46) Además, las organizaciones deben conservar registros sobre la aplicación de sus prácticas de DPF UE-EE.UU. y ponerlos a disposición, previa solicitud, en el contexto de una investigación o una denuncia por incumplimiento ante un organismo independiente de resolución de litigios o una autoridad competente en la aplicación de la normativa[66].

---

dounidense de DPF -como la que controla el tratamiento bajo cuyas instrucciones opera el agente- debe adoptar estas medidas. Véase el anexo I, sección II.3.

60 Anexo I, sección II.3.b.

61 *Ibid*.

62 Anexo I, sección II.7.d.

63 Véase también el principio complementario "Autocertificación" (anexo I, sección III.6).

64 Véase también el principio complementario "Resolución de litigios y ejecución" (Anexo I, sección III.11).

65 Véase también el principio complementario "Verificación" (anexo I, sección III.7).

66 Anexo I, sección III.7.

2.3. Administración, supervisión y aplicación

(47) El DPF UE-EE.UU. será administrado y supervisado por el DoC. El Marco prevé mecanismos de supervisión y aplicación para verificar y garantizar que las organizaciones del DPF UE-EE.UU. cumplen los Principios y que se aborda cualquier incumplimiento. Estos mecanismos se establecen en los Principios (Anexo I) y en los compromisos asumidos por el DoC (Anexo III), la FTC (Anexo IV) y el DoT (Anexo V).

2.3.1. (Re)certificación

(48) Para certificarse con arreglo al DPF UE-EE.UU. (o recertificarse anualmente), las organizaciones deben declarar públicamente su compromiso de cumplir los Principios, poner a disposición sus políticas de privacidad y aplicarlas plenamente[67]. Como parte de su (re-) solicitud de certificación, las organizaciones tienen que presentar información a la DdC sobre, entre otras cosas, el nombre de la organización pertinente, una descripción de los fines para los que la organización tratará los datos personales, los datos personales que estarán cubiertos por la certificación, así como el método de verificación elegido, el mecanismo de recurso independiente pertinente y el organismo estatutario que tiene jurisdicción para exigir el cumplimiento de los Principios[68].

(49) Las organizaciones pueden recibir datos personales sobre la base del DPF UE-EE.UU. a partir de la fecha en que el DoC las incluya en la lista de DPF. Para garantizar la seguridad jurídica y evitar "falsas alegaciones", las organizaciones que se certifican por primera vez no pueden hacer referencia pública a su adhesión a los Principios antes de que el DoC haya determinado que la presentación de certificación de la organización está completa y haya añadido la organización a la lista DPF[69]. Para poder seguir dependiendo del DPF UE-EE.UU. para recibir datos personales de la Unión, dichas organizaciones deben volver a certificar anualmente su participación en el marco. Cuando una organización abandona el DPF UE-EE.UU. por cualquier motivo, debe eliminar todas las declaraciones que impliquen que la organización sigue participando en el Marco[70].

(50) Como se refleja en los compromisos establecidos en el anexo III, la DdC verificará si las organizaciones cumplen todos los requisitos de certificación y han establecido una política de privacidad (pública) que contenga la información requerida en virtud del *principio de notificación*[71]. Basándose en la experiencia adquirida con el proceso de (re)certificación en el marco del Escudo de la privacidad, la DdC llevará a cabo una serie de comprobaciones, entre ellas verificar si las políticas de privacidad de las organizaciones contienen un hiperenlace al formulario de reclamación correcto en el sitio web del mecanismo de resolución de litigios pertinente y, cuando varias entidades y filiales de una organización estén incluidas en una presentación de certificación, si las políticas de pri-

67 Anexo I, Sección I. 2.

68 Anexo I, sección III.6.b y Anexo III, véase la sección "Verificar los requisitos de autocertificación".

69 Anexo I, nota 12.

70 Anexo I, sección III.6.h.

71 Anexo I, sección III.6.a y nota a pie de página 12, así como y Anexo III, véase la sección "Verificar los requisitos de autocertificación".

vacidad de cada una de esas entidades cumplen los requisitos de certificación y son fácilmente accesibles a disposición de los interesados[72] . Además, cuando sea necesario, el DoC realizará comprobaciones cruzadas con la FTC y el DoT para verificar que las organizaciones están sujetas al organismo de supervisión identificado en sus presentaciones de (re)certificación, y trabajará con los organismos de resolución alternativa de litigios para verificar que las organizaciones están registradas para el mecanismo de recurso independiente identificado en su presentación de (re)certificación[73].

(51) La DdC informará a las organizaciones de que, para completar la (re)certificación, deben abordar todas las cuestiones identificadas durante su revisión. En caso de que una organización n o responda en el plazo establecido por la DdC (por ejemplo, en lo que respecta a la recertificación, se espera que el proceso se complete en 45 días)[74] o no complete su certificación, la presentación se considerará abandonada. En ese caso, cualquier tergiversación sobre la participación o el cumplimiento del DPF UE-EE.UU. podrá ser objeto de medidas coercitivas por parte de la FTC o el DoT[75].

(52) Para garantizar la correcta aplicación del DPF UE-EE.UU., las partes interesadas, como los interesados, los exportadores de datos y las autoridades nacionales de protección de datos (APD), deben poder identificar a las organizaciones que se adhieren a los Principios. Para garantizar dicha transparencia en el "punto de entrada", la DdC se ha comprometido a mantener y poner a disposición del público la lista de organizaciones que han certificado su adhesión a los Principios y que se encuentran dentro de la jurisdicción de al menos una de las autoridades de control mencionadas en los anexos IV y V de la presente Decisión[76]. El DoC actualizará la lista sobre la base de la presentación anual de recertificación de una organización y siempre que una organización se retire o sea eliminada del DPF UE-EE.UU.. Además, para garantizar la transparencia también en el "punto de salida", el DoC mantendrá y pondrá a disposición del público un registro de las organizaciones que hayan sido eliminadas de la lista, identificando en cada caso el motivo de dicha eliminación[77]. Por último, proporcionará un enlace a la página web de la FTC sobre el DPF UE-EE.UU., en la que se enumerarán las medidas de ejecución de la FTC en virtud del Marco[78].

---

72 Anexo III, sección "Verificar los requisitos de autocertificación.

73 Del mismo modo, la DdC colaborará con el tercero que actuará como depositario de los fondos recaudados mediante una tasa para el panel de APD (véase el considerando 73) para verificar que las organizaciones que eligen las APD como su mecanismo de recurso independiente han abonado la tasa correspondiente al año en cuestión. Véase el anexo III, sección "Verificar los requisitos de autocertificación".

74 Anexo III, nota 2.

75 Véase el anexo III, sección "Verificar los requisitos de autocertificación".

76 Encontrará información sobre la gestión de la Lista DPF en el Anexo III (véase la introducción bajo el epígrafe "Administración y supervisión del Programa Marco de Privacidad de Datos por el Departamento de Comercio") y en el Anexo I (Sección I.3, Sección I.4, III.6.d, y Sección III.11.g).

77 Anexo III, véase la introducción bajo "Administración y supervisión del programa marco de privacidad de datos por el Departamento de Comercio".

78 Véase el anexo III, sección "Adaptar el sitio web del marco de privacidad de datos a audiencias específicas".

2.3.2. Control del cumplimiento

(53) El DoC supervisará de forma continua el cumplimiento efectivo de los Principios por parte de las organizaciones de DPF de la UE y de EE.UU. a través de diferentes mecanismos[79]. En particular, llevará a cabo "controles aleatorios" de organizaciones seleccionadas al azar, así como controles aleatorios *ad hoc* de organizaciones específicas cuando se detecten posibles problemas de cumplimiento (por ejemplo, notificados a la DdC por terceros) para verificar si (i) el punto o puntos de contacto para la tramitación de reclamaciones y solicitudes de los interesados están disponibles y responden; (ii) la política de privacidad de la organización está fácilmente disponible, tanto en su sitio web como a través de un hipervínculo en el sitio web de la DdC; (iii) la política de privacidad de la organización sigue cumpliendo los requisitos de certificación y (iv) el mecanismo independiente de resolución de conflictos elegido por las organizaciones está disponible para tramitar las reclamaciones[80].

(54) Si existen pruebas creíbles de que una organización no cumple sus compromisos en virtud del DPF UE-EE.UU. (incluso si la DoC recibe quejas o la organización no responde satisfactoriamente a las indagaciones de la DoC), la DoC exigirá a la organización que cumplimente y envíe un cuestionario detallado[81]. La organización que no responda satisfactoria y puntualmente al cuestionario será remitida a la autoridad competente (la FTC o el DoT) para la posible adopción de medidas coercitivas[82]. Como parte de sus actividades de supervisión del cumplimiento en el marco del Escudo de la privacidad, el DoC llevó a cabo periódicamente los controles aleatorios mencionados en el considerando 53 y supervisó continuamente los informes públicos, lo que le permitió identificar, abordar y resolver los problemas de cumplimiento[83]. Las organizaciones que incumplan persistentemente los Principios serán eliminadas de la Lista DPF y deberán devolver o suprimir los datos personales recibidos en virtud del Marco[84].

---

79 Véase el anexo III, sección "Realización de revisiones y evaluaciones periódicas de oficio del cumplimiento del programa marco de privacidad de datos".

80 Como parte de sus actividades de supervisión, el DoC puede utilizar diferentes herramientas, entre ellas comprobar si hay enlaces rotos a las políticas de privacidad o vigilar activamente las noticias en busca de informes que aporten pruebas creíbles de incumplimiento.

81 Véase el anexo III, sección "Realización de revisiones y evaluaciones periódicas de oficio del cumplimiento del programa marco de privacidad de datos".

82 Véase el anexo III, sección "Realización de revisiones y evaluaciones periódicas de oficio del cumplimiento del programa marco de privacidad de datos".

83 Durante la segunda revisión anual del Escudo de la privacidad, el DoC informó de que había realizado controles aleatorios de 100 organizaciones y enviado cuestionarios de cumplimiento en 21 casos (tras lo cual se rectificaron los problemas detectados), véase SWD (2018) 497 final de la Comisión, p. 9. Del mismo modo, el DoC informó durante la tercera revisión anual del Escudo de la privacidad de que había detectado tres incidentes a través de su supervisión de los informes públicos y había iniciado la práctica de realizar controles aleatorios de 30 empresas cada mes, lo que dio lugar a un seguimiento con cuestionarios de cumplimiento en el 28 % de los casos (tras lo cual los problemas detectados se rectificaron inmediatamente o, en tres casos, se resolvieron tras una carta de advertencia), véase SWD de la Comisión (2019) 495 final, p. 8.

84 Anexo I, sección III.11.g. Un incumplimiento persistente se produce, en particular, cuando

(55) En otros casos de supresión, como la retirada voluntaria de la participación o la falta de recertificación, la organización debe suprimir o devolver los datos, o puede conservarlos, siempre que afirme anualmente a la DdC su compromiso de seguir aplicando los Principios o proporcione una protección adecuada de los datos personales por otro medio autorizado (por ejemplo, utilizando un contrato que refleje plenamente los requisitos de las cláusulas contractuales tipo pertinentes aprobadas por la Comisión)[85] . En este caso, una organización también tiene que identificar un punto de contacto dentro de la organización para todas las cuestiones relacionadas con los DPF UE-EE.UU.

2.3.3. Identificación y tratamiento de las declaraciones falsas de participación

(56) La DdC controlará cualquier declaración falsa de participación en el DPF UE-EE.UU. o el uso indebido de la marca de certificación DPF UE-EE.UU., tanto de oficio como sobre la base de denuncias (por ejemplo, recibidas de las APD)[86] . En particular, el DoC verificará de forma continuada que las organizaciones que (i) se retiren de la participación en el DPF UE-EE.UU., (ii) no completen la recertificación anual (es decir, que hayan iniciado el proceso de recertificación anual pero no lo hayan completado a tiempo o que ni siquiera lo hayan iniciado el proceso de recertificación anual), iii) sean dadas de baja como participantes, en particular por "incumplimiento persistente", o iv) no completen una certificación inicial (es decir, hayan iniciado el proceso de certificación inicial, pero no lo hayan completado a su debido tiempo), eliminen de cualquier política de privacidad publicada pertinente las referencias al DPF UE-EE.UU. que impliquen que la organización participa activamente en el Marco[87] . El DoC también realizará búsquedas en Internet para identificar referencias al DPF UE-EE.UU. en las políticas de privacidad de las organizaciones, incluso para identificar declaraciones falsas de organizaciones que nunca participaron en el DPF UE-EE.UU.[88].

(57) Cuando el DoC compruebe que no se han eliminado las referencias al DPF UE-EE.UU. o que se utilizan indebidamente, informará a la organización sobre una posible remisión a la FTC/DoT[89]. Si una organización no responde satisfactoriamente, el DoC remitirá el asunto a la agencia pertinente para una posible acción coercitiva[90]. Cualquier tergiversación al público en general por parte de una organización en relación con su adhesión a los Principios en forma de declaraciones o prácticas engañosas está sujeta a medidas coercitivas por parte de la FTC, el DoT u otras autoridades coercitivas estadounidenses pertinentes. Las declaraciones falsas al DoC son exigibles en virtud de la Ley de Declaraciones Falsas (18 U.S.C. § 1001).

---

una organización se niega a cumplir una resolución firme de cualquier autoridad de autorregulación de la privacidad, de resolución independiente de litigios o de ejecución.

85 Anexo I, sección III.6.f.

86 Anexo III, sección "Búsqueda y tratamiento de solicitudes falsas de participación".

87 *Ibid*.

88 *Ibid*.

89 *Ibid*.

90 En el marco del Escudo de la privacidad, el DoC informó durante la tercera revisión anual del marco que había identificado 669 casos de falsas declaraciones de participación (entre octubre de 2018 y octubre de 2019), la mayoría de los cuales se resolvieron después de la carta de advertencia del DoC, con 143 casos remitidos a la FTC (véase el considerando 62 a continuación). Véase el documento SWD (2019) 495 final de la Comisión, p. 10.

2.3.4. Ejecución

(58) Para garantizar en la práctica un nivel adecuado de protección de datos, debe existir una autoridad de control independiente con competencias para supervisar y hacer cumplir las normas de protección de datos.

(59) Las organizaciones de DPF UE-EE.UU. deben estar sujetas a la jurisdicción de las autoridades estadounidenses competentes -la FTC y el DoT-, que disponen de los poderes de investigación y ejecución necesarios para garantizar eficazmente el cumplimiento de los Principios[91].

(60) La FTC es una autoridad independiente compuesta por cinco Comisarios, nombrados por el Presidente con el asesoramiento y consentimiento del Senado[92]. Los Comisionados son nombrados por un periodo de siete años y sólo pueden ser destituidos por el Presidente por ineficacia, negligencia en el cumplimiento del deber o mala conducta en el cargo. La FTC no puede tener más de tres Comisionados del mismo partido político y los Comisionados no pueden, durante su nombramiento, dedicarse a ningún otro negocio, vocación o empleo.

(61) La FTC puede investigar el cumplimiento de los Principios, así como las afirmaciones falsas de adhesión a los Principios o de participación en el DPF UE-EE.UU. por parte de organizaciones que ya no figuran en la lista de DPF o que nunca han certificado[93]. La FTC puede imponer el cumplimiento solicitando órdenes administrativas o de los tribunales federales (incluidas las "órdenes de consentimiento" logradas a través de acuerdos)[94] para medidas cautelares preliminares o permanentes u otros recursos, y supervisará sistemáticamente el cumplimiento de dichas órdenes[95]. Cuando las organizaciones incumplan dichas órdenes, la FTC podrá solicitar sanciones civiles y otras reparaciones, incluido cualquier perjuicio causado por la conducta ilegal. Cada orden de consentimiento emitida a una organización de DPF UE-EE.UU. tendrá disposiciones de autoinforme[96], y se exigirá a las organizaciones que hagan públicas todas las secciones pertinentes relacionadas con DPF UE-EE.UU. de cualquier informe de cumplimiento o eva-

---

91 Una organización de DPF de la UE y EE.UU. tiene que declarar públicamente su compromiso de cumplir los Principios, divulgar sus políticas de privacidad de acuerdo con estos Principios y aplicarlos plenamente. El incumplimiento es exigible en virtud del artículo 5 de la Ley FTC, que prohíbe los actos desleales y engañosos en el comercio o que afecten a éste (15 U.S.C. §45), y del artículo 49 U.S.C. §41712, que prohíbe a un transportista o agente de venta de billetes realizar prácticas desleales o engañosas en el transporte aéreo o en la venta de transporte aéreo.

92 15 U.S.C. § 41.

93 Anexo IV.

94 Según la información facilitada por la FTC, no está facultada para realizar inspecciones in situ en el ámbito de la protección de la intimidad. Sin embargo, está facultada para obligar a las organizaciones a presentar documentos y prestar declaración a testigos (véase el artículo 20 de la Ley de la FTC), y puede recurrir al sistema judicial para hacer cumplir dichas órdenes en caso de incumplimiento.

95 Véase el anexo IV, sección "Órdenes de búsqueda y seguimiento".

96 La FTC o las órdenes judiciales pueden exigir a las empresas que apliquen programas de privacidad y que pongan periódicamente a disposición de la FTC informes de cumplimiento o evaluaciones de terceros independientes sobre dichos programas.

luación presentado a la FTC. Por último, la FTC mantendrá una lista en línea de organizaciones sujetas a órdenes de la FTC o de los tribunales en casos de DPF UE-EE.UU.[97].

(62) Por lo que respecta al Escudo de la privacidad, la FTC adoptó medidas coercitivas en unos 22 casos, tanto en relación con infracciones de requisitos específicos del marco (por ejemplo, no afirmar a la DoC que la organización seguía aplicando las protecciones del Escudo de la privacidad después de abandonar el marco, no verificar, mediante una autoevaluación o una revisión externa del cumplimiento, que la organización cumplía el marco)[98] como con falsas afirmaciones de participación en el marco (por ejemplo, por parte de organizaciones que no completaron los pasos necesarios para obtener la certificación o permitieron que su certificación caducara pero falsearon su participación continuada en el marco).p. ej. por organizaciones que no completaron los pasos necesarios para obtener la certificación, o que dejaron que su certificación caducara pero falsearon su participación continuada)[99] . Esta acción coercitiva se derivó, entre otras cosas, del uso proactivo de citaciones administrativas para obtener materiales de determinados participantes en el Escudo de la privacidad con el fin de comprobar si se habían producido violaciones sustantivas de las obligaciones del Escudo de la privacidad[100].

(63) En términos más generales, la FTC ha adoptado en los últimos años medidas coercitivas en una serie de casos relativos al cumplimiento de requisitos específicos de protección de datos que también se contemplan en la DPF UE-EE. UU., por ejemplo en lo que respecta a los principios de limitación de la finalidad y conservación de datos[101], minimización de datos[102], seguridad de datos[103] y exactitud de datos[104].

---

97 Anexo IV, sección "Órdenes de búsqueda y seguimiento".

98 Comisión SWD (2019) 495 final, p. 11.

99 Véanse los casos enumerados en el sitio web de la FTC, disponible a través de https:// www.ftc.gov/business-guidance/privacy- security/privacy-shield. Véanse también SWD de la Comisión (2017) 344 final, p. 17; SWD de la Comisión (2018) 497 final, p. 12 y SWD de la Comisión (2019) 495 final, p. 11.

100 Véase, por ejemplo, Prepared Remarks of Chairman Joseph Simons at the Second Privacy Shield Annual Review (ftc.gov).

101 Véase, por ejemplo, la orden de la FTC en el caso Drizly, LLC, en la que, entre otras cosas, se exige a la empresa (1) que destruya todos los datos personales que haya recopilado y que no sean necesarios para proporcionar productos o servicios a los consumidores, (2) que se abstenga de recopilar o almacenar información personal a menos que sea necesaria para fines específicos descritos en un calendario de conservación.

102 Véase, por ejemplo, la orden de la FTC en *CafePress* (24 de marzo de 2022) que exige, entre otras cosas, reducir al mínimo la cantidad de datos que se recopilan.

103 Véase, por ejemplo, la acción coercitiva de la FTC en Drizzly, LLC y *CafePress*, donde exigió a las empresas en cuestión que pusieran en marcha un programa de seguridad específico o medidas de seguridad concretas. Además, en lo que respecta a las violaciones de datos, véase también la orden de la FTC de 27 de enero de 2023 en Chegg, el acuerdo alcanzado con Equifax en 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/ equifax-pay-575-million-part- settlement-ftc-cfpb-states-related-2017-data-breach).

104 Véase, por ejemplo, el caso de RealPage, Inc (16 de octubre de 2018), en el que la FTC adoptó medidas coercitivas en virtud de la FCRA contra una empresa de selección de

(64) El DoT tiene autoridad exclusiva para regular las prácticas de privacidad de las compañías aéreas, y comparte jurisdicción con la FTC respecto a las prácticas de privacidad de los agentes de venta de billetes en la venta de transporte aéreo. Los funcionarios del DoT intentan en primer lugar llegar a un acuerdo y, si esto no es posible, pueden iniciar procedimientos de aplicación que implican una audiencia probatoria ante un juez de derecho administrativo del DoT que tiene autoridad para emitir órdenes de cese y sanciones civiles[105]. Los jueces de derecho administrativo se benefician de varias protecciones en virtud de la Ley de Procedimiento Administrativo (APA) para garantizar su independencia e imparcialidad. Por ejemplo, sólo pueden ser destituidos por causa justificada; se les asignan casos por rotación; no pueden desempeñar funciones incompatibles con sus deberes y responsabilidades como jueces de derecho administrativo; no están sujetos a la supervisión del equipo de investigación de la autoridad para la que trabajan (en este caso, el DoT); y deben llevar a cabo su función de adjudicación/aplicación de forma imparcial[106]. El DoT se ha comprometido a supervisar las órdenes de ejecución y a garantizar que las órdenes resultantes de los procedimientos de infracción de la UE se ejecuten de forma imparcial. Los casos de DPF en EE.UU. están disponibles en su sitio web[107].

2.4. Reparación

(65) Para garantizar una protección adecuada y, en particular, el respeto de los derechos individuales, el interesado debe disponer de vías de recurso administrativas y judiciales eficaces.

(66) El DPF UE-EE.UU., a través del *Principio de Recurso, Ejecución y Responsabilidad*, exige a las organizaciones que proporcionen recursos a las personas afectadas por el incumplimiento y, por tanto, la posibilidad de que los interesados de la Unión presenten reclamaciones relativas al incumplimiento por parte de las organizaciones del DPF UE-EE.UU. y de que estas reclamaciones se resuelvan, en caso necesario, mediante una decisión que proporcione una solución efectiva[108]. Como parte de su certificación, las organizaciones deben satisfacer los requisitos de este Principio proporcionando mecanismos de recurso independientes, efectivos y fácilmente disponibles, mediante los cuales las reclamaciones y disputas de cada individuo puedan ser investigadas y resueltas rápidamente sin coste alguno para el individuo[109].

---

inquilinos que facilitaba informes de antecedentes de personas a inmobiliarias, propietarios y empresas de gestión inmobiliaria, basándose en información procedente de historiales de alquiler, información de registros públicos (incluidos historiales penales y de desahucios) e información crediticia, que se utilizaban como factor para determinar la elegibilidad para una vivienda. La FTC descubrió que la empresa no tomaba medidas razonables para garantizar la exactitud de la información que proporcionaba en base a su herramienta de autodecisión.

105 Véase el anexo V, sección "Prácticas de aplicación".

106 Véanse 5 U.S.C. §§ 3105, 7521(a), 554(d) y 556(b)(3).

107 Anexo V, véase la sección "Seguimiento y publicación de las órdenes de ejecución relativas a las infracciones de los DPF UE-EE.UU.".

108 Anexo I, sección II.7.

109 Anexo I, sección III.11.

(67) Las organizaciones pueden elegir mecanismos de recurso independientes en la Unión o en Estados Unidos. Como se explica con más detalle en el considerando 73, esto incluye la posibilidad de comprometerse voluntariamente a cooperar con las APD de la UE. Cuando las organizaciones traten datos de recursos humanos, dicho compromiso de cooperar con las APD de la UE es obligatorio. Otras alternativas incluyen la resolución alternativa independiente de litigios o programas de privacidad desarrollados por el sector privado que incorporen los Principios a sus normas. Estos últimos deben incluir mecanismos efectivos de aplicación de conformidad con los requisitos del *Principio de recurso, aplicación y responsabilidad*.

(68) En consecuencia, el DPF UE-EE.UU. ofrece a los interesados una serie de posibilidades para hacer valer sus derechos, presentar reclamaciones por incumplimiento por parte de las organizaciones UE-EE.UU. y que sus reclamaciones se resuelvan, en caso necesario, mediante una decisión, proporcionar un recurso efectivo. Los particulares pueden presentar una denuncia directamente a una organización, a un organismo independiente de resolución de litigios designado por la organización, a las APD nacionales, a la DdC o a la FTC. En los casos en que sus reclamaciones no hayan sido resueltas por ninguno de estos mecanismos de recurso o ejecución, los particulares también tienen derecho a invocar un arbitraje vinculante (Anexo I del Anexo I de la presente Decisión). Salvo en el caso del panel arbitral, que exige que se hayan agotado determinadas vías de recurso antes de poder invocarlo, los particulares son libres de recurrir a cualquiera de los mecanismos de reparación de su elección, o a todos ellos, y no están obligados a elegir un mecanismo en lugar de otro ni a seguir una secuencia específica.

(69) En primer lugar, los interesados de la Unión pueden reclamar en caso de incumplimiento de los Principios a través de contactos directos con las organizaciones UE-EE.UU. de DPF[110]. Para facilitar la resolución, la organización debe establecer un mecanismo de recurso eficaz para tramitar dichas reclamaciones. Por lo tanto, la política de privacidad de una organización debe informar claramente a los particulares sobre un punto de contacto, dentro o fuera de la organización, que se encargará de las reclamaciones (incluido cualquier establecimiento pertinente de la Unión que pueda responder a consultas o reclamaciones), así como sobre el organismo independiente de resolución de litigios designado (véase el considerando 70). Una vez recibida la reclamación de un particular, directamente de éste o a través de la DdC tras su remisión por una APD, la organización debe proporcionar una respuesta al interesado de la Unión en un plazo de 45 días[111]. Del mismo modo, las organizaciones están obligadas a responder con prontitud a las consultas y otras solicitudes de información de la DdC o de una APD[112] (cuando la organización se haya comprometido a cooperar con la APD) en relación con su adhesión a los Principios.

(70) En segundo lugar, los particulares también pueden presentar una reclamación directamente ante el organismo independiente de resolución de litigios (ya sea en Estados Unidos o en la Unión) designado por una organización para

110 Anexo I, sección III.11.d.(i).

111 Anexo I, sección III.11.d.(i).

112 Se trata de la autoridad de tratamiento designada por el grupo de APD previsto en el Principio complementario sobre "La función de las autoridades de protección de datos" (anexo I, sección III.5).

investigar y resolver las reclamaciones individuales (a menos que sean manifiestamente infundadas o frívolas) y para proporcionar un recurso adecuado y gratuito al particular[113]. Las sanciones y vías de recurso impuestas por dicho organismo deberán ser lo suficientemente rigurosas como para garantizar el cumplimiento de los Principios por parte de las organizaciones y deberán prever la reversión o corrección por parte de la organización de los efectos del incumplimiento y, dependiendo de las circunstancias, el cese del tratamiento ulterior de los datos personales en cuestión y/o su supresión, así como la publicidad de las constataciones de incumplimiento[114]. Los organismos independientes de resolución de litigios designados por una organización están obligados a incluir en sus sitios web públicos información pertinente sobre el DPF UE- EE.UU. y los servicios que prestan en virtud del mismo[115]. Cada año, deben publicar un informe anual con estadísticas agregadas sobre estos servicios[116].

(71) Como parte de sus procedimientos de revisión del cumplimiento, el DoC puede verificar que las organizaciones de DPF de la UE y de EE.UU. están realmente registradas en los mecanismos de recurso independientes que ellos afirman estar registrados en[117]. Tanto las organizaciones como los mecanismos de recurso independientes responsables deberán responder con prontitud a las consultas y solicitudes de información del DoC en relación con el DPF UE-EE.UU.. El DoC trabajará con los mecanismos de recurso independientes para verificar que incluyen información en sus sitios web sobre los Principios y los servicios que prestan en el marco del DPFUE-EE.UU. y que publican informes anuales[118].

(72) En los casos en que la organización incumpla la resolución de un organismo de resolución de litigios o de autorregulación, éste deberá notificar dicho incumplimiento al DoC y a la FTC (u otra autoridad estadounidense con jurisdicción para investigar el incumplimiento por parte de la organización), o a un tribunal competente[119]. Si una organización se niega a cumplir una resolución firme de cualquier organismo autorregulador de la privacidad, de resolución de litigios independiente o gubernamental, o si dicho organismo determina que una organización incumple con frecuencia los Principios, esto puede considerarse un incumplimiento persistente, con el resultado de que el DoC, tras notificarlo primero con 30 días de antelación y dar la oportunidad de responder a la organización que ha incumplido,

113 Anexo I, sección III.11.d.

114 Anexo I, sección II.7 y III.11.e.

115 Anexo I, sección III.11.d.(ii).

116 El informe anual debe incluir: (1) el número total de reclamaciones relacionadas con el DPF UE-EEUU recibidas durante el año del informe; (2) los tipos de reclamaciones recibidas; (3) las medidas de calidad de la resolución de conflictos, como el tiempo que se tarda en tramitar las reclamaciones; y (4) los resultados de las reclamaciones recibidas, especialmente el número y los tipos de soluciones o sanciones impuestas.

117 Anexo I, sección "Verificar los requisitos de autocertificación".

118 Véase el anexo III, sección "Facilitar la cooperación con los órganos alternativos de resolución de litigios que prestan servicios relacionados con los Principios". Véase también el anexo I, sección III.11.d.(ii)-(iii).

119 Véase el anexo I, sección III.11.e.

eliminará a la organización de la lista de DPF[120]. Si, una vez eliminada de la lista, la organización sigue alegando la certificación DPF UE-EE.UU., el DoC la remitirá a la FTC o a otro organismo de ejecución[121].

(73) En tercer lugar, los particulares también pueden presentar sus denuncias ante una APD nacional de la Unión, que puede hacer uso de sus competencias de investigación y reparación en virtud del Reglamento (UE) 2016/679. Las organizaciones están obligadas a cooperar en la investigación y la resolución de una denuncia por parte de una APD, ya sea cuando se trate del tratamiento de datos de recursos humanos recogidos en el contexto de una relación laboral o cuando la organización respectiva se haya sometido voluntariamente a la supervisión de las APD[122]. En particular, las organizaciones tienen que responder a las preguntas, cumplir los consejos de la APD, incluidas las medidas correctoras o compensatorias, y proporcionar a la APD una confirmación por escrito de que se han tomado dichas medidas[123]. En caso de incumplimiento de las recomendaciones de la APD, ésta remitirá el caso al DoC (que podrá retirar a las organizaciones de la lista de APD UE-EE.UU.) o, para posibles medidas coercitivas, a la FTC o al DoT (la falta de cooperación con las APD o de cumplimiento de los Principios es perseguible con arreglo a la legislación estadounidense)[124].

(74) A fin de facilitar la cooperación para una tramitación eficaz de las denuncias, tanto el DoC como la FTC han establecido un punto de contacto específico que se encarga de relacionarse directamente con las APD[125]. Estos puntos de contacto ayudan con las consultas de las APD sobre el cumplimiento de los Principios por parte de una organización.

(75) El asesoramiento proporcionado por los APD[126] se emite después de que ambas partes en litigio hayan tenido una oportunidad razonable de presentar sus observaciones y aportar las pruebas que deseen. El panel puede emitir su dictamen tan pronto como lo permita el requisito del debido proceso y, por regla general, en un plazo de 60 días a partir de la recepción de la reclamación[127]. Si una organización no cumple en un plazo de 25 días a partir de la entrega del asesoramiento y no ha ofrecido una explicación satisfactoria del retraso, el panel puede notificar su intención de someter el asunto a la FTC (u otra autoridad estadounidense competente en la aplicación de la ley) o concluir que se ha incumplido gravemente el compromiso de cooperación. En la primera alternativa, esto puede dar lugar a una acción coercitiva basada en la Sección 5 de la Ley FTC (o estatuto similar)[128].

---

120 Véase el anexo I, sección III.11.g, en particular los incisos ii) y iii).

121 Véase el anexo III, sección sobre "Búsqueda y tratamiento de solicitudes falsas de participación".

122 Anexo I, sección II.7.b.

123 Anexo I, sección III.5.

124 Anexo I, sección III.5.c.(ii).

125 Anexo III (véase la sección "Facilitar la cooperación con las APD") y Anexo IV (véanse las secciones "Priorización de remisiones e investigación" y "Cooperación con las APD de la UE en materia de aplicación de la legislación").

126 Las normas de procedimiento del panel informal de APD deben ser establecidas por las APD basándose en su competencia para organizar su trabajo y cooperar entre sí.

127 Anexo I, sección III.5.c.(i).

128 Anexo I, sección III.5.c.(ii).

En la segunda alternativa, el panel informará al DoC, que considerará la negativa de la organización a cumplir con el consejo del panel DPA como un incumplimiento persistente que conducirá a la eliminación de la organización de la Lista DPF.

(76) Si la APD a la que se ha dirigido la denuncia no ha tomado ninguna medida o ha tomado medidas insuficientes para atender una denuncia, el denunciante individual tiene la posibilidad de impugnar dicha (in)actuación ante los tribunales nacionales del respectivo Estado miembro de la UE.

(77) Los particulares también pueden presentar reclamaciones a las APD incluso cuando el panel de la APD no haya sido designado como órgano de resolución de litigios de una organización. En estos casos, la APD podrá remitir dichas denuncias a la DdC o a la FTC. Con el fin de facilitar y aumentar la cooperación en asuntos relacionados con las denuncias individuales y el incumplimiento por parte de las organizaciones DPF UE- EE.UU., el DoC establecerá un punto de contacto específico para actuar como enlace y ayudar con las consultas de las DPA en relación con el cumplimiento de los Principios por parte de una organización[129]. Del mismo modo, la FTC se ha comprometido a establecer un punto de contacto específico[130].

(78) En cuarto lugar, la DdC se ha comprometido a recibir, revisar y hacer todo lo posible para resolver las quejas sobre el incumplimiento de los Principios por parte de una organización[131]. A tal fin, la DdC establece procedimientos especiales para que las APD remitan las denuncias a un punto de contacto específico, hagan un seguimiento de las mismas y se pongan en contacto con las organizaciones para facilitar su resolución[132]. Con el fin de agilizar la tramitación de las denuncias individuales, el punto de contacto se pone en contacto directamente con la APD respectiva sobre cuestiones de cumplimiento y, en particular, la pone al día sobre el estado de las denuncias en un plazo no superior a 90 días desde su remisión[133]. Esto permite a los interesados presentar denuncias de incumplimiento por parte de las organizaciones de DPF UE-EE. UU. directamente a su DPA nacional y canalizarlas al DoC como autoridad estadounidense que administra el DPF UE-EE.UU..

(79) Cuando, sobre la base de sus verificaciones de oficio, reclamaciones o cualquier otra información, el DoC concluya que una organización ha incumplido de forma persistente los Principios, podrá eliminarla de la lista de DPF[134]. Negativa a acatar una resolución firme de cualquier organismo de autorregulación de la privacidad o de resolución de litigios independiente, resolución u organismo gubernamental, incluida una APD, se considerará un incumplimiento persistente[135].

---

129 Véase el anexo III, sección "Facilitar la cooperación con las APD".

130 Véase el anexo IV, secciones "Prioridad de remisión e investigación" y "Cooperación en materia de aplicación con las APD de la UE".

131 Anexo III, véase, por ejemplo, la sección "Facilitar la cooperación con las APD".

132 Anexo I, sección II.7.e y anexo III, sección "Facilitar la cooperación con las APD".

133 *Ibid*.

134 Anexo I, sección III.11.g.

135 Anexo I, sección III.11.g.

(80) En quinto lugar, una organización de DPF UE-EE.UU. debe estar sujeta a la jurisdicción de las autoridades estadounidenses, en particular la FTC[136], que tienen los poderes de investigación y ejecución necesarios para garantizar eficazmente el cumplimiento de los Principios. La FTC considera prioritarias las denuncias de incumplimiento de los Principios recibidas de organismos independientes de resolución de conflictos o de autorregulación, del DoC y de las APD (actuando por iniciativa propia o a raíz de denuncias) para determinar si se ha infringido el artículo 5 de la Ley FTC[137]. La FTC se ha comprometido a crear un proceso de remisión normalizado, a designar un punto de contacto en la agencia para las remisiones de las APD y a intercambiar información sobre las remisiones. Además, puede aceptar denuncias directamente de particulares y emprender investigaciones de la APD UE- EE.UU. por iniciativa propia, en particular como parte de su investigación más amplia de cuestiones de privacidad.

(81) En sexto lugar, como mecanismo de recurso de "última instancia" en caso de que ninguna de las demás vías de recurso disponibles haya resuelto satisfactoriamente la reclamación de un particular, el interesado de la Unión podrá invocar el arbitraje vinculante del "Panel del Marco de Privacidad de Datos UE-EE. UU." (Panel DPF UE- EE.UU.)[138]. Las organizaciones deben informar a los particulares de su posibilidad de recurrir al arbitraje vinculante y están obligadas a responder una vez que un particular haya recurrido a esta opción mediante notificación a la organización afectada[139].

(82) Este Panel de DPF UE-EE.UU. está formado por un grupo de al menos diez árbitros que serán designados por el DoC y la Comisión en función de su independencia, integridad y experiencia en la legislación estadounidense sobre privacidad y protección de datos de la Unión. Para cada litigio individual, las partes seleccionan de este grupo un panel de uno o tres árbitros[140].

(83) El Centro Internacional para la Resolución de Disputas (ICDR), la división internacional de la Asociación Americana de Arbitraje (AAA), fue seleccionado por el DoC para administrar los arbitrajes. Los procedimientos ante el Panel UE-EE. UU. de DPF se regirán por un conjunto de normas de arbitraje acordadas y un código de conducta para los árbitros designados. El sitio web del ICDR- AAA ofrece información clara y concisa a los particulares sobre el mecanismo de arbitraje y el procedimiento para solicitar un arbitraje.

(84) Las normas de arbitraje acordadas entre el DoC y la Comisión complementan el DPF UE-EE.UU., que contiene varias características que mejoran la accesibilidad de este mecanismo para los interesados de la Unión. que contiene varias características que mejoran la accesibilidad de este mecanismo para los interesados de la Unión: (i) en la preparación de una demanda ante el panel, el interesado podrá contar con la asistencia de su APD nacional; (ii) aunque el

136 Una organización de DPF de la UE y EE.UU. tiene que declarar públicamente su compromiso de cumplir los Principios, divulgar públicamente sus políticas de privacidad en consonancia con estos Principios y aplicarlos plenamente. El incumplimiento es exigible en virtud del artículo 5 de la Ley FTC, que prohíbe los actos desleales y engañosos en el comercio o que afecten a éste.

137 Véanse también los compromisos similares asumidos por el DoT, Anexo V.

138 Véase el Anexo I, "Modelo arbitral".

139 Véase el anexo I, sección II.1.a.(xi) y II.7.c.

140 El número de árbitros del panel deberá ser acordado entre las partes.

arbitraje tendrá lugar en los Estados Unidos, los interesados de la Unión podrán optar por participar a través de videoconferencia o conferencia telefónica, que se facilitará sin coste alguno para el interesado; (iii) aunque la lengua utilizada en el arbitraje será, por regla general, el inglés, en principio se facilitará interpretación en la audiencia arbitral y traducción previa solicitud motivada y sin coste alguno para el interesado; (iv) por último, aunque cada una de las partes deberá correr con sus propios gastos, (v) el arbitraje tendrá lugar en los Estados Unidos. Los honorarios de los abogados, si están representados por un abogado ante el panel, el DoC mantendrá un fondo alimentado con contribuciones anuales de las organizaciones de DPF UE-EE.UU., que deberán cubrir los costes del procedimiento de arbitraje hasta los importes máximos que determinen las autoridades de EE.UU. en consulta con la Comisión[141].

(85) El Panel DPF UE-EE.UU. tiene autoridad para imponer medidas equitativas no monetarias específicas para cada persona[142] necesarias para remediar el incumplimiento de los Principios. Si bien el panel tiene en cuenta otras soluciones ya obtenidas por otros mecanismos de DPF UE-EE.UU. a la hora de tomar su decisión, los particulares pueden seguir recurriendo al arbitraje si consideran que estas otras soluciones son insuficientes. Esto permite a los interesados de la Unión invocar el arbitraje en todos los casos en que la acción o inacción de las organizaciones de DPF UE-EE.UU., los mecanismos de recurso independientes o las autoridades estadounidenses competentes (por ejemplo, la FTC) no hayan resuelto satisfactoriamente sus reclamaciones. El arbitraje no podrá invocarse si una APD tiene autoridad legal para resolver la reclamación en cuestión con respecto a la organización de DPF de la UE-EE.UU., a saber, en aquellos casos en que la organización esté obligada a cooperar y cumplir el asesoramiento de las APD en lo que respecta al tratamiento de datos de recursos humanos recogidos en el contexto laboral, o se haya comprometido voluntariamente a hacerlo. Los particulares pueden ejecutar el laudo arbitral en los tribunales estadounidenses en virtud de la Ley Federal de Arbitraje, garantizando así un recurso legal en caso de incumplimiento por parte de una organización.

(86) En séptimo lugar, cuando una organización no cumple su compromiso de respetar los Principios y la política de privacidad publicada, la legislación estadounidense ofrece otras vías de recurso judicial, incluida la obtención de una indemnización por daños y perjuicios. Por ejemplo, los particulares pueden, en determinadas condiciones, obtener reparación judicial (incluida la indemnización por daños y perjuicios) en virtud de la legislación estatal sobre consumidores en casos de tergiversación fraudulenta, actos o prácticas desleales o engañosos[143], y en virtud del derecho de responsabilidad extracontractual (en

141 Anexo I del anexo I, sección G.6.

142 Los particulares no pueden reclamar daños y perjuicios en el arbitraje, pero invocar el arbitraje no excluye la opción de reclamar daños y perjuicios ante los tribunales ordinarios estadounidenses.

143 Véanse, por ejemplo, las leyes estatales de protección de los consumidores de California (Cal. Civ. Code §§ 1750 - 1785 (West) Consumers Legal Remedies Act); Distrito de Columbia (D.C. Code §§ 28- 3901); Florida (Fla. Stat. §§ 501.201 - 501.213, Deceptive and Unfair Trade Practices Act); Illinois (815 Ill. Comp. Stat. 505/1 - 505/12, Consumer Fraud and Deceptive Business Practices Act); Pensilvania (73 Pa. Stat. Ann. §§ 201-1 - 201-9.3 (West) Ley de prácticas comerciales desleales y protección de los consumidores).

particular, en virtud de los delitos de intrusión en la intimidad[144], apropiación de nombre o imagen[145] y divulgación pública de hechos privados[146]).

(87) En conjunto, las diversas vías de recurso descritas anteriormente garantizan que cada reclamación relativa al incumplimiento del DPF UE-EE.UU. por parte de las organizaciones certificadas será resuelta y subsanada eficazmente.

3. ACCESO Y UTILIZACIÓN DE DATOS PERSONALES TRANSFERIDOS DESDE LA UNIÓN EUROPEA POR LAS AUTORIDADES PÚBLICAS DE LOS ESTADOS UNIDOS

(88) La Comisión también evaluó las limitaciones y salvaguardias, incluidos los mecanismos de supervisión y de recurso individual disponibles en la legislación de los Estados Unidos en lo que respecta a la recogida y posterior utilización por las autoridades públicas de los Estados Unidos de los datos personales transferidos a los responsables y encargados del tratamiento en los Estados Unidos en aras del interés público, en particular con fines policiales penales y de seguridad nacional (acceso gubernamental)[147]. Al evaluar si las condiciones en las que el gobierno accede a los datos transferidos a los Estados Unidos en virtud de la presente Decisión cumplen la prueba de "equivalencia esencial" de conformidad con el artículo 45, apartado 1, del Reglamento (UE) 2016/679, según la interpretación del Tribunal de Justicia a la luz de la Carta de los Derechos Fundamentales, la Comisión tuvo en cuenta varios criterios.

(89) En particular, toda limitación al derecho a la protección de datos personales debe estar prevista por la ley y la base jurídica que permite la injerencia en tal derecho debe definir por sí misma el alcance de la limitación al ejercicio del derecho de que se trate[148]. Además, para cumplir el requisito de proporcio-

144 Es decir, en caso de injerencia intencionada en los asuntos o intereses privados de un individuo, de una manera que resultaría altamente ofensiva para una persona razonable (Restatement (2nd) of Torts, §652(b)).

145 Este agravio se aplica comúnmente en caso de apropiación y uso del nombre o imagen de una persona para publicitar una empresa o producto, o para algún fin comercial similar (véase Restatement (2nd) of Torts, §652C).

146 Es decir, cuando se hace pública información relativa a la vida privada de una persona, cuando esto es altamente ofensivo para una persona razonable y la información no es de interés legítimo para el público (Restatement (2nd) of Torts, §652D).

147 Esto también es pertinente a la luz de la Sección I.5 del Anexo I. De conformidad con esta sección y de forma similar al RGPD, el cumplimiento de los requisitos y derechos de protección de datos que forman parte de los Principios de Privacidad puede estar sujeto a limitaciones. Sin embargo, dichas limitaciones no son absolutas, sino que sólo pueden invocarse en varias condiciones, por ejemplo, en la medida en que sea necesario para cumplir una orden judicial o satisfacer requisitos de interés público, aplicación de la ley o seguridad nacional. En este contexto y en aras de la claridad, esta sección también hace referencia a las condiciones establecidas en la OE 14086 que se evalúan, entre otros, en los considerandos 127 a 141.

148 Véase *Schrems II*, apartados 174-175 y la jurisprudencia citada. Véanse también, por lo que respecta al acceso de las autoridades públicas de los Estados miembros, el asunto

nalidad, según el cual las excepciones y limitaciones a la protección de datos personales sólo deben aplicarse en la medida estrictamente necesaria en una sociedad democrática para alcanzar objetivos específicos de interés general equivalentes a los reconocidos por la Unión, dicha base jurídica debe establecer normas claras y precisas que regulen el alcance y la aplicación de las medidas en cuestión e imponer garantías mínimas para que las personas cuyos datos hayan sido transferidos dispongan de garantías suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso[149]. Además, estas normas y garantías deben ser jurídicamente vinculantes y exigibles por los particulares[150]. En particular, los interesados deben tener la posibilidad de emprender acciones legales ante un tribunal independiente e imparcial para acceder a sus datos personales u obtener la rectificación o supresión de los mismos[151].

3.1. Acceso y uso por parte de las autoridades públicas estadounidenses con fines de aplicación de la ley penal

(90) Por lo que se refiere a la interferencia con los datos personales transferidos en virtud del DPF UE-EE.UU. con fines de aplicación de la ley penal, la legislación de los Estados Unidos impone una serie de limitaciones al acceso y la utilización de los datos personales, y establece mecanismos de supervisión y recurso que se ajustan a los requisitos mencionados en el considerando 89 de la presente Decisión. Las condiciones en las que puede tener lugar dicho acceso y las salvaguardias aplicables al uso de dichos poderes se evalúan detalladamente en las secciones siguientes. A este respecto, el Gobierno de EE.UU. (a través del Departamento de Justicia, DoJ) también ha ofrecido garantías sobre las limitaciones y salvaguardias aplicables (Anexo VI de la presente Decisión).

3.1.1. Bases jurídicas, limitaciones y garantías

3.1.1.1. Limitaciones y salvaguardias en la recogida de datos personales con fines de represión penal

(91) Los fiscales federales y los agentes federales de investigación de los EE.UU. podrán acceder a los datos personales tratados por organizaciones certificadas de los EE.UU. que se transferirían desde la Unión sobre la base del DPF UE-EE.UU. con fines de aplicación de la ley penal con arreglo a distintos procedimientos, como se explica con más detalle en los considerandos 92-99. Estos procedimientos se aplican de la misma manera cuando se obtiene información de

C-623/17, *Privacy International* ECLI:EU:C:2020:790, apartado 65; y los asuntos acumulados C-511/18, C-512/18 y C-520/18, La *Quadrature du Net y otros* ECLI:EU:C:2020:791, apartado 175.

149 Véase *Schrems II*, apartados 176 y 181, así como la jurisprudencia citada. Véase también, por lo que se refiere al acceso de las autoridades públicas de los Estados miembros, *Privacy International,* apartado 68; y La *Quadrature du Net y otros*, apartado 132.

150 Véase *Schrems II*, apartados 181-182.

151 Véase *Schrems I*, apartado 95 y *Schrems II*, apartado 194. A este respecto, el TJUE ha subrayado especialmente que el respeto del artículo 47 de la Carta de los Derechos Fundamentales, que garantiza el derecho a la tutela judicial efectiva ante un tribunal independiente e imparcial, "contribuye al nivel de protección exigido en la Unión Europea [y] debe ser determinado por la Comisión antes de que adopte una decisión de adecuación con arreglo al artículo 45, apartado 1, del Reglamento (UE) 2016/679" (*Schrems II*, apartado 186).

cualquier organización de los EE.UU., independientemente de la nacionalidad o el lugar de residencia de los interesados. Estos procedimientos se aplican del mismo modo cuando la información se obtiene de cualquier organización estadounidense, independientemente de la nacionalidad o del lugar de residencia de los interesados[152].

(92) En primer lugar, a petición de un agente de las fuerzas y cuerpos de seguridad federales o de un abogado de la Administración, un juez puede dictar una orden de registro o incautación (incluida la de información almacenada electrónicamente)[153]. Dicha orden sólo puede emitirse si existe una "causa probable"[154] de que es probable que se encuentren "objetos incautables" (pruebas de un delito, objetos poseídos ilegalmente o bienes diseñados o destinados a ser utilizados o utilizados en la comisión de un delito) en el lugar especificado por la orden. La orden debe identificar los bienes o artículos que se van a incautar y designar al juez al que debe devolverse la orden. Una persona sujeta a un registro o cuyos bienes estén sujetos a un registro puede solicitar la supresión de las pruebas obtenidas o derivadas de un registro ilegal si dichas pruebas se presentan contra esa persona durante un juicio penal[155]. Cuando un titular de datos (por ejemplo, una empresa) está obligado a revelar datos en virtud de una orden judicial, puede impugnar en particular el requisito de revelación por considerarlo indebidamente gravoso[156].

(93) En segundo lugar, una citación puede ser emitida por un gran jurado (un órgano de investigación del tribunal constituido por un juez o magistrado) en el contexto

152 Véase el anexo VI. Véase, por ejemplo, con respecto a la Ley de escuchas telefónicas, la Ley de comunicaciones almacenadas y la Ley Pen Register (mencionadas con más detalle en los considerandos 95 a 98), *Suzlon Energy Ltd v. Microsoft Corp., 671 F.3d 726, 729* (9th Cir. 2011).

153 Reglas Federales de Procedimiento Penal, 41. En una sentencia de 2018, el Tribunal Supremo confirmó que también se requiere una orden de registro o una excepción de orden judicial para que las autoridades policiales accedan a los registros históricos de localización de sitios celulares, que proporcionan una visión general 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*, No. 16-402, 585 U.S. (2018)). Como resultado, tales datos generalmente no pueden obtenerse de una compañía celular sobre la base de una orden judicial sobre la base de motivos razonables para creer que la información es relevante y material para una investigación criminal en curso, sino que requiere demostrar la existencia de una causa probable cuando se utiliza una orden judicial.

154 Según el Tribunal Supremo, la "causa probable" es una norma "práctica y no técnica" que recurre a las "consideraciones fácticas y prácticas de la vida cotidiana sobre las que actúan los hombres razonables y prudentes [...]" (*Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Por lo que respecta a las órdenes de registro, existe causa probable cuando hay una probabilidad razonable de que un registro dé lugar al descubrimiento de pruebas de un delito (id).

155 *Mapp v. Ohio*, 367 U.S. 643 (1961).

156 Véase *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir. 1979) (que sostiene que "el debido proceso exige una audiencia sobre la cuestión de la onerosidad antes de obligar a una compañía telefónica a proporcionar" asistencia con una orden de registro) e *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

de las investigaciones de ciertos delitos graves[157], normalmente a petición de un fiscal federal, para exigir a alguien que presente o ponga a disposición registros comerciales, información almacenada electrónicamente u otros elementos tangibles. Además, diferentes leyes autorizan el uso de citaciones administrativas para presentar o poner a disposición registros comerciales, información almacenada electrónicamente u otros elementos tangibles en investigaciones sobre fraude en la atención sanitaria, abuso de menores, protección del Servicio Secreto, casos de sustancias controladas e investigaciones del Inspector General[158]. En ambos casos, la información debe ser pertinente para la investigación y la citación no puede ser irrazonable, es decir, excesiva, opresiva o gravosa (y puede ser impugnada por el destinatario de la citación por esos motivos)[159].

(94) Condiciones muy similares se aplican a las citaciones administrativas emitidas para solicitar el acceso a datos en poder de empresas en EE.UU. con fines civiles o reglamentarios ("interés público"). La autoridad de las agencias con responsabilidades civiles y reguladoras para emitir tales citaciones administrativas debe establecerse por ley. El uso de una citación administrativa está sujeto a una "prueba de razonabilidad", que requiere que la investigación se lleve a cabo con un fin legítimo, que la información solicitada en la citación sea relevante para ese fin, que la agencia no disponga ya de la información que busca con la citación y que se hayan seguido los pasos administrativos necesarios para emitir la citación[160]. La jurisprudencia del Tribunal Supremo también ha aclarado la necesidad de equilibrar la importancia del interés público en la información que se solicita con la importancia de los intereses de privacidad personales y organizativos[161]. Aunque el uso de una citación administrativa no está sujeto a aprobación judicial previa, se somete a revisión judicial en caso de que el destinatario la impugne por los motivos antes mencionados, o si el organismo emisor intenta hacer cumplir la citación ante los tribunales[162]. Además de estas limitaciones generales, los estatutos individuales pueden establecer requisitos específicos (más estrictos)[163].

---

157 La Quinta Enmienda de la Constitución de EE.UU. exige la acusación del gran jurado por cualquier "delito capital o infamante". El gran jurado está compuesto por entre 16 y 23 miembros y determina si existe causa probable para creer que se ha cometido un delito. Para llegar a esta conclusión, los grandes jurados están investidos de poderes de investigación que les permiten emitir citaciones.

158 Véase el anexo VI.

159 Reglas Federales de Procedimiento Penal, 17.

160 *Estados Unidos contra Powell*, 379 U.S. 48 (1964)

161 *Oklahoma Press Publishing Co. contra Walling*, 327 U.S. 186 (1946).

162 El Tribunal Supremo ha aclarado que, en caso de impugnación de una citación administrativa, un tribunal debe considerar si (1) la investigación es para un propósito legalmente autorizado, (2) la autoridad de citación en cuestión está dentro del poder de mando del Congreso, y (3) los "documentos buscados son relevantes para la investigación". El Tribunal también señaló que una solicitud de citación administrativa debe ser "razonable", es decir, debe requerir "una especificación de los documentos que deben presentarse adecuada, pero no excesiva, para los fines de la investigación pertinente", incluida la "particularidad en la 'descripción del lugar que debe registrarse y de las personas o cosas que deben incautarse'".

163 Por ejemplo, la Ley sobre el Derecho a la Intimidad Financiera faculta a una autoridad gubernamental para obtener registros financieros en poder de una institución financiera

(95) En tercer lugar, varias bases jurídicas permiten a las autoridades encargadas de la aplicación de la ley penal obtener acceso a los datos de las comunicaciones. Un tribunal puede dictar una orden que autorice la recogida de información en tiempo real, sin contenido, de marcación, encaminamiento, direccionamiento y señalización sobre un número de teléfono o correo electrónico (mediante el uso de un registro de pluma o un dispositivo de trampa y rastreo), si considera que la autoridad ha certificado que la información que probablemente se obtenga es relevante para una investigación penal pendiente[164]. La orden debe, entre otras cosas, especificar la identidad, si se conoce, del sospechoso; los atributos de las comunicaciones a las que se aplica y una declaración del delito al que se refiere la información que se va a recopilar. El uso de un registro de pluma o de un dispositivo de trampa y rastreo puede autorizarse por un periodo máximo de sesenta días, que sólo puede prorrogarse mediante una nueva orden judicial.

(96) Además, el acceso con fines de aplicación de la ley penal a la información de los abonados, los datos de tráfico y el contenido almacenado de las comunicaciones en poder de los proveedores de servicios de Internet, las compañías telefónicas y otros terceros proveedores de servicios puede obtenerse sobre la base de la Ley de Comunicaciones Almacenadas[165]. Para obtener el contenido almacenado de las comunicaciones electrónicas, las autoridades encargadas de la aplicación de la ley penal deben, en principio, obtener una orden judicial de un juez basada en una causa probable para creer que la cuenta en cuestión contiene pruebas de un delito[166]. Para obtener la información de registro del abonado, las direcciones IP y las marcas de tiempo asociadas, así como la información de facturación, las autoridades penales pueden utilizar una cita-

---

en virtud de una citación administrativa sólo si (1) hay motivos para creer que los registros solicitados son pertinentes para una investigación legítima de aplicación de la ley y (2) se ha facilitado al cliente una copia de la citación o requerimiento junto con una notificación en la que se indique con razonable especificidad la naturaleza de la investigación (12 U.S.C. §3405). Otro ejemplo es la Ley de Informes de Crédito Justos, que prohíbe a las agencias de informes de los consumidores revelar informes de los consumidores en respuesta a solicitudes de citación administrativa (y sólo les permite responder a solicitudes de citación del gran jurado u órdenes judiciales, 15 U.S.C. §1681 y siguientes). Por lo que se refiere al acceso a la información sobre comunicaciones, se aplican los requisitos específicos de la Ley de Comunicaciones Almacenadas, incluido lo relativo a la posibilidad de utilizar citaciones administrativas (véanse los considerandos 96- 97 para una visión detallada).

164 18 U.S.C. §3123.

165 18 U.S.C. §§ 2701-2713.

166 18 U.S.C. §§ 2701(a)-(b)(1)(A). Si se notifica al abonado o cliente afectado (por adelantado o, en determinadas circunstancias, mediante una notificación diferida), la información de contenido almacenada durante más de 180 días también puede obtenerse sobre la base de una citación administrativa o una citación del gran jurado (18 U.S.C. §§ 2701(b)(1)(B)) o una orden judicial (si hay motivos razonables para creer que la información es pertinente y material para una investigación penal en curso (18 U.S.C. §§ 2701(d)). Sin embargo, de acuerdo con una sentencia de un tribunal federal de apelación, los investigadores del gobierno generalmente obtienen órdenes de registro de los jueces para recoger el contenido de las comunicaciones privadas o los datos almacenados de un proveedor de servicios de comunicaciones comerciales. Estados Unidos contra Warshak, 631 F.3d 266 (6th Cir. 2010).

ción judicial. Para la mayoría del resto de la información almacenada y no contenida, como las cabeceras de los correos electrónicos sin la línea del asunto, una autoridad penal debe obtener una orden judicial, que se emitirá si el juez está convencido de que existen motivos razonables para creer que la información solicitada es relevante y material para una investigación penal en curso.

(97) Los proveedores que reciben solicitudes en virtud de la Ley de Comunicaciones Almacenadas pueden notificar voluntariamente a un cliente o abonado cuya información se busca, excepto cuando la autoridad de aplicación de la ley penal pertinente obtiene una orden de protección que prohíbe dicha notificación[167]. Dicha orden de protección es una orden judicial que exige a un proveedor de servicios de comunicaciones electrónicas o servicios informáticos a distancia al que se dirige una orden, citación u orden judicial, que no notifique a ninguna otra persona la existencia de la orden, citación u orden judicial, durante el tiempo que el tribunal considere oportuno. Las órdenes de protección se conceden si un tribunal considera que hay razones para creer que la notificación pondría en grave peligro una investigación o retrasaría indebidamente un juicio, por ejemplo, porque pondría en peligro la vida o la seguridad física de una persona, la huida de la acusación, la intimidación de posibles testigos, etc. Un memorando del Fiscal General Adjunto (que es vinculante para todos los abogados y agentes del DoJ) exige a los fiscales que determinen detalladamente la necesidad de una orden de protección y que justifiquen ante el tribunal cómo se cumplen los criterios legales para obtener una orden de protección en el caso concreto[168]. El memorando también exige que las solicitudes de órdenes cautelares en general no traten de retrasar la notificación más de un año. Cuando, en circunstancias excepcionales, puedan ser necesarias órdenes de mayor duración, dichas órdenes sólo podrán solicitarse con el acuerdo escrito de un supervisor designado por el Fiscal General o el Fiscal General Adjunto correspondiente. Además, un fiscal debe, al cerrar una investigación, evaluar inmediatamente si existe una base para mantener cualquier orden de protección pendiente y, cuando no sea el caso, poner fin a la orden de protección y asegurarse de que el proveedor de servicios sea notificado de ello[169].

(98) Las autoridades encargadas de la aplicación de la ley penal también pueden interceptar en tiempo real comunicaciones alámbricas, orales o electrónicas sobre la base de una orden judicial en la que un juez determine, entre otras cosas, que existe causa probable para creer que la intervención telefónica o electrónica aportará pruebas de un delito federal, o del paradero de un fugitivo que huye de la justicia[170].

(99) Diversas políticas y directrices del Departamento de Justicia, incluidas las Directrices del Fiscal General para las Operaciones Domésticas del FBI (AGG-DOM), que, entre otras cosas, exigen que la Oficina Federal de Investigación (FBI) utilice

---

167 18 U.S.C. § 2705(b).

168 Véase el Memorando publicado por el Fiscal General Adjunto Rod Rosenstein el 19 de octubre de 2017 sobre una política más restrictiva en materia de solicitudes de órdenes de protección (o de no divulgación), disponible en https://www.justice.gov/criminal-ccips/page/file/1005791/download.

169 Memorando emitido por la Fiscal General Adjunta Lisa Moncao el 27 de mayo de 2022 sobre una política suplementaria relativa a las solicitudes de órdenes de protección de conformidad con 18 U.S.C. §2705(b).

170 18 U.S.C. §§ 2510-2522.

los métodos de investigación menos intrusivos posibles, teniendo en cuenta el efecto sobre la intimidad y las libertades civiles[171], ofrecen más protección.

(100) Según las declaraciones del Gobierno de EE.UU., las mismas o mayores protecciones descritas anteriormente se aplican a las investigaciones policiales a nivel estatal (con respecto a las investigaciones llevadas a cabo en virtud de las leyes estatales)[172]. En particular, las disposiciones constitucionales, así como los estatutos y la jurisprudencia a nivel estatal reafirman las protecciones antes mencionadas contra registros e incautaciones irrazonables al exigir la emisión de una orden de registro[173]. De forma similar a las protecciones otorgadas en

171 Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations (septiembre de 2008), disponible en http://www.justice.gov/archive/opa/docs/guidelines.pdf. En el United States Attorneys' Manual, disponible en http://www.justice.gov/usam/united-states-attorneys- manual, se establecen normas y políticas adicionales que prescriben limitaciones a las actividades de investigación de los fiscales federales. Para apartarse de estas Directrices, debe obtenerse la aprobación previa del Director del FBI, del Director Adjunto o del Subdirector Ejecutivo designado por el Director, a menos que dicha aprobación no pueda obtenerse debido a la inmediatez o gravedad de una amenaza para la seguridad de las personas o los bienes o para la seguridad nacional (en cuyo caso el Director u otra persona autorizada debe ser notificado tan pronto como sea posible). Cuando no se sigan las Directrices, el FBI deberá notificarlo al DoJ, que a su vez informará al Fiscal General y al Fiscal General Adjunto.

172 Anexo VI, nota 2. Véase también, por ejemplo, *Arnold v. City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) ("En los ámbitos de los derechos individuales y las libertades civiles, la Constitución de los Estados Unidos, cuando es aplicable a los Estados, establece un nivel por debajo del cual no pueden caer las decisiones de los tribunales estatales"); *Cooper v. California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) ("Nuestra posición, por supuesto, no afecta a la facultad del Estado para imponer normas más estrictas sobre registros e incautaciones que las exigidas por la Constitución federal, si decide hacerlo"); *Petersen v. City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) ("Aunque la Constitución de Arizona puede imponer normas más estrictas sobre registros e incautaciones que la Constitución federal, los tribunales de Arizona no pueden proporcionar menos protección que la que ofrece la Cuarta Enmienda").

173 La mayoría de los estados han reproducido las protecciones de la Cuarta Enmienda en sus constituciones. Véase Alabama Const. art. I, § 5); Alaska Const. art. I, § 14; 1; Arkansas Const. art. II, § 15; California Const. art. I, § 13; Const. de Colorado art. II, § 7; Const. de Connecticut art. I, § 7; Delaware Const. art. I, § 6; Florida. Art. I, § 12; Const. de Georgia art. I, § I, para. XIII; Const. de Hawai, art. I, § 7; Idaho Const. art. I, § 17; Constitución de Illinois, art. I, § 6; Const. de Indiana art. I, § 11; Iowa Const. art. I, § 8; Kansas Const. Bill of Rights, § 15; Kentucky Const. § 10; Constitución de Luisiana, art. I, § 5; Const. de Maine art. I, § 5; Massachusets Const. Decl. de Derechos art. 14; Const. de Michigan art. I, § 11; Const. de Minnesota art. I, § 10; Const. de Mississippi art. III, § 23; Const. de Missouri art. I, § 15; Const. de Montana art. II, § 11; Nebraska Const. art. I, § 7; Const. de Nevad, art. I, § 18; Const. de New Hampshire pt. 1, art. 19; N.J. Const. art. II, § 7; Const. de Nuevo México art. II, § 10; Const. de Nueva York art. I, § 12; Const. de Dakota del Norte art. I, § 8; Const. de Ohio art. I, § 14; Constitución de Oklahoma, art. II, § 30; Constitución de Oregón, art. I, § 9; Const. de Pensilvania art. I, § 8; Rhode Island Const. art. I, § 6; Const. de Carolina del Sur art. I, § 10; Constitución de Dakota del Sur, art. VI, § 11; Constitución de Tennessee, art. I, § 7; Constitución de Texas, art. I, § 9; Constitución de Utah, art. I, § 14; Const. de Vermont ch. I, art. 11; Constitución de Virginia Occidental, art. III, § 6; Const. de Wisconsin art. I, § 11; Wyoming Const. art. I, § 4. Otros (por ejemplo, Maryland, Carolina del Norte y Virginia) han consagrado en sus constituciones un lenguaje específico relativo a las órdenes

el ámbito federal las órdenes de registro sólo pueden emitirse previa demostración de causa probable y deben describir el lugar que se va a registrar y la persona o cosa que se va a incautar[174].

3.1.1.2. Uso posterior de la información recogida

(101) Por lo que se refiere al uso posterior de los datos recogidos por las autoridades federales encargadas de la aplicación de la ley penal, diferentes estatutos, directrices y normas imponen salvaguardias específicas. A excepción de los instrumentos específicos aplicables a las actividades del FBI (AGG-DOM y FBI Domestic Investigations and Operations Guide), los requisitos descritos en esta sección se aplican en general al uso posterior de los datos por parte de cualquier autoridad federal, incluidos los datos a los que se accede con fines civiles o reglamentarios. Esto incluye los requisitos derivados de los memorandos/reglamentos de la Oficina de Gestión y Presupuesto, la Ley Federal de Modernización de la Gestión de la Seguridad de la Información, la Ley de Administración Electrónica y la Ley Federal de Registros.

(102) De conformidad con la autoridad otorgada por la Ley Clinger-Cohen (P.L. 104-106, División E) y la Ley de Seguridad Informática de 1987 (P.L. 100-235), la Oficina de Gestión y Presupuesto (OMB) publicó la Circular nº A-130 para establecer orientaciones generales vinculantes que se aplican a todos los organismos federales (incluidas las autoridades policiales) cuando manejan información de identificación personal[175]. En particular, la circular exige a todas las agencias federales que "limiten la creación, recogida, uso, procesamiento, almacenamiento, mantenimiento, difusión y divulgación de información de identificación personal a la que esté legalmente autorizada, sea pertinente y se considere razonablemente necesaria para el correcto desempeño de las funciones autorizadas de la agencia"[176]. Además, en la medida en que sea razonablemente factible, los organismos federales deben garantizar que los datos de identifica-

judiciales que ha sido interpretado judicialmente para proporcionar protecciones similares o superiores a la Cuarta Enmienda (véase Maryland. Decl. of Rts. art. 26; Const. de Carolina del Norte art. I, § 20; Virginia Const. art. I, § 10, y la jurisprudencia pertinente, por ejemplo, *Hamel v. State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; State v. Johnson, 861 S.E.2d 474, 483 (N.C. 2021) y *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Por último, Arizona y Washington tienen disposiciones constitucionales que protegen la intimidad de forma más general (Const. de Arizona art. 2, § 8; Const. de Washington art. I, § 7), que han sido interpretadas por los tribunales en el sentido de que proporcionan más protección que la Cuarta Enmienda (véanse, por ejemplo, State v. Bolt, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506.), 511, 688 P.2d 151, 155 (1984), *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

174 Véase, por ejemplo, California Penal Code § 1524.3(b); Rule 3.6-3.13 Alabama Rules of Criminal Procedure; Section 10.79.035; Revised Code of Washington; Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia.

175 Es decir, "información que puede utilizarse para distinguir o rastrear la identidad de un individuo, ya sea por sí sola o combinada con otra información vinculada o vinculable a un individuo concreto", véase la Circular OMB nº A-130, p. 33 (definición de "información de identificación personal").

176 Circular OMB n.º A-130, Managing Information as a Strategic Resource, apéndice II, Responsibilities for Managing Personally Identifiable Information, 81 Fed. Reg. 49.689 (28 de julio de 2016), p. 17.

ción personal no se divulguen a terceros, que la información identificable sea exacta, pertinente, oportuna y completa, y se reduzca al mínimo necesario para el correcto desempeño de las funciones de un organismo. En términos más generales, las agencias federales deben establecer un programa integral de privacidad para garantizar el cumplimiento de los requisitos de privacidad aplicables, desarrollar y evaluar las políticas de privacidad y gestionar los riesgos de privacidad; mantener procedimientos para detectar, documentar y notificar incidentes de cumplimiento de la privacidad; desarrollar programas de sensibilización y formación sobre privacidad para empleados y contratistas; y establecer políticas y procedimientos para garantizar que el personal sea responsable del cumplimiento de los requisitos y políticas de privacidad[177].

(103) Además, la Ley de Administración Electrónica[178] exige a todos los organismos federales (incluidas las autoridades encargadas de la aplicación de la ley penal) que establezcan protecciones de seguridad de la información que sean proporcionales al riesgo y a la magnitud del daño que se derivaría de un acceso, uso, divulgación, perturbación, modificación o destrucción no autorizados; que cuenten con un Director General de Información que garantice el cumplimiento de los requisitos de seguridad de la información y que realicen una evaluación anual independiente (por ejemplo, por parte de un Inspector General, véase el considerando 109) de su programa y prácticas de seguridad de la información[179] . Del mismo modo, la Ley Federal de Registros (FRA)[180] y la normativa complementaria[181] exigen que la información en poder de los organismos federales esté sujeta a salvaguardias que garanticen la integridad física de la información y la protejan contra el acceso no autorizado.

(104) En virtud de la autoridad legal federal, incluida la Ley Federal de Modernización de la Seguridad de la Información de 2014, la OMB y el Instituto Nacional de Normas y Tecnología (NIST) han desarrollado normas que son vinculantes para los organismos federales (incluidas las autoridades encargadas de la aplicación de la ley penal) y que especifican los requisitos mínimos de seguridad de la información que deben establecerse, incluidos los controles de acceso, la sensibilización y la formación, los planes de contingencia, la respuesta a incidentes, las herramientas de auditoría y rendición de cuentas, la garantía de la integridad del sistema y de la información, la realización de evaluaciones de riesgos para la privacidad y la seguridad, etc.[182] . Además, todos los organismos federales (incluidas las autoridades encargadas de la aplicación de la ley penal) deben, de conformidad con las directrices de la OMB, mantener y aplicar un plan para hacer frente a las violaciones de datos, incluso a la hora de responder a dichas violaciones y evaluar los riesgos de daños[183]

177 Apéndice II, §5(a)-(h).

178 44 U.S.C. Capítulo 36.

179 44 U.S.C. §§ 3544-3545.

180 FAC, 44 U.S.C. § 3105

181 36 C.F.R. §§ 1228.150, et seq., 1228.228, y Apéndice A.

182 Véanse, por ejemplo, la Circular OMB nº A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10 de diciembre de 2020); y el NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

183 Memorándum 17-12, "Preparing for and Responding to a Breach of Personally Identifia-

(105) Por lo que respecta a la conservación de datos, la FRA[184] exige a las agencias federales estadounidenses (incluidas las autoridades encargadas de la aplicación de la ley penal) que establezcan periodos de conservación para sus registros (tras los cuales dichos registros deben eliminarse), que deben ser aprobados por la Administración de Archivos y Registros[185]. La duración de estos periodos de conservación se fija en función de distintos factores, como el tipo de investigación, si las pruebas siguen siendo relevantes para la investigación, etc. Con respecto al FBI, la AGG-DOM establece que el FBI debe disponer de un plan de conservación de registros de este tipo y mantener un sistema que permita recuperar rápidamente el estado y la base de las investigaciones.

(106) Por último, la Circular A-130 de la OMB también contiene ciertos requisitos para la difusión de información de identificación personal. En principio, la difusión y divulgación de información de identificación personal debe limitarse a lo que esté legalmente autorizado, sea pertinente y se considere razonablemente necesario para el correcto desempeño de las funciones de un organismo[186]. Al compartir información de identificación personal con otras entidades gubernamentales, las agencias federales estadounidenses deben imponer, cuando proceda, condiciones (incluida la aplicación de controles específicos de seguridad y privacidad) que rijan el tratamiento de la información mediante acuerdos escritos (incluidos contratos, acuerdos de uso de datos, acuerdos de intercambio de información y memorandos de entendimiento)[187]. Por lo que se refiere a los motivos por los que puede difundirse la información, la AGG- DOM y la Guía de investigaciones y operaciones nacionales del FBI[188] establecen, por ejemplo, que el FBI puede estar obligado legalmente a hacerlo (por ejemplo, en virtud de un acuerdo internacional) o está autorizado a difundir información en determinadas circunstancias, por ejemplo, a otras agencias de EE.UU. si la divulgación es compatible con la protección de datos. agencias si la divulgación es compatible con el fin para el que se recopiló la información y está relacionada con sus responsabilidades; a comités del Congreso; a agencias extranjeras si la información está relacionada con sus responsabilidades y la divulgación es compatible con los intereses de Estados Unidos; la divulgación es especialmente necesaria para proteger la seguridad o la protección de personas o bienes, o para proteger o prevenir un delito o una amenaza para la seguridad nacional y la divulgación es compatible con el fin para el que se recopiló la información[189].

---

ble Information", disponible en https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17- 12_0.pdf y Circular OMB n° A-130. Por ejemplo, los procedimientos de respuesta a las violaciones de datos del Departamento de Justicia, véase https://www.justice.gov/file/4336/download.

184 FRA, 44 U.S.C. §§3101 y ss.

185 La Administración Nacional de Archivos y Registros está facultada para evaluar las prácticas de gestión de registros de los organismos y puede determinar si está justificada la conservación continuada de determinados registros (44 U.S.C. §§ 2904(c), 2906).

186 Circular OMB n° A-130, Sección 5.f.1.(d)

187 Circular OMB n° A-130, Apéndice I §3(d).

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

189 AGG-DOM, Sección VI, B y C; FBI Domestic Investigations and Operations Guide (DIOG) Sección 14.

3.1.2. Supervisión

(107) Las actividades de las fuerzas y cuerpos de seguridad federales están sujetas a la supervisión de diversos organismos[190]. Como se explica en los considerandos 92-99, en la mayoría de los casos esto incluye la supervisión previa del poder judicial, que tiene que autorizar las medidas individuales de recogida antes de que puedan utilizarse. Además, otros organismos supervisan distintas fases de las actividades de las autoridades encargadas de la aplicación de la ley penal, incluida la recogida y el tratamiento de datos personales. Juntos, estos organismos judiciales y no judiciales garantizan que las autoridades policiales estén sujetas a una supervisión independiente.

(108) En primer lugar, existen funcionarios encargados de la intimidad y las libertades civiles en diversos departamentos con responsabilidades en materia de aplicación de la ley penal[191]. Si bien las competencias específicas de estos funcionarios pueden variar en cierta medida en función de la ley que los autorice, normalmente abarcan la supervisión de los procedimientos para garantizar que el departamento u organismo respectivo tenga debidamente en cuenta las preocupaciones en materia de privacidad y libertades civiles y haya establecido procedimientos adecuados para atender las quejas de las personas que consideren que se ha violado su privacidad o sus libertades civiles. Los jefes de cada departamento u organismo deben garantizar que los responsables de la privacidad y las libertades civiles dispongan del material y los recursos necesarios para cumplir su mandato, tengan acceso a todo el material y el personal necesarios para desempeñar sus funciones y sean informados y consultados sobre los cambios de política propuestos[192]. Los responsables de la protección de la intimidad y

190 Los mecanismos mencionados en esta sección también se aplican a la recogida y utilización de datos por parte de las autoridades federales con fines civiles y reglamentarios. Las agencias federales civiles y reguladoras están sujetas al escrutinio de sus respectivos Inspectores Generales y a la supervisión del Congreso, incluida la Oficina de Rendición de Cuentas del Gobierno, la agencia de auditoría e investigación del Congreso. A menos que el organismo cuente con un Oficial de Privacidad y Libertades Civiles designado -un cargo que suele encontrarse en organismos como el Departamento de Justicia y el Departamento de Seguridad Nacional (DHS) debido a sus responsabilidades en materia de aplicación de la ley y seguridad nacional-, estas funciones recaen en el Oficial Superior de Privacidad del organismo (SAOP). Todas las agencias federales están legalmente obligadas a designar un SAOP, que tiene la responsabilidad de garantizar el cumplimiento de las leyes de privacidad por parte de la agencia y supervisar los asuntos relacionados. Véase, por ejemplo, OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy (2016).

191 Véase 42 U.S.C. § 2000ee-1. Esto incluye, por ejemplo, el Departamento de Justicia, el Departamento de Seguridad Nacional y el FBI. En el DHS, además, un Director de Privacidad es responsable de preservar y mejorar la protección de la privacidad y promover la transparencia en el Departamento (6U.S.C. 142, Sección 222). Todos los sistemas, tecnologías, formularios y programas del DHS que recojan datos personales o tengan un impacto sobre la privacidad están sujetos a la supervisión del Director de Privacidad, que tiene acceso a todos los registros, informes, auditorías, revisiones, documentos, ponencias, recomendaciones y otros materiales de que disponga el Departamento, y si es necesario mediante citación. El Director de Protección de la Intimidad debe informar anualmente al Congreso sobre las actividades del Departamento que afecten a la intimidad, incluidas las denuncias de violaciones de la intimidad.

192 42 U.S.C. § 2000ee-1(d).

las libertades civiles deben informar periódicamente al Congreso, en particular sobre el número y la naturaleza de las denuncias recibidas por el departamento u organismo y un resumen de la resolución de dichas denuncias, las revisiones e investigaciones realizadas y el impacto de las actividades llevadas a cabo por el responsable[193].

(109) En segundo lugar, un Inspector General independiente supervisa las actividades del Departamento de Justicia, incluido el FBI[194]. Los Inspectores Generales son estatutariamente independientes[195] y responsables de llevar a cabo investigaciones, auditorías e inspecciones independientes de los programas y operaciones del Departamento. Tienen acceso a todos los registros, informes, auditorías, revisiones, documentos, papeles, recomendaciones u otro material pertinente, si es necesario mediante citación, y pueden tomar declaración[196]. Aunque los Inspectores Generales emiten recomendaciones no vinculantes para la adopción de medidas correctoras, sus informes, incluidos los relativos a las medidas de seguimiento (o a la falta de ellas)[197] suelen hacerse públicos y enviarse al Congreso, que puede ejercer sobre esta base su función de supervisión (véase el considerando 111)[198].

(110) En tercer lugar, en la medida en que llevan a cabo actividades antiterroristas, los departamentos con responsabilidades de aplicación de la ley penal están sujetos a la supervisión de la Junta de Supervisión de la Privacidad y las Libertades Civiles (PCLOB), un organismo independiente dentro del poder ejecutivo compuesto por una Junta bipartidista de cinco miembros nombrados por el

193 Véase 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). Por ejemplo, el informe del Director de Privacidad y Libertades Civiles del DOJ y de la Oficina de Privacidad y Libertades Civiles correspondiente al período comprendido entre octubre de 2020 y marzo de 2021 muestra que se llevaron a cabo 389 revisiones de la privacidad, incluidos los sistemas de información y otros programas (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4-21opclsection803reportfy20sa1_final.pdf).

194 Del mismo modo, la Ley de Seguridad Nacional de 2002 creó una Oficina del Inspector General en el Departamento de Seguridad Nacional.

195 Los Inspectores Generales gozan de estabilidad en el cargo y sólo pueden ser destituidos por el Presidente, que debe comunicar por escrito al Congreso los motivos de la destitución.

196 Véase la Ley del Inspector General de 1978, § 6.

197 Véase a este respecto, por ejemplo, el resumen elaborado por la Oficina del Inspector General del Departamento de Justicia sobre las recomendaciones formuladas y el grado de aplicación de las mismas a través de las medidas de seguimiento del departamento y de la agencia, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

198 Véase la Ley del Inspector General de 1978, §§ 4(5), 5. Por ejemplo, la Oficina del Inspector General del Departamento de Justicia publicó recientemente su informe semestral al Congreso (1 de octubre de 2021- 31 de marzo de 2022, https://oig.justice.gov/node/23596), que ofrece una visión general de sus auditorías, evaluaciones, inspecciones, revisiones especiales e investigaciones de los programas y operaciones del DOJ. Estas actividades incluyó una investigación de un antiguo contratista en relación con la revelación ilegal de vigilancia electrónica (la intervención telefónica de una persona) en una investigación en curso, que condujo a la condena del contratista. La Oficina del Inspector General también llevó a cabo una investigación de los programas y prácticas de seguridad de la información de los organismos del DOJ, que incluye la comprobación de la eficacia de las políticas, procedimientos y prácticas de seguridad de la información de un subconjunto representativo de los sistemas de los organismos.

Presidente para un mandato fijo de seis años con la aprobación del Senado[199]. Según su estatuto fundacional, el PCLOB tiene encomendadas responsabilidades en el ámbito de las políticas antiterroristas y su aplicación, con vistas a proteger la intimidad y las libertades civiles. En su examen puede acceder a todos los registros, informes, auditorías, revisiones, documentos, papeles y recomendaciones pertinentes de la agencia, incluida la información clasificada, realizar entrevistas y escuchar testimonios[200]. Recibe informes de los responsables de las libertades civiles y la intimidad de varios departamentos y organismos federales[201], puede formular recomendaciones al Gobierno y a las autoridades encargadas de hacer cumplir la ley, e informa periódicamente a los comités del Congreso y al Presidente[202]. Los informes del Consejo, incluidos los dirigidos al Congreso, deben hacerse públicos en la mayor medida posible[203].

(111) Por último, las actividades de aplicación de la ley penal están sujetas a la supervisión de Comités específicos del Congreso de Estados Unidos (los Comités Judiciales de la Cámara de Representantes y del Senado). Los Comités Judiciales llevan a cabo la supervisión periódica de diferentes maneras, en particular mediante audiencias, investigaciones, revisiones e informes[204].

3.1.3. Reparación

(112) Como se ha indicado, en la mayoría de los casos las autoridades encargadas de la aplicación de la ley penal deben obtener autorización judicial previa para recabar datos personales. Aunque esto no es necesario en el caso de las citaciones administrativas, éstas se limitan a situaciones específicas y estarán sujetas a revisión judicial independiente, al menos cuando el gobierno solicite su ejecución ante los tribunales. En particular, los receptores de citaciones

199 Los miembros del Consejo deben ser seleccionados exclusivamente en función de sus cualificaciones profesionales, logros, prestigio público, conocimientos en materia de libertades civiles y privacidad, y experiencia relevante, y sin tener en cuenta su afiliación política. En ningún caso podrá haber más de tres miembros del Consejo que pertenezcan al mismo partido político. Las personas nombradas para el Consejo no podrán, mientras formen parte del mismo, ser cargos electos, funcionarios o empleados del Gobierno Federal, salvo en calidad de miembros del Consejo. Véase 42 U.S.C. § 2000ee (h).

200 42 U.S.C. § 2000ee (g).

201 Véase 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Entre ellos se incluyen, como mínimo, el Departamento de Justicia, el Departamento de Defensa, el Departamento de Seguridad Nacional y cualquier otro departamento, agencia o elemento del poder ejecutivo que la PCLOB considere apropiado cubrir.

202 42 U.S.C. §2000ee, (e).

203 42 U.S.C. § 2000ee (f).

204 Por ejemplo, las Comisiones organizan audiencias temáticas (véase, por ejemplo, una reciente audiencia de la Comisión Judicial de la Cámara de Representantes de los Estados Unidos sobre "redes digitales", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), así como audiencias periódicas de supervisión, por ejemplo del FBI y el DoJ, véase https://www.judiciary.senate.gov/meetings/08/04/2022/oversight- of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 y https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899.

administrativas pueden impugnarlas ante los tribunales por ser irrazonables, es decir, excesivamente amplias, opresivas o gravosas[205].

(113) Los particulares pueden, en primer lugar, presentar solicitudes o denuncias ante las autoridades policiales penales en relación con el tratamiento de sus datos personales. Esto incluye la posibilidad de solicitar el acceso y la corrección de los datos personales[206] . Por lo que respecta a las actividades relacionadas con la lucha contra el terrorismo, las personas también pueden presentar una reclamación ante los responsables de la protección de la intimidad y las libertades civiles (u otros funcionarios encargados de la protección de la intimidad) de las autoridades policiales[207].

(114) Además, la legislación estadounidense prevé una serie de vías de recurso judicial para los particulares, contra una autoridad pública o uno de sus funcionarios, cuando estas autoridades tratan datos personales[208]. Estas vías, que incluyen en particular la APA, la Freedom of Information Act (FOIA) y la Electronic Communications Privacy Act (ECPA), están abiertas a todos los particulares con independencia de su nacionalidad, con sujeción a las condiciones aplicables.

(115) En general, en virtud de las disposiciones sobre revisión judicial de la APA[209], "cualquier persona que sufra un agravio legal debido a la actuación de un organismo, o que se vea perjudicada o agraviada por la actuación de un organismo", tiene derecho a solicitar una revisión judicial[210]. Esto incluye la posibilidad de solicitar al tribunal que "declare ilegales y anule la actuación, los resultados y las conclusiones de la agencia que se consideren [...] arbitrarios, caprichosos, un abuso de discrecionalidad o no conformes a derecho"[211].

(116) Más concretamente, el Título II de la ECPA[212] establece un sistema de derechos legales de privacidad y, como tal, regula el acceso de las fuerzas de seguridad al contenido de las comunicaciones telefónicas, orales o electrónicas almacenadas por terceros proveedores de servicios[213] . Tipifica como delito el

---

205 Véase el anexo VI.

206 Circular OMB nº A-130, Apéndice II, Sección 3(a) y (f), que exige a las agencias federales que garanticen el acceso y la corrección adecuados a petición de los particulares, y que establezcan procedimientos para recibir y atender las quejas y peticiones relacionadas con la privacidad.

207 Véase 42 U.S.C. § 2000ee-1 por lo que respecta, por ejemplo, al DoJ y al Departamento de Seguridad Nacional. Véase también el Memorándum M-16-24 de la OMB, *Role and Designation of Senior Agency Officials for Privacy*.

208 Los mecanismos de recurso mencionados en esta sección también se aplican a la recogida y utilización de datos por parte de las autoridades federales con fines civiles y reglamentarios.

209 5 U.S.C. § 702.

210 En general, sólo la acción "final" de un organismo -en lugar de la acción "preliminar, procesal o intermedia"- está sujeta a revisión judicial. Véase 5 U.S.C. § 704.

211 5 U.S.C. § 706(2)(A).

212 18 U.S.C. §§ 2701-2712.

213 La ECPA protege las comunicaciones mantenidas por dos clases definidas de proveedores de servicios de red, a saber, los proveedores de: (i) servicios de comunicación electrónica, por ejemplo telefonía o correo electrónico; (ii) servicios informáticos a distancia, como servicios de almacenamiento o procesamiento informático.

acceso ilícito (es decir, no autorizado por un tribunal o permitido de otro modo) a dichas comunicaciones y ofrece a los afectados la posibilidad de interponer una demanda civil ante un tribunal federal de EE.UU. por daños y perjuicios reales y punitivos, así como una reparación equitativa o declaratoria contra un funcionario público que haya cometido intencionadamente tales actos ilícitos, o contra los Estados Unidos.

(117) Además, otras leyes conceden a los particulares el derecho a demandar a una autoridad pública. UU con respecto al tratamiento de sus datos personales, como la Ley de escuchas telefónicas (Wiretap Act)[214], la Ley de fraude y abuso informático (Computer Fraud and Abuse Act)[215], la Ley federal de agravios (Federal Torts Claim Act[216], la Right to Financial Privacy Act[217], y la Fair Credit Reporting Act[218].

(118) Asimismo, en virtud de la FOIA[219], 5 U.S.C. § 552 cualquier persona tiene derecho a obtener acceso a los registros de los organismos federales, incluso cuando éstos contengan datos personales del individuo. Una vez agotados los recursos administrativos, una persona puede invocar ese derecho de acceso ante un tribunal, a menos que esos registros estén protegidos de la divulgación pública por una exen-

---

214 18 U.S.C. §§ 2510 y ss. En virtud de la Ley de escuchas telefónicas (18 U.S.C. § 2520), una persona cuyas comunicaciones telefónicas, orales o electrónicas hayan sido interceptadas, divulgadas o utilizadas intencionadamente puede entablar una acción civil por violación de la Ley de escuchas telefónicas, incluso en determinadas circunstancias contra un funcionario del Gobierno o contra los Estados Unidos. Para la recopilación de información no relacionada con el contenido (por ejemplo, dirección IP, dirección de correo electrónico de entrada y salida), véase también el capítulo del Título 18 sobre registros de pluma y dispositivos de trampa y rastreo (18 U.S.C. §§ 3121-3127 y, para la acción civil, § 2707).

215 18 U.S.C. § 1030. En virtud de la Ley de Fraude y Abuso Informático, una persona puede interponer una demanda contra cualquier persona en relación con el acceso no autorizado intencionado (o que exceda el acceso autorizado) para obtener información de una institución financiera, un sistema informático del gobierno de EE.UU. u otro ordenador especificado, incluso en determinadas circunstancias contra un funcionario del gobierno individual.

216 28 U.S.C. §§ 2671 y ss. En virtud de la Ley Federal de Reclamaciones por Agravios (Federal Tort Claims Act), una persona puede interponer una demanda, en determinadas circunstancias, contra los Estados Unidos en relación con "la acción u omisión negligente o culposa de cualquier empleado del Gobierno mientras actúa en el ámbito de su cargo o empleo".

217 12 U.S.C. §§ 3401 y ss. En virtud de la Ley sobre el derecho a la privacidad financiera, una persona puede interponer una demanda, en determinadas circunstancias, contra los Estados Unidos con respecto a la obtención o divulgación de registros financieros protegidos en violación de la ley. El acceso del gobierno a los registros financieros protegidos está generalmente prohibido a menos que el gobierno haga la solicitud sujeta a una citación legal u orden de registro o, sujeto a limitaciones, una solicitud formal por escrito y el individuo cuya información se busca reciba notificación de dicha solicitud.

218 15 U.S.C. §§ 1681-1681x. En virtud de la Ley de Informes de Crédito Justos, una persona puede interponer una demanda contra cualquier persona que incumpla los requisitos (en particular, la necesidad de autorización legal) relativos a la recopilación, difusión y uso de informes de crédito de los consumidores o, en determinadas circunstancias, contra un organismo gubernamental.

219 5 U.S.C. § 552.

ción o exclusión especial de aplicación de la ley[220]. En este caso, el tribunal evaluará si se aplica alguna exención o si la autoridad pública pertinente la ha invocado legalmente.

3.2. Acceso y utilización por las autoridades públicas estadounidenses con fines de seguridad nacional

(119) La legislación de los Estados Unidos contiene diversas limitaciones y salvaguardias en relación con el acceso y la utilización de datos personales con fines de seguridad nacional, y establece mecanismos de supervisión y recurso que se ajustan a los requisitos mencionados en el considerando 89 de la presente Decisión. Las condiciones en las que puede tener lugar dicho acceso y las salvaguardias aplicables al uso de estos poderes se evalúan detalladamente en las secciones siguientes.

3.2.1. Bases jurídicas, limitaciones y garantías

3.2.1.1. Marco jurídico aplicable

(120) Los datos personales transferidos desde la Unión a las organizaciones DPF UE-EE.UU. pueden ser recogidos por las autoridades estadounidenses con fines de seguridad nacional sobre la base de diferentes instrumentos jurídicos, sujetos a condiciones y salvaguardias específicas.

(121) Una vez recibidos los datos personales por organizaciones situadas en Estados Unidos, Las agencias de inteligencia de EE.UU. pueden solicitar el acceso a dichos datos con fines de seguridad nacional únicamente si así lo autoriza la legislación, concretamente en virtud de la Ley de Vigilancia de la Inteligencia

220 No obstante, estas exclusiones están enmarcadas. Por ejemplo, según 5 U.S.C. § 552 (b)(7), los derechos previstos en la FOIA quedan excluidos en el caso de "registros o información recopilados con fines policiales, pero sólo en la medida en que la producción de dichos registros o información policial (A) pudiera razonablemente interferir en los procedimientos de aplicación de la ley, (B) privara a una persona del derecho a un juicio justo o a un fallo imparcial, (C) pudiera constituir una invasión injustificada de la intimidad personal, (D) pudiera revelar la identidad de una fuente confidencial, incluida una agencia o autoridad estatal, local o extranjera, o cualquier institución privada que haya facilitado información con carácter confidencial, y, en el caso de un registro o información recopilada por las autoridades encargadas de la aplicación de la ley penal en el curso de una investigación penal o por un organismo que lleve a cabo una investigación legal de inteligencia sobre seguridad nacional, la información facilitada por una fuente confidencial, (E) revelaría técnicas y procedimientos para investigaciones o enjuiciamientos policiales, o revelaría directrices para investigaciones o enjuiciamientos policiales, si cabe esperar razonablemente que dicha revelación suponga un riesgo de elusión de la ley, o (F) cabe esperar razonablemente que ponga en peligro la vida o la seguridad física de cualquier persona." Asimismo, "[c]uando se presente una solicitud que implique el acceso a registros [cuya producción pudiera razonablemente esperarse que interfiriera con los procedimientos de aplicación de la ley] y- (A) la investigación o procedimiento implique una posible violación de la ley penal; y (B) hay razones para creer que (i) el sujeto de la investigación o procedimiento no es consciente de su pendencia, y (ii) la divulgación de la existencia de los registros podría razonablemente interferir con los procedimientos de aplicación, la agencia puede, sólo durante el tiempo que dure esa (B) circunstancia, tratar los registros como no sujetos a los requisitos de esta sección." (5 U.S.C. § 552 (c)(1)).

Exterior (FISA) o y las disposiciones legales que autorizan el acceso a través de Cartas de Seguridad Nacional (NSL)[221]. La FISA contiene varias bases jurídicas que pueden utilizarse para recoger (y posteriormente tratar) los datos personales de los interesados de la Unión transferidos en virtud de la DPF UE-EE.UU. (Sección 105 FISA[222], Sección 302 FISA[223], Sección 402 FISA[224], Sección 501 FISA[225] y Sección 702 FISA[226]), como se describe con más detalle en los considerandos 142-152.

(122) Las agencias de inteligencia estadounidenses también tienen posibilidades de recopilar datos personales fuera de Estados Unidos, lo que puede incluir datos personales en tránsito entre la Unión y Estados Unidos. La recogida fuera de Estados Unidos se basa en la Orden Ejecutiva 12333 (EO 12333)[227], dictada por el Presidente[228].

(123) La recopilación de inteligencia de señales es la forma de recopilación de inteligencia más relevante para la presente conclusión de adecuación, ya que se refiere a la recopilación de comunicaciones electrónicas y datos de sistemas de información. Dicha recogida puede ser llevada a cabo por las agencias de inteligencia estadounidenses tanto dentro de Estados Unidos (sobre la base de la FISA) como mientras los datos están en tránsito hacia Estados Unidos (sobre la base de la OE 12333).

(124) El 7 de octubre de 2022, el Presidente de los Estados Unidos emitió la OE 14086 sobre la mejora de las salvaguardias para la inteligencia de señales de los Estados Unidos, que establece limitaciones y salvaguardias para todas las actividades de inteligencia de señales de los Estados Unidos. Esta OE susti-

---

221 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; y 18 U.S.C. § 2709. Véase el considerando 153.

222 50 U.S.C. § 1804, que se refiere a la vigilancia electrónica individualizada tradicional.

223 50 U.S.C. §1822, que se refiere a los registros físicos con fines de inteligencia exterior.

224 50 U.S.C. § 1842 con § 1841(2) y la Sección 3127 del Título 18, que se refiere a la instalación de pen registers o dispositivos de trampa y rastreo.

225 50 U.S.C. § 1861, que permite al FBI presentar "una solicitud de orden por la que se autorice a un transportista común, a un establecimiento de alojamiento público, a un establecimiento de almacenamiento físico o a un establecimiento de alquiler de vehículos a entregar los registros que obren en su poder para una investigación destinada a recabar información de inteligencia extranjera o una investigación relativa al terrorismo internacional".

226 50 U.S. Code § 1881a, que permite a los elementos de la Comunidad de Inteligencia de EE.UU. buscar acceso a información, incluido el contenido de las comunicaciones por Internet, de empresas estadounidenses, dirigida a determinadas personas no estadounidenses fuera de Estados Unidos con la asistencia legalmente obligada de los proveedores de comunicaciones electrónicas.

227 EO 12333: United States Intelligence Activities, Federal Register Vol. 40, No 235 (8 de diciembre de 1981, modificado el 30 de julio de 2008). La OE 12333 define de manera más general los objetivos, orientaciones, deberes y responsabilidades de las actividades de inteligencia de Estados Unidos (incluido el papel de los distintos elementos de la Comunidad de Inteligencia) y establece los parámetros generales para la realización de las actividades de inteligencia.

228 En virtud del Artículo II de la Constitución de Estados Unidos, la responsabilidad de garantizar la seguridad nacional, incluida en particular la recopilación de información de inteligencia extranjera, corresponde al Presidente como Comandante en Jefe de las fuerzas armadas.

tuye a la Directiva Política Presidencial (PPD-28) en gran medida[229], refuerza las condiciones, limitaciones y salvaguardias que se aplican a todas las actividades de inteligencia de señales (es decir, sobre la base de la FISA y de la OE 12333), independientemente de dónde tengan lugar[230], y establece un nuevo mecanismo de recurso a través del cual los particulares pueden invocar y hacer cumplir estas salvaguardias[231] (véanse con más detalle los considerandos 176-194). De este modo, aplica en la legislación estadounidense el resultado de las conversaciones que tuvieron lugar entre la UE y los EE.UU. tras la invalidación de la Decisión de adecuación de la Comisión sobre el Escudo de la privacidad por el Tribunal de Justicia (véase el considerando 6). Se trata, por tanto, de un elemento especialmente importante del marco jurídico evaluado en la presente Decisión.

(125) Las limitaciones y salvaguardias introducidas por la OE 14086 complementan las previstas por la Sección 702 de la FISA y la OE 12333. Los requisitos que se describen a continuación (en las secciones 3.2.1.2 y 3.2.1.3) deben ser aplicados por los organismos de inteligencia al realizar actividades de inteligencia de señales de conformidad con la Sección 702 de la FISA y la OE 12333, por ejemplo, al seleccionar/identificar las categorías de información de inteligencia extranjera que deben adquirirse de conformidad con la Sección 702 de la FISA; al recopilar inteligencia extranjera o contrainteligencia de conformidad con la OE 12333; y al tomar decisiones sobre objetivos individuales de conformidad con la Sección 702 de la FISA y la OE 12333.

(126) Los requisitos establecidos en esta Orden Ejecutiva emitida por el Presidente son vinculantes para toda la Comunidad de Inteligencia. Deben aplicarse además mediante políticas y procedimientos de los organismos que los plasmen en orientaciones concretas para las operaciones cotidianas. A este respecto, la OE 14086 concede a las agencias de inteligencia estadounidenses un plazo máximo de un año para actualizar sus políticas y procedimientos existentes (es decir, antes del 7 de octubre de 2023) a fin de adaptarlos a los requisitos

---

229 La OE 14086 deroga una Directiva Presidencial anterior, la PPD 28, a excepción de su Sección 3 y un Anexo complementario, (que exige a los organismos de inteligencia que revisen anualmente sus prioridades y necesidades de inteligencia de señales, teniendo en cuenta los beneficios de las actividades de inteligencia de señales para los intereses nacionales de EE.UU., así como el riesgo que plantean dichas actividades) y la Sección 6 (que contiene disposiciones generales).(que exige a los organismos de inteligencia que revisen anualmente sus prioridades y necesidades en materia de inteligencia de señales, teniendo en cuenta los beneficios de las actividades de inteligencia de señales para los intereses nacionales de Estados Unidos, así como el riesgo que plantean dichas actividades) y la Sección 6 (que contiene disposiciones generales), véase el Memorando de Seguridad Nacional sobre la revocación parcial de la Directiva Política Presidencial 28, disponible en https://www.whitehouse.gov/briefing-room/statements- releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy- directive-28/

230 Véase la sección 5(f) de la OE 14086, que explica que la OE tiene el mismo ámbito de aplicación que el PPD-28, que, según su nota 3, se aplicaba a las actividades de inteligencia de señales realizadas con el fin de recopilar comunicaciones o información sobre comunicaciones, excepto las actividades de inteligencia de señales realizadas para probar o desarrollar capacidades de inteligencia de señales.

231 Véase a este respecto, por ejemplo, la sección 5(h) de la OE 14086, que aclara que las salvaguardias de la OE crean un derecho legal y pueden ser aplicadas por los particulares a través del mecanismo de recurso.

de la OE. Dichas políticas y procedimientos actualizados deben elaborarse en consulta con el Fiscal General, el Oficial de Protección de las Libertades Civiles del Director de Inteligencia Nacional (ODNI CLPO) y el PCLOB -un órgano de supervisión independiente autorizado para revisar las políticas del Poder Ejecutivo y su aplicación, con vistas a proteger la intimidad y las libertades civiles (véase el considerando 110 en lo que respecta a la función y el estatuto del PCLOB)- y ponerse a disposición del público[232] . Además, una vez que las políticas y procedimientos actualizados estén en vigor, el PCLOB llevará a cabo una revisión para garantizar que son coherentes con la OE. En un plazo de 180 días a partir de la finalización de dicha revisión por parte del PCLOB, cada agencia de inteligencia deberá estudiar detenidamente y aplicar o abordar de otro modo todas las recomendaciones del PCLOB. El 3 de julio de 2023, el gobierno estadounidense publicó dichas políticas y procedimientos actualizados[233].

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

(127) La OE 14086 establece una serie de requisitos de gran alcance que se aplican a todas las actividades de inteligencia de señales (recogida, uso, difusión, etc. de datos personales).

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

(129) En segundo lugar, deben establecerse salvaguardias adecuadas para garantizar que la privacidad y las libertades civiles sean consideraciones integrales en la planificación de tales actividades[235].

(130) En particular, cualquier actividad de inteligencia de señales sólo podrá llevarse a cabo "previa determinación, basada en una evaluación razonable de todos los factores pertinentes, de que las actividades son necesarias para avanzar en una prioridad de inteligencia validada" (por lo que respecta a la noción de "prioridad de inteligencia validada", véase el considerando 135)[236].

(131) Además, dichas actividades sólo pueden llevarse a cabo "en la medida y de la manera que sean proporcionales a la prioridad de inteligencia validada para la que han sido autorizadas"[237]. En otras palabras, debe alcanzarse un equilibrio adecuado "entre la importancia de la prioridad de inteligencia que se persigue

232 Véase la sección 2(c)(iv)(C) de la OE 14086.

233 https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures- aplicación-de-las-nuevas-garantías-en-la-orden-ejecutiva-14086.

234 Sección 2(a)(i) OE 14086.

235 Sección 2(a)(ii) OE 14086.

236 Sección 2(a)(ii)(A) OE 14086. Esto no siempre requiere que la inteligencia de señales sea el único medio para avanzar en aspectos de una prioridad de inteligencia validada. Por ejemplo, la recopilación de inteligencia de señales puede utilizarse para garantizar vías alternativas de validación (por ejemplo, para corroborar la información recibida de otras fuentes de inteligencia) o para mantener un acceso fiable a la misma información (Sección 2(c)(i)(A) de la OE 14086).

237 Sección 2(a)(ii)(B) OE 14086.

y el impacto sobre la intimidad y las libertades civiles de las personas afectadas, con independencia de su nacionalidad o del lugar en que residan"[238].

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

(133) Estos requisitos generales se refuerzan en lo que respecta a la recogida de información de inteligencia mediante una serie de condiciones y limitaciones que garantizan que la injerencia en los derechos de las personas se limite a lo necesario y proporcionado para alcanzar un objetivo legítimo.

(134) En primer lugar, la OE limita de dos maneras los motivos por los que se pueden recoger datos en el marco de las actividades de inteligencia de señales. Por una parte, la OE establece los objetivos legítimos que pueden perseguirse mediante la recogida de información de inteligencia, por ejemplo, comprender o evaluar las capacidades, intenciones o actividades de organizaciones extranjeras, incluidas las organizaciones terroristas internacionales, que supongan una amenaza actual o potencial para la seguridad nacional de Estados Unidos; protegerse contra las capacidades y actividades militares extranjeras; comprender o evaluar las amenazas transnacionales que repercuten en la seguridad mundial, como el cambio climático y otros cambios ecológicos, los riesgos para la salud pública y amenazas humanitarias[240]. Por otra parte, la OE enumera determinados objetivos que nunca deben perseguirse mediante actividades de inteligencia de señales, por ejemplo, con el fin de obstaculizar la crítica, la disidencia o la libre expresión de ideas u opiniones políticas por parte de individuos o de la prensa; con el fin de perjudicar a personas por su origen étnico, raza, género, identidad de género, orientación sexual o religión; o para proporcionar una ventaja competitiva a empresas estadounidenses[241].

(135) Además, las agencias de inteligencia no pueden basarse en los objetivos legítimos establecidos en la OE 14086 por sí solos para justificar la recopilación de inteligencia de señales, sino que deben fundamentarse, a efectos operativos, en prioridades más concretas para las que pueda recopilarse inteligencia de señales. En otras palabras, la recopilación real sólo puede tener lugar para promover una prioridad más específica. Dichas prioridades se establecen mediante un proceso específico destinado a garantizar el cumplimiento de los requisitos legales aplicables, incluidos los relativos a la intimidad y las libertades civiles. Más concretamente, las prioridades de inteligencia son desarrolladas en primer lugar por el Director de Inteligencia Nacional (a través del denominado Marco Nacional de Prioridades de Inteligencia) y sometidas a la aprobación del Presi-

238 Sección 2(a)(ii)(B) OE 14086.

239 Sección 2(a)(iii), junto con la Sección 2(d) OE 14086.

240 Sección 2(b)(i) de la OE 14086. Debido a la lista circunscrita de objetivos legítimos de la OE, que no abarca posibles amenazas futuras, la OE prevé la posibilidad de que el Presidente actualice esta lista si surgen nuevos imperativos de seguridad nacional, como nuevas amenazas a la seguridad nacional. En principio, estas actualizaciones deben hacerse públicas, a menos que el Presidente determine que hacerlo supondría en sí mismo un riesgo para la seguridad nacional de Estados Unidos (Sección 2(b)(i)(B) de la OE 14086).

241 Sección 2(b)(ii) OE 14086.

dente[242]. Antes de proponer prioridades de inteligencia al Presidente, el Director debe, de conformidad con la OE 14086, obtener una evaluación de la CLPO de la ODNI para cada prioridad en cuanto a si (1) avanza uno o más objetivos legítimos enumerados en la OE; (2) no fue diseñado ni se prevé que dé lugar a la recopilación de señales de inteligencia para un objetivo prohibido enumerado en la OE; y (3) se estableció después de la consideración adecuada de la privacidad y las libertades civiles de todas las personas, independientemente de su nacionalidad o de donde puedan residir[243] . En caso de que el Director no esté de acuerdo con la evaluación de la CLPO, ambas opiniones deberán presentarse al Presidente[244].

(136) Por lo tanto, este proceso garantiza especialmente que las consideraciones relativas a la privacidad se tengan en cuenta desde la fase inicial en la que se elaboran las prioridades de inteligencia.

(137) En segundo lugar, una vez que se ha establecido una prioridad de inteligencia, una serie de requisitos rigen la decisión sobre si se puede recopilar inteligencia de señales para promover dicha prioridad y en qué medida. Estos requisitos hacen operativas las normas generales de necesidad y proporcionalidad establecidas en la Sección 2(a) de la OE.

(138) En particular, la inteligencia de señales sólo puede recopilarse "tras la determinación de que, sobre la base de una evaluación razonable de todos los factores pertinentes, la recopilación es necesaria para avanzar en una prioridad de inteligencia específica"[245]. Para determinar si una actividad específica de recopilación de inteligencia de señales es necesaria para avanzar en una prioridad de inteligencia validada, las agencias de inteligencia de EE.UU. deben considerar la disponibilidad, viabilidad e idoneidad de otras fuentes y métodos menos intrusivos, incluidos los procedentes de fuentes diplomáticas y públicas[246]. Cuando estén disponibles, deberá darse prioridad a estas fuentes y métodos alternativos menos intrusivos[247].

(139) Cuando, en aplicación de tales criterios, se considere necesaria la recogida de información de inteligencia de señales, ésta deberá "adaptarse en la medida de lo posible" y "no afectar de manera desproporcionada a la intimidad ni a las libertades civiles"[248]. Para garantizar que la intimidad y las libertades civiles no se vean afectadas de forma desproporcionada - es decir, para lograr un equilibrio adecuado entre las necesidades de seguridad nacional y la protección de la intimidad y las libertades civiles - deben tenerse debidamente en cuenta todos los factores pertinentes, como la naturaleza del objetivo perseguido; el carácter intrusivo de la actividad de recopilación, incluida su duración; la con-

242 Sección 102A de la Ley de Seguridad Nacional y Sección 2(b)(iii) de la OE 14086.

243 En casos excepcionales (en particular, cuando dicho proceso no pueda llevarse a cabo debido a la necesidad de abordar una necesidad de inteligencia nueva o en evolución), dichas prioridades podrán ser establecidas directamente por el Presidente o el jefe de un elemento de la Comunidad de Inteligencia, que en principio deberán aplicar los mismos criterios que los descritos en la sección 2(b)(iii)(A)(1)-(3), véase la sección 4(n) de la OE 14086.

244 Sección 2(b)(iii)(C) OE 14086.

245 Sección 2(b) y (c)(i)(A) OE 14086.

246 Sección 2(c)(i)(A) OE 14086.

247 Sección 2(c)(i)(A) OE 14086.

248 Sección 2(c)(i)(B) OE 14086.

tribución probable de la recopilación al objetivo perseguido; las consecuencias razonablemente previsibles para las personas; y la naturaleza y sensibilidad de los datos que deben recopilarse[249].

(140) Por lo que se refiere al tipo de recogida de información de inteligencia de señales, la recogida de datos dentro de Estados Unidos, que es la más pertinente para la presente conclusión de adecuación, ya que se refiere a datos que han sido transferidos a organizaciones de Estados Unidos, debe ser siempre selectiva, como se explica con más detalle en los considerandos 142-153.

(141) La "recogida masiva"[250] sólo puede llevarse a cabo fuera de Estados Unidos, en virtud de la EO 12333. También en este caso, de conformidad con la OE 14086, la recogida selectiva debe ser prioritaria[251]. Por el contrario, la recogida masiva sólo se permite cuando la información necesaria para avanzar en una prioridad de inteligencia validada no puede obtenerse razonablemente mediante la recogida selectiva[252]. Cuando sea necesario llevar a cabo una recogida masiva de datos fuera de Estados Unidos, se aplicarán las salvaguardias específicas previstas en la OE nº 14086[253]. En primer lugar, deben aplicarse métodos y medidas técnicas para limitar los datos recogidos a lo estrictamente necesario para hacer avanzar una prioridad de inteligencia validada, minimizando al mismo tiempo la recogida de información no pertinente[254]. En segundo lugar, la OE limita el uso de la información La inteligencia de señales obtenida en masa (incluidas las consultas) se destinará a seis objetivos específicos, entre ellos la

249 Sección 2(c)(i)(B) OE 14086.

250 Es decir, la recogida de grandes cantidades de inteligencia de señales que, debido a consideraciones técnicas u operativas, se adquiere sin utilizar discriminantes (por ejemplo, sin utilizar identificadores específicos o términos de selección), véase la Sección 4(b) de la OE 14086. De conformidad con la OE 14086 y como se explica con más detalle en el considerando 141, la recogida masiva con arreglo a la OE 12333 sólo tiene lugar cuando es necesaria para avanzar en prioridades específicas de inteligencia validadas y está sujeta a una serie de limitaciones y salvaguardias destinadas a garantizar que no se accede a los datos de forma indiscriminada. Por lo tanto, la recogida masiva debe contrastarse con la recogida generalizada e indiscriminada ("vigilancia masiva") sin limitaciones ni salvaguardias.

251 Sección 2(c)(ii)(A) OE 14086.

252 Sección 2(c)(ii)(A) OE 14086.

253 Las normas específicas sobre recogida masiva de la OE 14086 también se aplican a una actividad de recogida selectiva de señales de inteligencia que utilice temporalmente datos adquiridos sin discriminantes (por ejemplo, términos de selección o identificadores específicos), es decir, a granel (lo que sólo es posible fuera del territorio de Estados Unidos). Este no es el caso cuando dichos datos sólo se utilizan para apoyar la fase técnica inicial de la actividad de recogida selectiva de señales de inteligencia, se conservan únicamente durante el breve período de tiempo necesario para completar esta fase y se suprimen inmediatamente después (Sección 2(c)(ii)(D) EO 14086). En este caso, el único propósito de la recogida inicial sin discriminantes es permitir una recogida selectiva de información aplicando un identificador o término de selección específico. En tal supuesto, sólo los datos que responden a la aplicación de un determinado discriminante se introducen en las bases de datos gubernamentales, mientras que los datos restantes se destruyen. Por lo tanto, esta recogida selectiva sigue rigiéndose por las normas generales que se aplican a la recogida de información de inteligencia, incluidas las secciones 2(a)-(b) y 2(c)(i) de la OE 14086.

254 Sección 2(c)(ii)(A) OE 14086.

protección contra el terrorismo, la toma de rehenes y la retención de personas cautivas por o en nombre de un gobierno, organización o persona extranjeros; la protección contra el espionaje, el sabotaje o el asesinato extranjeros; la protección contra las amenazas derivadas del desarrollo, la posesión o la proliferación de armas de destrucción masiva o tecnologías y amenazas conexas, etc.[255] Por último, cualquier consulta de inteligencia de señales obtenida de forma masiva sólo podrá tener lugar cuando sea necesario para avanzar en una prioridad de inteligencia validada, en la búsqueda de estos seis objetivos y de acuerdo con políticas y procedimientos que tengan debidamente en cuenta el impacto de las consultas sobre la privacidad y las libertades civiles de todas las personas, independientemente de su nacionalidad o de donde residan[256].

(142) Además de los requisitos de la OE 14086, la recogida de datos de inteligencia de señales que se han transferido a una organización de Estados Unidos está sujeta a limitaciones y salvaguardias específicas reguladas por la Sección 702 de la FISA[257]. La Sección 702 de la FISA permite la recogida de información de inteligencia extranjera a través de la selección de personas no estadounidenses que se crea razonablemente que se encuentran fuera de Estados Unidos con la asistencia obligada de proveedores de servicios de comunicaciones electrónicas estadounidenses[258]. Para recopilar información de inteligencia extranjera de conformidad con la Sección 702 de la FISA, el Fiscal General y el Director de Inteligencia Nacional presentan certificaciones anuales al Tribunal de Vigilancia de Inteligencia Extranjera (FISC) que identifican las categorías de información de inteligencia extranjera que debe adquirirse[259]. Las certificaciones deben ir acompañadas de procedimientos de selección, minimización y consulta, que también son aprobados por el Tribu nal y son jurídicamente vinculantes para las agencias de inteligencia estadounidenses.

(143) La FISC es un tribunal independiente[260] creado por ley federal cuyas decisiones pueden ser recurridas ante el Tribunal de Revisión de la Vigilancia de Inte-

---

255 Sección 2(c)(ii)(B) OE 14086. En caso de que surjan nuevos imperativos de seguridad nacional, como nuevas amenazas a la seguridad nacional, el Presidente podrá actualizar esta lista. En principio, dichas actualizaciones deben hacerse públicas, a menos que el Presidente determine que hacerlo supondría en sí mismo un riesgo para la seguridad nacional de Estados Unidos (Sección 2(c)(ii)(C) OE 14086). Por lo que se refiere a las consultas de datos recogidos en bloque, véase la Sección 2(c)(iii)(D) de la OE 14086.

256 Sección 2(a)(ii)(A), en relación con la Sección 2(c)(iii)(D) OE 14086. Véase también el anexo VII.

257 50 U.S.C. § 1881.

258 50 U.S.C. § 1881a (a). En particular, como señaló el PCLOB, la vigilancia de la Sección 702 "consiste enteramente en dirigirse a personas [no estadounidenses] específicas sobre las que se ha tomado una determinación individualizada" (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 if the Foreign Intelligence Surveillance Act, 2 de julio de 2014, Informe de la Sección 702, p. 111). Véase también NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16 de abril de 2014. El término "proveedor de servicios de comunicaciones electrónicas" se define en 50 U.S.C. § 1881 (a)(4).

259 50 U.S.C. § 1881a (g).

260 La FISC está compuesto por jueces nombrados por el Presidente del Tribunal Supremo de Estados Unidos de entre Jueces de tribunales de distrito de Estados Unidos, que previamente han sido nombrados por el Presidente y confirmados por el Senado. Los jueces, que son vitalicios y sólo pueden ser destituidos por causa justificada, forman

ligencia Extranjera (FISCR)[261] y, en última instancia, ante el Tribunal Supremo de los Estados Unidos[262]. El FISC (y el FISCR) cuenta con el apoyo de un grupo permanente de cinco abogados y cinco expertos técnicos con experiencia en asuntos de seguridad nacional, así como en libertades civiles[263]. De entre este grupo, el tribunal nombra a una persona para que actúe como *amicus curiae* para ayudar en el examen de cualquier solicitud de orden o revisión que, en opinión del tribunal, presente una interpretación novedosa o significativa de la ley, a menos que el tribunal considere que tal nombramiento no es apropiado[264]. Esto garantiza, en particular, que las consideraciones de privacidad se reflejen adecuadamente en la evaluación del tribunal. El tribunal también puede designar a una persona u organización para que actúe como *amicus curiae*, incluso para que aporte conocimientos técnicos, siempre que lo considere oportuno o, previa petición, autorizar a una persona u organización a presentar un escrito *amicus curiae*[265].

(144) La FISC revisa las certificaciones y los procedimientos relacionados (en particular los procedimientos de selección y minimización) para comprobar si cumplen los requisitos de la FISA. Si considera que no se cumplen los requisitos, puede denegar la certificación total o parcialmente y solicitar que se modifiquen los procedimientos[266]. A este respecto, la FISC ha confirmado en repetidas ocasiones que su examen de los procedimientos de selección y minimización del artículo 702 no se limita a los procedimientos tal como están redactados, sino que también incluye la forma en que los procedimientos son aplicados por el Gobierno[267].

(145) La Agencia de Seguridad Nacional (NSA, la agencia de inteligencia responsable de la selección de objetivos en virtud del artículo 702 de la FISA) determina

---

parte de la FISC por mandatos escalonados de siete años. La FISA exige que los jueces sean elegidos entre al menos siete Circuitos judiciales estadounidenses. Véase 50 U.S.C. § 1803 (a). Los jueces cuentan con el apoyo de asistentes jurídicos judiciales experimentados que constituyen el personal jurídico del tribunal y preparan el análisis jurídico de las solicitudes de recopilación. Véase la Carta del Honorable Reggie B. Walton, Juez Presidente del Tribunal de Vigilancia de Inteligencia Extranjera de Estados Unidos, al Honorable Patrick J. Leahy, Presidente del Comité Judicial del Senado de Estados Unidos (29 de julio de 2013) (Carta de Walton), p. 2, disponible en https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

261 El FISCR está compuesto por jueces nombrados por el Presidente del Tribunal Supremo de Estados Unidos y procedentes de Tribunales de distrito o tribunales de apelación de EE.UU., con mandatos escalonados de siete años. Véase 50 U.S.C. § 1803 (b).

262 Véanse 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

263 50 U.S.C. § 1803 (i)(1),(3)(A).

264 50 U.S.C. § 1803 (i)(2)(A).

265 50 U.S.C. § 1803 (i)(2)(B).

266 Véase por ejemplo FISC Dictamen de 18 octubre 2018, disponible enhttps://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, confirmado por el Tribunal de Revisión de Inteligencia Extranjera en su Dictamen de 12 de julio de 2019, disponible en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_O pinion_12Jul19.pdf .

267 Véase, por ejemplo, FISC, Memorandum Opinion and Order en 35 (18 de noviembre de 2020) (autorizado para su publicación el 26 de abril de 2021), (anexo D).

los objetivos individuales de conformidad con los procedimientos de selección de objetivos aprobados por la FISC, que exigen que la NSA evalúe, basándose en la totalidad de las circunstancias, que es probable que la selección de una persona específica permita obtener una categoría de información de inteligencia extranjera identificada en una certificación[268]. Esta evaluación debe estar particularizada y basada en hechos, y basarse en el juicio analítico, la formación especializada y la experiencia del analista, así como en la naturaleza de la información de inteligencia extranjera que debe obtenerse[269]. La selección de objetivos se lleva a cabo mediante la identificación de los denominados selectores, que identifican medios de comunicación específicos, como la dirección de correo electrónico o el número de teléfono del objetivo, pero nunca palabras clave o nombres de personas[270].

(146) Los analistas de la NSA identificarán en primer lugar a las personas no estadounidenses situadas en el extranjero cuya vigilancia conducirá, según la evaluación de los analistas, a la inteligencia extranjera pertinente especificada en la certificación[271]. Tal como se establece en los procedimientos de selección de objetivos de la NSA, ésta sólo puede dirigir la vigilancia a un objetivo cuando ya ha averiguado algo sobre el mismo[272]. Esto puede proceder de información de distintas fuentes, por ejemplo, inteligencia humana. A través de estas otras fuentes, el analista también debe conocer un selector específico (es decir, una cuenta de comunicación) utilizado por el objetivo potencial. Una vez que estas personas individualizadas han sido identificadas y su selección ha sido aprobada por un amplio mecanismo de revisión dentro de la NSA[273], los selectores que identifican los medios de comunicación (como las direcciones de correo electrónico) utilizados por los objetivos serán "tasked" (es decir, desarrollados y aplicados)[274].

---

268 50 U.S.C. § 1881a(a), Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, de marzo de 2018 (NSA targeting procedures), disponible en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Tar geting_27Mar18.pdf, p. 1-4, explicado con más detalle en el informe de la PCLOB, pp. 41-42.

269 Procedimientos de selección de objetivos de la NSA, p. 4.

270 Véase PCLOB, Informe sobre la Sección 702, pp. 32-33, 45 con referencias adicionales. Véase también Evaluación semestral del cumplimiento de los procedimientos y directrices emitidos de conformidad con la Sección 702 de la Ley de Vigilancia de Inteligencia Extranjera, presentada por el Fiscal General y el Director de Inteligencia Nacional, Período de presentación de informes: 1 de diciembre de 2016 - 31 de mayo de 2017, p. 41 (octubre de 2018), disponible en: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

271 PCLOB, Informe sobre la Sección 702, pp. 42-43.

272 Procedimientos de selección de objetivos de la NSA, p. 2.

273 PCLOB, Informe sobre la Sección 702, p. 46. Por ejemplo, la NSA debe verificar que existe una conexión entre el objetivo y el selector, debe documentar la información de inteligencia extranjera que se espera adquirir, esta información debe ser revisada y aprobada por dos analistas superiores de la NSA, y el proceso global será objeto de seguimiento para posteriores revisiones de cumplimiento por parte de la ODNI y el Departamento de Justicia. Véase NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702, 16 de abril de 2014.

274 50 U.S.C. § 1881a (h).

(147) La NSA deberá documentar los hechos en los que se basa la selección del objetivo[275] y, a intervalos regulares tras la selección inicial, confirmar que se sigue cumpliendo la norma de selección de objetivos[276]. Cuando deje de cumplirse la norma de selección de objetivos, deberá cesar la recogida[277]. Los funcionarios de las oficinas de supervisión de los servicios de inteligencia del Departamento de Justicia revisan cada dos meses la selección de cada objetivo por parte de la NSA, así como el registro de cada evaluación y justificación de la selección de objetivos, para comprobar que se cumplen los procedimientos de selección de objetivos, y tienen la obligación de informar de cualquier infracción al FISC y al Congreso[278]. La documentación escrita de la NSA facilita la supervisión por parte de la FISC de si determinadas personas son objeto de una investigación adecuada en virtud del artículo 702 de la FISA, de conformidad con sus competencias de supervisión descritas en los considerandos 173 a 174[279]. Por último, el Director de Inteligencia Nacional (DNI) también está obligado a informar cada año del número total de objetivos de la Sección 702 FISA en informes públicos anuales de transparencia estadística. Las empresas que reciben directrices FISA de la Sección 702 pueden publicar datos agregados (a través de informes de transparencia) sobre las solicitudes que reciben[280].

(148) En cuanto a las demás bases jurídicas para recoger datos personales transferidos a organizaciones en EE.UU., se aplican diferentes limitaciones y salvaguardias. En general, la recopilación de datos en bloque está específicamente prohibida en virtud de la Sección 402 de la FISA (autoridad de registro de

---

275 Procedimientos de selección de objetivos de la NSA, p. 8. Véase también PCLOB, Section 702 Report, p 46. La no presentación de una justificación por escrito constituye un incidente de cumplimiento de la documentación que debe notificarse al FISC y al Congreso. Véase Evaluación semestral del cumplimiento de los procedimientos y directrices emitidos de conformidad con la Sección 702 de la Ley de Vigilancia de Inteligencia Extranjera, presentada por el Fiscal General y el Director de Inteligencia Nacional, Período del informe: 1 de diciembre de 2016 - 31 de mayo de 2017, p. 41 (octubre de 2018), DOJ/ODNI Compliance Report to FISC for Dec. 2016 - May 2017 en p. A-6, disponible en https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

276 Véase U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, en 2-3 (15 de julio de 2015) y la información facilitada en el anexo VII.

277 Véase U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summary of Notable Section 702 Requirements, en 2-3 (15 de julio de 2015), que establece que el Gobierno "[s]i el Gobierno evalúa posteriormente que no se espera que la continuación de la asignación de tareas al selector de un objetivo dé lugar a la obtención de información de inteligencia extranjera, se requiere la pronta desasignación de tareas, y la demora puede dar lugar a un incidente de cumplimiento notificable". Véase también la información facilitada en el anexo VII.

278 PCLOB, Section 702 Report, pp. 70-72; Rule 13(b) of the Rules of Procedure of the United States Intelligence, disponible en https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

279 Véase también DOJ/ODNI Compliance Report to FISC for Dec. 2016 - May 2017 en p. A-6.

280 50 U.S.C. § 1874.

pluma y de trampa y rastreo) y mediante el uso de NSL, y en su lugar se exige el uso de "términos de selección" específicos[281].

(149) Para llevar a cabo una vigilancia electrónica individualizada tradicional (de conformidad con la Sección 105 de la FISA), las agencias de inteligencia deben presentar una solicitud a la FISC con una declaración de los hechos y circunstancias en los que se basan para justificar la creencia de que existe causa probable de que la instalación es utilizada o está a punto de ser utilizada por una potencia extranjera o un agente de una potencia extranjera[282]. La FISC evaluará, entre otras cosas, si sobre la base de los hechos presentados existe causa probable de que así sea efectivamente[283].

(150) Para llevar a cabo un registro de locales o bienes que tenga por objeto la inspección, incautación, etc. de información, material o bienes (por ejemplo, un dispositivo informático) sobre la base de la Sección 301 de la FISA, se requiere una solicitud de orden de la FISC[284]. Dicha solicitud debe, entre otras cosas, demostrar que existe una causa probable de que el objetivo de la búsqueda es una potencia extranjera o un agente de una potencia extranjera; que el local o la propiedad que se va a registrar contiene información de inteligencia extranjera y que el local que se va a registrar es propiedad de una potencia extranjera (agente de una), o es utilizado o está en posesión de una potencia extranjera (agente de una) o está en tránsito hacia o desde una potencia extranjera(agente de una)[285].

(151) Del mismo modo, la instalación de registros de pluma o dispositivos de trampa y rastreo (de conformidad con la sección 402 de la FISA) requiere una solicitud de orden de la FISC (o de un juez de primera instancia de EE.UU.) y el uso de un término de selección específico, es decir, un término que identifique específicamente a una persona, cuenta, etc. y que se utilice para limitar, en la mayor medida razonablemente posible, el alcance de la información buscada[286]. Esta autoridad no se refiere al contenido de las comunicaciones, sino que tiene por objeto la información sobre el cliente o abonado que utiliza un servicio (como nombre, dirección, número de abonado, duración/tipo de servicio recibido, fuente/mecanismo de pago).

(152) El artículo 501 de la FISA[287], que permite la recopilación de registros comerciales de un transportista común (es decir, cualquier persona o entidad que transporte personas o bienes por tierra, ferrocarril, agua o aire a cambio de una remuneración), un establecimiento de alojamiento público (por ejemplo, un hotel, motel o posada), un establecimiento de alquiler de vehículos o un establecimiento de almacenamiento físico (es decir, que proporcione espacio o

---

281 50 U.S. Code § 1842(c)(3) y, por lo que se refiere a NSL, 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C.§ 1681v(a); y 18 U.S.C. § 2709(a).

282 Un "agente de una potencia extranjera" puede incluir a personas no estadounidenses que se dediquen al terrorismo internacional o a la proliferación internacional de armas de destrucción masiva (incluidos los actos preparatorios) (50 U.S.C. § 1801 (b)(1)).

283 50 U.S.C. § 1804. Véase también § 1841(4) con respecto a la elección de las condiciones de selección.

284 50 U.S.C. § 1821(5).

285 50 U.S.C. § 1823(a).

286 50 U.S.C. § 1842 con § 1841(2) y Sección 3127 del Título 18.

287 50 U.S.C. § 1862.

servicios relacionados con el almacenamiento de bienes y materiales)[288], también requiere una solicitud a la FISC o a un juez de instrucción. Esta solicitud debe especificar los registros solicitados y los hechos específicos y articulables que dan motivos para creer que la persona a la que pertenecen los registros es una potencia extranjera o un agente de una potencia extranjera[289].

(153) Por último, las NSL están autorizadas por diferentes estatutos y permiten a los organismos de investigación obtener cierta información (sin incluir el contenido de las comunicaciones) de determinadas entidades (por ejemplo, instituciones financieras, agencias de información crediticia, proveedores de comunicaciones electrónicas) contenida en informes de crédito, registros financieros y registros electrónicos de abonados y transacciones[290]. El estatuto NSL que autoriza el acceso a las comunicaciones electrónicas sólo puede ser utilizado por el FBI y requiere que las solicitudes utilicen un término que identifique específicamente a una persona, entidad, número de teléfono o cuenta y certifique que la información es relevante para una investigación autorizada de seguridad nacional para proteger contra el terrorismo internacional o actividades clandestinas de inteligencia[291]. Los destinatarios de una NSL tienen derecho a impugnarla ante los tribunales[292].

3.2.1.3. Uso posterior de la información recogida

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

(155) En primer lugar, cada agencia de inteligencia debe garantizar la seguridad adecuada de los datos e impedir el acceso de personas no autorizadas a los datos personales recogidos a través de la inteligencia de señales. A este respecto, distintos instrumentos, incluidos estatutos, directrices y normas, especifican con mayor detalle los requisitos mínimos de seguridad de la información que deben establecerse (por ejemplo, autenticación multifactor, cifrado, etc.)[293]. El acceso a los datos recopilados debe limitarse al personal autorizado y formado

288 50 U.S.C. §§ 1861-1862.

289 50 U.S.C. § 1862(b).

290 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; y 18 U.S.C. § 2709.

291 18 U.S.C. § 2709(b).

292 Por ejemplo, 18 U.S.C. § 2709(d).

293 Sección 2(c)(iii)(B)(1) de la OE 14086. Véase también el Título VIII de la Ley de Seguridad Nacional (que detalla los requisitos de acceso a la información clasificada), E.O. 12333 sección 1.5 (que exige a los Jefes de las Agencias de la Comunidad de Inteligencia que sigan las directrices de intercambio de información y seguridad, privacidad de la información y otros requisitos legales), Directiva de Seguridad Nacional 42, "Política Nacional para la Seguridad de las Telecomunicaciones de Seguridad Nacional y Sistemas de Información" (que ordena al Comité de Sistemas de Seguridad Nacional que proporcione orientación sobre la seguridad de los sistemas de seguridad nacional a los departamentos ejecutivos y agencias), y National Security Memorandum 8, "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems" (en el que se establecen plazos y orientaciones sobre cómo se aplicarán los requisitos de ciberseguridad a los sistemas de seguridad nacional, incluida la autenticación multifactor, el cifrado, las tecnologías en la nube y los servicios de detección de puntos finales).

que necesite conocer la información para llevar a cabo su misión[294]. En términos más generales, las agencias de inteligencia deben proporcionar una formación adecuada a sus empleados, incluidos los procedimientos para denunciar y abordar las infracciones de la ley (incluida la OE 14086)[295].

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

(157) En tercer lugar, en lo que respecta a la conservación de datos, la OE 14086 aclara que los datos personales de personas no estadounidenses están sujetos a los mismos periodos de conservación que los que se aplican a los datos de Personas estadounidenses[297]. Las agencias de inteligencia están obligadas a definir periodos de conservación específicos y/o los factores que deben tenerse en cuenta para determinar la duración de los periodos de conservación aplicables (por ejemplo, si la información es prueba de un delito; si la información constituye información de inteligencia extranjera; si la información es necesaria para proteger la seguridad de personas u organizaciones, incluidas las víctimas u objetivos del terrorismo internacional), que se establecen en diferentes instrumentos jurídicos[298].

(158) En cuarto lugar, se aplican normas específicas en lo que respecta a la difusión de datos personales recogidos a través de la inteligencia de señales. Como requisito general, los datos personales sobre personas no estadounidenses sólo pueden difundirse si se trata del mismo tipo de información que puede difundirse sobre personas estadounidenses, por ejemplo, información necesaria para proteger la seguridad de una persona u organización (como objetivos, víctimas o rehenes de organizaciones terroristas internacionales)[299]. Además, los datos personales no podrán difundirse únicamente en razón de la nacionalidad o el país de residencia de una persona o con el fin de eludir los requisitos de la OE 14086[300]. La difusión dentro de la Administración estadounidense sólo puede tener lugar si una persona autorizada y capacitada tiene la convicción razonable de que el destinatario

294 Sección 2(c)(iii)(B)(2) OE 14086. Además, sólo se podrá acceder a los datos personales para los que no se haya tomado una decisión definitiva de conservación con el fin de tomar o apoyar dicha decisión o para llevar a cabo funciones administrativas, de prueba, desarrollo, seguridad o supervisión autorizadas (Sección 2(c)(iii)(B)(3) de la OE 14086.

295 Sección 2(d)(ii) OE 14086.

296 Sección 2(c)(iii)(C) OE 14086.

297 Sección 2(c)(iii)(A)(2)(a)-(c) OE 14086. En términos más generales, cada agencia debe establecer políticas y procedimientos diseñados para minimizar la difusión y conservación de los datos personales recogidos a través de la inteligencia de señales (Sección 2(c)(iii)(A) OE 14086).

298 Véase, por ejemplo, la Sección 309 de la Ley de Autorización de Inteligencia para el Año Fiscal 2015; los procedimientos de minimización adoptados por las agencias de inteligencia individuales en virtud de la Sección 702 de la FISA y autorizados por la FISC; los procedimientos aprobados por el Fiscal General y la FRA (que exigen a las agencias federales estadounidenses, incluidas las agencias de seguridad nacional, que establezcan periodos de conservación para sus registros que deben ser aprobados por la Administración Nacional de Archivos y Registros).

299 Sección 2(c)(iii)(A)(1)(a) y 5(d) OE 14086, junto con la sección 2.3 OE 12333.

300 Sección 2(c)(iii)(A)(1)(b) y (e)OE 14086.

tiene necesidad de conocer la información[301] y la protegerá adecuadamente[302]. Para determinar si los datos personales pueden difundirse a destinatarios ajenos a la Administración estadounidense (incluido un Gobierno extranjero o una organización internacional), deben tenerse en cuenta la finalidad de la difusión, la naturaleza y el alcance de los datos que se difunden y el posible impacto perjudicial sobre la persona o personas afectadas[303].

(159) Por último, también con el fin de facilitar la supervisión del cumplimiento de los requisitos legales aplicables, así como la reparación efectiva, cada agencia de inteligencia está obligada, en virtud de la OE 14086, a conservar la documentación adecuada sobre la recogida de información de inteligencia de señales. Los requisitos de documentación cubren elementos tales como la base fáctica para la evaluación de que una actividad de recopilación específica es necesaria para avanzar en una prioridad de inteligencia validada[304].

(160) Además de las citadas salvaguardias de la OE n° 14086 para el uso de la información recopilada a través de la inteligencia de señales, todas las agencias de inteligencia estadounidenses están sujetas a requisitos más generales sobre limitación de fines, minimización de datos, exactitud, seguridad, conservación y difusión, derivados en particular de la Circular A-130 de la OMB, la Ley de Administración Electrónica, la Ley Federal de Registros (véanse los considerandos 101 a 106) y las orientaciones del Comité de Sistemas de Seguridad Nacional (CNSS)[305].

3.2.2. Supervisión

(161) Las actividades de las agencias de inteligencia estadounidenses están sujetas a la supervisión de distintos organismos.

(162) En primer lugar, la OE 14086 exige que cada agencia de inteligencia cuente con funcionarios de alto nivel encargados de las cuestiones jurídicas, la supervisión y el cumplimiento para garantizar el cumplimiento de la legislación estadounidense aplicable[306]. En particular, deben llevar a cabo una supervisión periódica de las actividades de inteligencia de señales y garantizar que se ponga remedio a cualquier incumplimiento. Las agencias de inteligencia deben proporcionar a dichos funcionarios acceso a toda la información pertinente para llevar a cabo

---

301 Véase, por ejemplo, el AGG-DOM, que establece que el FBI sólo puede difundir información si el destinatario tiene necesidad de conocerla para cumplir su misión o para proteger al público.

302 Sección 2(c)(iii)(A)(1)(c) OE 14086. Las agencias de inteligencia pueden, por ejemplo, difundir información en circunstancias relevantes para una investigación penal o en relación con un delito, incluyendo, por ejemplo, la difusión de advertencias de amenazas de muerte, lesiones corporales graves o secuestro; la difusión de información sobre amenazas cibernéticas, incidentes o respuesta a intrusiones; y la notificación a las víctimas o la advertencia a las víctimas potenciales de delitos.

303 Sección 2(c)(iii)(A)(1)(d) OE 14086.

304 Sección 2(c)(iii)(E) OE 14086.

305 Véase la Política n° 22 del CNSS, Política de gestión de riesgos de ciberseguridad, y la Instrucción 1253 del CNSS, que ofrece orientaciones detalladas sobre las medidas de seguridad que deben aplicarse a los sistemas de seguridad nacional.

306 Sección 2(d)(i)(A)-(B) OE 14086.

sus funciones de supervisión y no pueden tomar ninguna medida para obstaculizar o influir indebidamente en sus actividades de supervisión[307]. Por otra parte, cualquier incidente significativo de incumplimiento[308] identificado por un funcionario de supervisión o cualquier otro empleado debe ser comunicado sin demora al jefe de la agencia de inteligencia y al Director de Inteligencia Nacional, quienes deben garantizar que se tomen las medidas necesarias para remediar y prevenir la repetición del incidente significativo de incumplimiento[309].

(163) Esta función de supervisión es desempeñada por funcionarios con un papel designado en materia de cumplimiento, así como por responsables de privacidad y libertades civiles e inspectores generales[310].

(164) Al igual que en el caso de las autoridades encargadas de la aplicación de la ley penal, en todos los organismos de inteligencia existen responsables de la privacidad y las libertades civiles[311]. Las competencias de estos responsables suelen abarcar la supervisión de los procedimientos para garantizar que el respectivo departamento/organismo tiene debidamente en cuenta los problemas relacionados con la privacidad y las libertades civiles y ha establecido los procedimientos adecuados para atender las quejas de las personas que consideren que se ha vulnerado su privacidad o sus libertades civiles (y en algunos casos, como el de la Oficina del Director de Inteligencia Nacional (ODNI), pueden estar ellos mismos facultados para investigar las quejas[312]). Los jefes de los organismos de inteligencia deben garantizar que los responsables de la privacidad y las libertades civiles dispongan de los recursos necesarios para cumplir su mandato, tengan acceso al material y al personal necesarios para desempeñar sus funciones, y sean informados y consultados sobre los cambios de política propuestos[313]. Los responsables de la protección de la intimidad y las libertades civiles informan periódicamente al Congreso y al PCLOB, en particular sobre el número y la naturaleza de las denuncias recibidas por el departamento/organismo con un resumen de la resolución de dichas denuncias, las revisiones e investigaciones realizadas y el impacto de las actividades llevadas a cabo por el funcionario[314].

---

307 Secciones 2(d)(i)(B)-(C) OE 14086.

308 Es decir, un incumplimiento sistemático o intencionado de la legislación estadounidense aplicable que podría poner en entredicho la reputación o integridad de un elemento de la Comunidad de Inteligencia o cuestionar de otro modo la corrección de una actividad de la Comunidad de Inteligencia, incluso a la luz de cualquier impacto significativo en los intereses de privacidad y libertades civiles de la persona o personas afectadas, véase la Sección 5(l) de la OE 14086.

309 Sección 2(d)(iii) OE 14086.

310 Sección 2(d)(i)(B) OE 14086.

311 Véase 42 U.S.C. § 2000ee-1. Esto incluye, por ejemplo, el Departamento de Estado, el Departamento de Justicia, el Departamento de Seguridad Nacional, el Departamento de Defensa, la NSA, la Agencia Central de Inteligencia (CIA), el FBI y la ODNI.

312 Véase la sección 3(c) de la OE 14086.

313 42 U.S.C. § 2000ee-1(d).

314 Véase 42 U.S.C. § 2000ee-1 (f)(1),(2). Por ejemplo, el informe de la Oficina de Libertades Civiles, Privacidad y Transparencia de la NSA de enero de 2021 a junio de 2021 muestra que llevó a cabo 591 revisiones de las libertades civiles y el impacto en la privacidad en diversos contextos, por ejemplo, con respecto a las actividades de recopilación, los acuerdos y decisiones de intercambio de información, las decisiones de conservación de datos,

(165) En segundo lugar, cada organismo de inteligencia cuenta con un Inspector General independiente encargado, entre otras cosas, de supervisar las actividades de inteligencia exterior. Esto incluye, dentro de la ODNI, una Oficina del Inspector General de la Comunidad de Inteligencia con jurisdicción global sobre toda la Comunidad de Inteligencia que está autorizada a investigar las quejas o informaciones relativas a alegaciones de conducta ilegal, o abuso de autoridad, en relación con los programas y actividades de la ODNI y/o de la Comunidad de Inteligencia[315]. Al igual que en el caso de las autoridades encargadas de la aplicación de la ley penal (véase el considerando 109), dichos Inspectores Generalmente son estatutariamente independientes[316] y responsables de realizar auditorías e investigaciones relativas a los programas y operaciones llevados a cabo por la agencia respectiva con fines de inteligencia nacional, incluso en lo que se refiere a abusos o violaciones de la ley[317]. Tienen acceso a todos

etc., teniendo en cuenta diferentes factores, como la cantidad y el tipo de información asociada a la actividad, las personas implicadas, la finalidad y el uso previsto de los datos, las salvaguardias existentes para mitigar los posibles riesgos para la privacidad, etc. (https://media.defense.gov/2022/Apr/11/2002974486/-1/- 1/1/REPORT%207_CLPT%20 JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Del mismo modo, la los informes de la Oficina de Privacidad y Libertades Civiles de la CIA de enero a junio de 2019 proporcionan información sobre las actividades de supervisión de la Oficina, por ejemplo, una revisión del cumplimiento de las Directrices del Fiscal General en virtud de la OE 12333 con respecto a la retención y difusión de información, orientación proporcionada sobre la aplicación del PPD 28 y los requisitos para identificar y abordar las violaciones de datos, y revisiones del uso y manipulación de información personal información personal (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual- Report.pdf).

315 Este Inspector General es nombrado por el Presidente, con confirmación del Senado, y sólo puede ser destituido por el Presidente.

316 Los Inspectores Generales gozan de estabilidad en el cargo y sólo pueden ser destituidos por el Presidente, que debe comunicar por escrito al Congreso las razones de su destitución. Esto no significa necesariamente que estén completamente libres de instrucciones. En algunos casos, el jefe del departamento puede prohibir al Inspector General que inicie, lleve a cabo o complete una auditoría o investigación cuando ello se considere necesario para preservar importantes intereses (de seguridad) nacionales. Sin embargo, el Congreso debe ser informado del ejercicio de esta autoridad y, sobre esta base, podría exigir responsabilidades al director respectivo. Véase, por ejemplo, Inspector General Act de 1978, § 8 (para el Departamento de Defensa); § 8E (para el DOJ), § 8G (d)(2)(A),(B) (para la NSA); 50. U.S.C. § 403q (b) (para la CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (para la Comunidad de Inteligencia).

317 Ley del Inspector General de 1978, modificada, Pub. L. 117-108, de 8 de abril de 2022. Por ejemplo, como se explica en sus informes semestrales al Congreso correspondientes al período comprendido entre el 1 de abril de 2021 y el 31 de marzo de 2022, el Inspector General de la NSA llevó a cabo evaluaciones del tratamiento de la información sobre personas estadounidenses recogida en virtud de la OE 12333, el proceso de depuración de datos de inteligencia de señales, una herramienta automatizada de selección de objetivos utilizada por la NSA, y el cumplimiento de las normas de documentación y consulta con respecto a la recogida de información en virtud de la Sección 702 de la FISA, y emitió varias recomendaciones en este contexto (véase https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%2021%20-%20Unclassified.pdf ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, pp. 5-8 y https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d %3d&ti-

los registros, informes, auditorías, revisiones, documentos, papeles, recomendaciones u otro material pertinente, si es necesario mediante citación, y pueden tomar declaración[318]. Los Inspectores Generales remiten los casos de presuntas infracciones penales para su enjuiciamiento y formulan recomendaciones de medidas correctoras a los responsables de los organismos[319]. Aunque sus recomendaciones no son vinculantes, sus informes, incluidos los relativos a las medidas de seguimiento (o a la falta de ellas)[320] suelen hacerse públicos y enviarse al Congreso, que puede ejercer así su propia función de supervisión (véanse los considerandos 168-169)[321].

(166) En tercer lugar, el Intelligence Oversight Board (IOB), creado en el seno del President's Intelligence Advisory Board (PIAB), supervisa el cumplimiento por parte de las autoridades de inteligencia estadounidenses de la Constitución y de todas las normas aplicables[322]. El PIAB es un órgano consultivo de la Oficina Ejecutiva del Presidente compuesto por 16 miembros nombrados por el Presidente de fuera del gobierno de Estados Unidos. El IOB está formado por un máximo de cinco miembros designados por el Presidente de entre los miembros del PIAB . De acuerdo con la OE 12333[323], los jefes de todas las agencias de inteligencia están obligados a informar a la IOB de cualquier actividad de

mestamp=1657810395907, pp. 10-13). Véanse también las recientes auditorías e investigaciones llevadas a cabo por el Inspector General de la Comunidad de Inteligencia sobre seguridad de la información y revelaciones no autorizadas de información clasificada de seguridad nacional (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, pp. 8, 11 y https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021- Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, pp. 19-20).

318 Véase la Ley del Inspector General de 1978, § 6.

319 Véase *ibid*. §§ 4, 6-5.

320 En cuanto al seguimiento que se da a los informes y recomendaciones de los Inspectores Generales, véase por ejemplo, la respuesta a un informe del inspector general del DoJ que determinó que el FBI no fue suficientemente transparente con el FISC en las solicitudes de 2014 a 2019, lo que dio lugar a reformas para mejorar el cumplimiento, la supervisión y la rendición de cuentas en el FBI (por ejemplo, el director del FBI ordenó más de 40 medidas correctivas, incluidas 12 específicas para el proceso FISA relacionadas con la documentación, la supervisión, el mantenimiento de archivos, la formación y las auditorías) (véase https://www.justice.gov/opa/pr/department-justice-and-federal- bureau-investigation- announce-critical-reforms-enhance y https://oig.justice.gov/reports/2019/o20012.pdf). Véase también, por ejemplo, la auditoría del Inspector General del Departamento de Justicia sobre las funciones y responsabilidades de la Oficina del Consejero General del FBI en la supervisión del cumplimiento de las leyes, políticas y procedimientos aplicables en relación con las actividades de seguridad nacional del FBI y el Apéndice 2, que incluye una carta del FBI aceptando todas las recomendaciones. A este respecto, el Apéndice 3 ofrece una visión general de las medidas de seguimiento y la información que el Inspector General exigió al FBI para poder cerrar sus recomendaciones (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

321 Véase la Ley del Inspector General de 1978, §§ 4(5), 5.

322 Véase la OE 13462.

323 Sección 1.6(c) OE 12333.

inteligencia de la que existan razones para creer que puede ser ilegal o contraria a una Orden Ejecutiva o Directiva Presidencial. Para garantizar que la IOB tenga acceso a la información necesaria para el desempeño de sus funciones, la Orden Ejecutiva 13462 ordena al Director de Inteligencia Nacional y a los jefes de las agencias de inteligencia que proporcionen cualquier información y asistencia que la IOB determine que es necesaria para el desempeño de sus funciones, en la medida en que lo permita la ley[324]. A su vez, la IOB está obligada a informar al Presidente sobre las actividades de inteligencia que considere que puedan infringir la legislación estadounidense (incluidas las Órdenes Ejecutivas) y que no estén siendo abordadas adecuadamente por el Fiscal General, el Director de Inteligencia Nacional o el jefe de una agencia de inteligencia[325]. Además, la IOB está obligada a informar al Fiscal General sobre posibles infracciones de la legislación penal.

(167) En cuarto lugar, las agencias de inteligencia están sujetas a la supervisión del PCLOB. Según su estatuto fundacional, el PCLOB tiene encomendadas responsabilidades en el ámbito de las políticas antiterroristas y su aplicación, con vistas a proteger la intimidad y las libertades civiles. En su revisión de las actuaciones de las agencias de inteligencia, puede acceder a todos los registros, informes, auditorías, revisiones, documentos, papeles y recomendaciones pertinentes de las agencias, incluyendo información clasificada, realizar entrevistas y escuchar testimonios[326]. Recibe informes de los responsables de libertades civiles y privacidad de varios departamentos y organismos federales[327], puede formular recomendaciones al Gobierno y a los organismos de inteligencia, e informa periódicamente a las comisiones del Congreso y al Presidente[328]. Los informes del Consejo, incluidos los dirigidos al Congreso, deben hacerse públicos en la mayor medida posible[329]. El PCLOB ha publicado varios informes de supervisión y seguimiento, incluido un análisis de los programas ejecutados sobre la base de la Sección 702 de la FISA y la protección de la intimidad en este contexto, la aplicación del PPD 28 y la OE 12333[330]. El PCLOB también está encargado de llevar a cabo funciones específicas de supervisión por lo que se refiere a la aplicación de la OE 14086, en particular revisando si los procedimientos de las agencias son coherentes con la OE (véase el considerando 126) y evaluando el correcto funcionamiento del mecanismo de recurso (véase el considerando 194).

---

324 Sección 8(a) OE 13462.

325 Sección 6(b) OE 13462.

326 42 U.S.C. § 2000ee (g).

327 Véase 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Estos incluyen al menos el Departamento de Justicia, el Departamento de Defensa, el Departamento de Seguridad Nacional, el Director de Inteligencia Nacional y la Agencia Central de Inteligencia, además de cualquier otro departamento, agencia o elemento del poder ejecutivo designado por el PCLOB como apropiado para la cobertura.

328 42 U.S.C. §2000ee (e).

329 42 U.S.C. § 2000ee (f).

330 Disponible en https://www.pclob.gov/Oversight.

(168) En quinto lugar, además de los mecanismos de supervisión dentro del poder ejecutivo, existen comités específicos en el Congreso de Estados Unidos (los Comités de Inteligencia y Judicial de la Cámara de Representantes y del Senado) que tienen responsabilidades de supervisión en relación con todas las actividades de inteligencia exterior de Estados Unidos. Los miembros de estos Comités tienen acceso a información clasificada, así como a métodos y programas de inteligencia[331]. Los Comités ejercen sus funciones de supervisión de distintas maneras, en particular mediante audiencias, investigaciones, revisiones e informes[332].

(169) Los Comités del Congreso reciben informes periódicos sobre las actividades de inteligencia, incluso del Fiscal General, el Director de Inteligencia Nacional, los organismos de inteligencia y otros órganos de supervisión (por ejemplo, los Inspectores Generales), véanse los considerandos 164-165. En particular, según la Ley de Seguridad Nacional, "[e]l Presidente se asegurará de que los comités de inteligencia del Congreso se mantengan plena y actualmente informados de las actividades de inteligencia de los Estados Unidos, incluida cualquier información significativa de actividad de inteligencia anticipada, tal y como exige este subcapítulo"[333]. Además, "[e]l Presidente se asegurará de que se informe sin demora a los comités de inteligencia del Congreso de cualquier actividad ilegal de inteligencia, así como de cualquier medida correctiva que se haya tomado o esté prevista en relación con dicha actividad ilegal"[334].

(170) Además, de estatutos específicos se derivan requisitos adicionales de información. En particular, la ley FISA exige al Fiscal General que "informe plenamente" a los Comités de Inteligencia y Judicial del Senado y de la Cámara de Representantes sobre las actividades del gobierno en virtud de determinadas secciones de la ley FISA[335]. También exige al Gobierno que proporcione a los comités del

331 50 U.S.C. § 3091.

332 Por ejemplo, las Comisiones organizan audiencias temáticas (véase, por ejemplo, una reciente audiencia de la Comisión Judicial de la Cámara de Representantes de los Estados Unidos). de la Cámara sobre "digitales dragnets", https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983, y una audiencia del Comité de Inteligencia de la Cámara de Representantes de la Cámara en el uso de uso de IA en la Inteligencia Inteligencia, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263) periódicas audiencias de supervisión, por ejemplo de la FBI y DoJ nacional seguridad nacional nacional, ver https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-f e d eral-bureau-of- investigación; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 y https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. Como ejemplo de investigación, véase la investigación del Comité de Inteligencia del Senado sobre la injerencia rusa en las elecciones de 2016. EE.UU. elecciones, véase https://www.intelligence.senate.gov/publications/report-select- committee- intelligence-united-states-senate-russian-active-measures. En cuanto a los informes, véase, por ejemplo, el resumen de las actividades (de supervisión) del Comité en el informe del Comité de Inteligencia del Senado correspondiente al periodo 4 enero 2019 3 Enero 2021 a el Senado, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states- senate-covering-period-january-4.

333 Véase 50 U.S.C. § 3091(a)(1). Esta disposición contiene los requisitos generales en materia de supervisión del Congreso en el ámbito de la seguridad nacional.

334 Véase 50 U.S.C. §3091(b).

335 Véase 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

Congreso copias de todas las decisiones, órdenes u opiniones del FISC o del FISCR que incluyan una "construcción o interpretación significativa" de las disposiciones de la FISA. En lo que respecta a la vigilancia en virtud de la Sección 702 de la FISA, la supervisión parlamentaria se ejerce mediante los informes exigidos por ley a los Comités de Inteligencia y Judicial, así como mediante frecuentes sesiones informativas y audiencias. Estos incluyen un informe semestral del Fiscal General en el que se describe el uso de la Sección 702 de la FISA, con documentos de apoyo, incluidos los informes de cumplimiento del Departamento de Justicia y del ODNI y una descripción de cualquier incidente de incumplimiento[336], y una evaluación semestral separada del Fiscal General y del DNI en la que se documenta el cumplimiento de los procedimientos de selección de objetivos y minimización[337].

(171) Además, la FISA exige que el gobierno de EE.UU. revele al Congreso (y al público) cada año el número de órdenes FISA solicitadas y recibidas, así como estimaciones del número de personas estadounidenses y no estadounidenses objeto de vigilancia, entre otros[338]. La Ley también exige información pública adicional sobre el número de NSL emitidas, también en relación con personas estadounidenses y no estadounidenses (al tiempo que permite a los receptores de órdenes y certificaciones FISA, así como de solicitudes de NSL, emitir informes de transparencia en determinadas condiciones)[339].

(172) En términos más generales, la comunidad de inteligencia de Estados Unidos lleva a cabo diversos esfuerzos para proporcionar transparencia sobre sus actividades de inteligencia (extranjera). Por ejemplo, en 2015, la ODNI adoptó los Principios de Transparencia de Inteligencia y un Plan de Implementación de Transparencia, y ordenó a cada agencia de inteligencia designar un Oficial de Transparencia de Inteligencia para fomentar la transparencia y liderar iniciativas de transparencia[340]. Como parte de estos esfuerzos, la Comunidad de Inteligencia ha hecho y sigue haciendo desclasificadas partes de políticas, procedimientos, informes de supervisión, informes sobre actividades en virtud de la Sección 702 de la FISA y la OE 12333, decisiones de la FISC y otros materiales públicos, incluso en una página web específica "IC on the Record", gestionada por el ODNI[341].

---

336 Véase 50 U.S.C. § 1881f.

337 Véase 50 U.S.C. § 1881a(l)(1).

338 50 U.S.C. § 1873(b). Además, según el artículo 402, "el Director de Inteligencia Nacional, en consulta con el Fiscal General, llevará a cabo una revisión de desclasificación de cada decisión, orden u opinión emitida por el Tribunal de Vigilancia de Inteligencia Extranjera o el Tribunal de Revisión de Vigilancia de Inteligencia Extranjera (según se define en el artículo 601(e)) que incluya una interpretación o interpretación significativa de cualquier disposición de la ley, incluida cualquier interpretación o interpretación nueva o significativa del término "término de selección específico", y, en consonancia con dicha revisión, pondrá a disposición del público en la mayor medida posible cada una de dichas decisiones, órdenes u opiniones".

339 50 U.S.C. §§ 1873(b)(7) y 1874.

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

341 Véase "IC on the Record", disponible en https://icontherecord.tumblr.com/.

(173) Por último, la recogida de datos personales en virtud del artículo 702 de la FISA está sujeta, además de a la supervisión de los organismos de control mencionados en los considerandos 162 a 168, a la supervisión de la FISC[342]. De conformidad con el artículo 13 del Reglamento interno de la FISC, los responsables del cumplimiento de las agencias de inteligencia de EE.UU. están obligados a informar de cualquier infracción de los procedimientos de selección, minimización y consulta del artículo 702 de la FISA al DoJ y al ODNI, que a su vez informan de ello a la FISC. Además, el DoJ y el ODNI presentan informes semestrales conjuntos de evaluación de la supervisión a la FISC, en los que se identifican las tendencias de cumplimiento de los objetivos, se facilitan datos estadísticos, se describen las categorías de incidentes de cumplimiento, se describen detalladamente las razones por las que se produjeron determinados incidentes de cumplimiento de los objetivos y se exponen las medidas que han adoptado los organismos de inteligencia para evitar que se repitan[343].

(174) En caso necesario (por ejemplo, si se detectan violaciones de los procedimientos de selección de objetivos), el Tribunal podrá ordenar a la agencia de inteligencia pertinente que adopte medidas correctoras[344]. Las medidas correctoras en cuestión pueden ir desde medidas individuales hasta estructurales, por ejemplo, desde la finalización de la adquisición de datos y la supresión de los datos obtenidos ilegalmente hasta un cambio en la práctica de recopilación, incluso en

342 En el pasado, la FISC concluyó que "[e]s evidente para el Tribunal que los organismos de ejecución, así como [el ODNI] y [la División de Seguridad Nacional del DOJ], dedican recursos sustanciales a sus responsabilidades de cumplimiento y supervisión en virtud de la Sección 702. Como regla general, los casos de incumplimiento se identifican con prontitud y se toman las medidas correctivas apropiadas, que incluyen la purga de información obtenida indebidamente o sujeta a requisitos de destrucción en virtud de los procedimientos aplicables. Por regla general, los casos de incumplimiento se identifican con prontitud y se adoptan las medidas correctivas apropiadas, que incluyen la eliminación de la información obtenida indebidamente o sujeta a requisitos de destrucción en virtud de los procedimientos aplicables". Tribunal FISA, Memorandum Opinion and Order [leyenda redactada] (2014), disponible en https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%20 26%20August%202014.pdf.

343 Véase, por ejemplo, DOJ/ODNI FISA 702 Compliance Report to FISC for June 2018 - Nov. 2018 en 21-65.

344 50 U.S.C. § 1803(h). Véase también PCLOB, Informe de la Sección 702, p. 76. Además, véase FISC Memorandum Opinion and Order de 3 de octubre de 2011 como ejemplo de una orden de deficiencia en la que se ordenó al gobierno a corregir la dirección deficiencias identificadas en deficiencias dentificadas en 30 días. Disponible en https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order- 20140716.pdf. Véase la carta de Walton, sección 4, pp. 10 -11. Véase también el dictamen de la FISC de 18 de octubre de 2018, disponible en https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin. _18Oct18.pdf, confirmado por el Tribunal de Revisión de Inteligencia Extranjera en su Dictamen de 12 de julio de 2019, disponible en https://www.intelligence.gov/assets/documents/702%20Documents/

términos de orientación y formación del personal[345]. Además, durante su revisión anual de las certificaciones de la Sección 702, la FISC examina los incidentes de incumplimiento para determinar si las certificaciones presentadas cumplen los requisitos de la FISA. Del mismo modo, si la FISC considera que las certificaciones del Gobierno no fueron suficientes, incluso debido a incidentes de cumplimiento concretos, puede emitir una denominada "orden de deficiencia" que exija al Gobierno subsanar la infracción en un plazo de 30 días o que exija al Gobierno cesar o no comenzar a aplicar la certificación de la Sección 702. Por último, la FISC evalúa las tendencias que observa en los problemas de cumplimiento y puede requerir cambios en los procedimientos o una supervisión e información adicionales para abordar las tendencias de cumplimiento[346].

3.2.3. Reparación

(175) Como se explica con más detalle en esta sección, varias vías en Estados Unidos ofrecen a los interesados de la Unión la posibilidad de emprender acciones legales ante un tribunal independiente e imparcial con poderes vinculantes. En conjunto, permiten a las personas tener acceso a sus datos personales, hacer que se revise la legalidad del acceso del gobierno a sus datos y, si se constata una violación, hacer que se subsane dicha violación, incluso mediante la rectificación o supresión de sus datos personales.

(176) En primer lugar, se establece un mecanismo de recurso específico, en virtud de la OE 14086, complementado por el Reglamento del Fiscal General por el que se crea el Tribunal de Revisión de la Protección de Datos, para tramitar y resolver las denuncias de particulares relativas a actividades de inteligencia de señales de Estados Unidos. Cualquier persona de la UE tiene derecho a presentar una denuncia ante el mecanismo de recurso en relación con una supuesta violación de la legislación estadounidense que regula las actividades de inteligencia de señales (por ejemplo, la OE 14086, la Sección 702 de la FISA, la OE 12333) que afecte negativamente a sus intereses en materia de privacidad y libertades civiles[347]. Este mecanismo de recurso está disponible para

---

declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, en la que la FISC, entre otras cosas, ordenó al Gobierno que cumpliera determinados requisitos de notificación, documentación y presentación de informes a la FISC.

345 Véase, por ejemplo, FISC, Memorandum Opinion and Order, en 76 (6 de diciembre de 2019) (autorizado para su publicación el 4 de septiembre de 2020), en el que la FISC ordenó al gobierno que presentara un informe escrito antes del 28 de febrero de 2020 sobre las medidas que el gobierno estaba tomando para mejorar los procesos de identificación y eliminación de informes derivados de la información FISA 702 que se retiraron por razones de cumplimiento, así como sobre otros asuntos. Véase también el anexo VII.

346 Véase el anexo VII.

347 Véase la sección 4(k)(iv) de la OE nº 14086, que establece que la denuncia ante el mecanismo de recurso debe ser presentada por un denunciante que actúe en su propio nombre (es decir, no como representante de un gobierno, organización no gubernamental u organización intergubernamental). La noción de "perjudicado" no exige que el denunciante alcance un determinado umbral para tener acceso al mecanismo de recurso (véase el considerando 178 a este respecto). Más bien aclara que la CLPO y el DPRC de la ODNI tienen autoridad para remediar las violaciones de la legislación estadounidense que rige las actividades de inteligencia de señales que afecten negativamente a los intereses individuales de privacidad y libertades civiles del denunciante. Por el contrario, las violaciones

las personas procedentes de países u organizaciones regionales de integración económica que hayan sido designados por el Fiscal General de Estados Unidos como "Estados cualificados"[348]. El 30 de junio de 2023, la Unión Europea y los tres países de la Asociación Europea de Libre Comercio que juntos constituyen el Espacio Económico Europeo han sido designados por el Fiscal General, en virtud de la Sección 3(f) de la OE 14086, como "Estado calificador"[349]. Esta designación se entiende sin perjuicio del artículo 4(2) del Tratado de la Unión Europea.

(177) El interesado de la Unión que desee presentar una reclamación de este tipo debe hacerlo ante una autoridad de control de un Estado miembro de la UE competente para la supervisión del tratamiento de datos personales por parte de las autoridades públicas (una APD)[350]. Esto garantiza un fácil acceso al mecanismo de recurso, al permitir a los particulares dirigirse a una autoridad "cercana" y con la que puedan comunicarse en su propia lengua. Una vez verificados los requisitos para presentar una reclamación a que se refiere el considerando 178, la APD competente canalizará, a través de la secretaría del Consejo Europeo de Protección de Datos, la reclamación al mecanismo de recurso.

(178) La presentación de una denuncia ante el mecanismo de recurso está sujeta a requisitos de admisibilidad reducidos, ya que los particulares no necesitan demostrar que sus datos han sido objeto de hecho de actividades de inteligencia de señales de Estados Unidos[351]. Al mismo tiempo, para proporcionar un punto de partida para que el mecanismo de reparación lleve a cabo una revisión, debe proporcionarse cierta información básica, por ejemplo, sobre los datos personales que razonablemente se cree que han sido transferidos a EE.UU. y los medios por los que se cree que fueron transferidos; la identidad de las entidades del Gobierno de EE.UU. que se cree que están implicadas en la presunta violación (si se conocen); la base para alegar que se produjo una violación de la legislación estadounidense (aunque esto tampoco requiere demostrar que los datos personales fueron recogidos de hecho por agencias de inteligencia estadounidenses) y la naturaleza de la reparación solicitada.

(179) La investigación inicial de las reclamaciones ante este mecanismo de recurso corre a cargo de la CLPO del ODNI, cuya función y competencias estatutarias existentes se han ampliado para las medidas específicas adoptadas en virtud de la OE 14086[352]. Dentro de la Comunidad de Inteligencia, la CLPO es responsable, entre otras cosas, de garantizar que la protección de las libertades civiles y la privacidad se incorpore adecuadamente a las políticas y procedimientos del ODNI y de las agencias de inteligencia; de supervisar el cumplimiento por parte del ODNI de los requisitos aplicables en materia de libertades civiles y privaci-

---

de los requisitos de la legislación estadounidense aplicable que no estén concebidas para proteger a las personas (por ejemplo, requisitos presupuestarios), quedarían fuera de la jurisdicción de la ODNI CLPO y el DPRC.

348 Sección 3(f) OE 14086.

349 https://www.justice.gov/opcl/executive-order-14086.

350 Sección 4(d)(v) OE 14086.

351 Véase la sección 4(k)(i)-(iv) de la OE 14086.

352 Sección 3(c)(iv) OE 14086. Véase también la Ley de Seguridad Nacional de 1947, 50 U.S.C. §403-3d, Sección 103D relativa al papel de la CLPO dentro del ODNI.

dad; y de realizar evaluaciones de impacto sobre la privacidad[353]. El CLPO de la ODNI sólo puede ser destituido por el Director de Inteligencia Nacional por causa justificada, es decir, en caso de mala conducta, prevaricación, incumplimiento de las obligaciones o incapacidad[354].

(180) Al llevar a cabo su revisión, el CLPO del ODNI tiene acceso a la información para su evaluación y puede contar con la asistencia obligada de los responsables de privacidad y libertades civiles de las distintas agencias de inteligencia[355]. Las agencias de inteligencia tienen prohibido obstaculizar o influir indebidamente en las revisiones del CLPO de la ODNI. Esto incluye al Director de Inteligencia Nacional, que no debe interferir en la revisión[356]. Al examinar una denuncia, el CLPO del ODNI debe "aplicar la ley con imparcialidad", teniendo en cuenta tanto los intereses de la seguridad nacional en las actividades de inteligencia de señales como la protección de la intimidad[357].

(181) Como parte de su revisión, la CLPO de la ODNI determina si se ha producido una infracción de la normativa estadounidense aplicable, y si ese es el caso, decide sobre una solución adecuada[358]. Esta última se refiere a las medidas que reparan plenamente una infracción identificada, como poner fin a la adquisición ilegal de datos, suprimir los datos recogidos ilegalmente, suprimir los resultados de consultas indebidas de datos recogidos legalmente, restringir el acceso a los datos recogidos legalmente al personal debidamente formado, o retirar los informes de inteligencia que contengan datos adquiridos sin autorización legal o que se hayan difundido ilegalmente[359]. Las decisiones de la CLPO de la ODNI sobre reclamaciones individuales (incluida la reparación) son vinculantes para las agencias de inteligencia afectadas[360].

(182) La CLPO del ODNI debe conservar la documentación de su revisión y elaborar una decisión clasificada que explique la base de sus conclusiones de hecho, la determinación de si se ha producido una violación cubierta y la determinación de la solución adecuada[361]. Si la revisión de la OPC del ODNI revela una violación de cualquier autoridad sujeta a la supervisión de la FISC, la OPC también deberá proporcionar un informe clasificado al Fiscal General Adjunto para la Seguridad Nacional, quien a su vez tiene la obligación de informar del incumplimiento al FISC, que puede adoptar nuevas medidas coercitivas (de conformidad con el procedimiento descrito en los considerandos 173 a 174)[362].

(183) Una vez finalizada la revisión, la CLPO de la ODNI informa al denunciante, a través de la autoridad nacional, de que "la revisión no identificó ninguna infracción cubierta o la CLPO de la ODNI emitió una determinación que requiere una repa-

353 50 U.S.C § 3029 (b).

354 Sección 3(c)(iv) OE 14086.

355 Sección 3(c)(iii) OE 14086.

356 Sección 3(c)(iv) OE 14086.

357 Sección 3(c)(i)(B)(i) y (iii) OE 14086.

358 Sección 3(c)(i) OE 14086.

359 Sección 4(a) OE 14086.

360 Sección 3(c)(d) OE 14086.

361 Sección 3(c)(i)(F)-(G) OE 14086.

362 Véase también la sección 3(c)(i)(D) de la OE 14086.

ración adecuada"[363]. Esto permite proteger la confidencialidad de las actividades llevadas a cabo para proteger la seguridad nacional, al tiempo que proporciona a las personas una decisión que confirma que su denuncia ha sido debidamente investigada y juzgada. Además, esta decisión puede ser impugnada por el interesado. Para ello, se le informará de la posibilidad de recurrir ante el DPRC para que se revisen las decisiones del CLPO (véanse los considerandos 184 y siguientes) y de que, en caso de que se recurra al Tribunal, se seleccionará a un abogado especial para que defienda los intereses del denunciante[364].

(184) Cualquier denunciante, así como cada elemento de la Comunidad de Inteligencia, puede solicitar la revisión de la decisión del CLPO de la ODNI ante el Tribunal de Revisión de Protección de Datos (DPRC). Dichas solicitudes de revisión deberán presentarse en un plazo de 60 días a partir de la recepción de la notificación de la ODNI CLPO de que su revisión ha concluido e incluir cualquier información que el interesado desee facilitar al DPRC (por ejemplo, argumentos sobre cuestiones de derecho o la aplicación de la ley a los hechos del caso)[365]. Los interesados de la Unión podrán presentar de nuevo su solicitud a la APD competente (véase el considerando 177).

(185) El DPRC es un tribunal independiente creado por el Fiscal General sobre la base de la OE 14086[366]. Está compuesto por un mínimo de seis jueces, nombrados por el Fiscal General en consulta con la PCLOB, el Secretario de Comercio y el Director de Inteligencia Nacional por mandatos renovables de cuatro años[367]. El nombramiento de los jueces por el Fiscal General se basa en los criterios utilizados por el poder ejecutivo a la hora de evaluar a los candidatos a la judicatura federal, teniendo en cuenta la experiencia judicial previa[368]. Además, los jueces deben ser profesionales del Derecho (es decir, miembros activos en regla del colegio de abogados y debidamente autorizados para ejercer la abogacía) y tener la experiencia adecuada en derecho de la intimidad y de la seguridad nacional. El Fiscal General debe esforzarse por garantizar que al menos la mitad de los jueces en un momento dado tengan experiencia judicial previa y todos los jueces deben poseer habilitaciones de seguridad para poder acceder a información clasificada de seguridad nacional[369].

(186) Sólo pueden ser nombradas miembros del DPRC las personas que reúnan los requisitos mencionados en el considerando 185 y no sean empleados del poder

363 Sección 3(c)(i)(E)(1) OE 14086.

364 Secciones 3(c)(i)(E)(2)-(3) OE 14086.

365 Secciones 201.6(a)-(b) del Reglamento AG.

366 Sección 3(d)(i)) y el Reglamento AG. El Tribunal Supremo de los Estados Unidos ha reconocido la posibilidad de que el Fiscal General establezca órganos independientes con poder de decisión, incluso para juzgar casos individuales, véanse en particular *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954) y *United States v. Nixon*, 418 U.S. 683, 695 (1974). El cumplimiento de los distintos requisitos de la OE 14086, por ejemplo, los criterios y el procedimiento de nombramiento y destitución de los jueces del DPRC, está sujeto, en particular, a la supervisión del Inspector General del Departamento de Justicia (véase también el considerando 109 sobre la autoridad estatutaria de los Inspectores Generales).

367 Sección 3(d)(i)(A) OE 14086 y Sección 201.3(a) Reglamento AG.

368 Sección 201.3(b) del Reglamento AG.

369 Sección 3(d)(i)(B) OE 14086.

ejecutivo en el momento de su nombramiento o en los dos años anteriores. Asimismo, durante su mandato en el DPRC, los jueces no podrán tener ningún cargo o empleo oficial en el Gobierno de EE.UU. (que no sea como jueces en el DPRC)[370].

(187) La independencia del proceso de adjudicación se consigue mediante una serie de garantías. En particular, el poder ejecutivo (el Fiscal General y las agencias de inteligencia) no pueden interferir o influir indebidamente en la revisión del DPRC[371]. El propio DPRC está obligado a resolver los casos con imparcialidad[372] y funciona de acuerdo con su propio reglamento interno (adoptado por mayoría de votos). Además, los jueces del DPRC sólo pueden ser destituidos por el Fiscal General y únicamente por causa justificada (es decir, mala conducta, prevaricación, quebrantamiento de la seguridad, negligencia en el cumplimiento del deber o incapacidad), tras tener debidamente en cuenta las normas aplicables a los jueces federales establecidas en las Reglas de Conducta Judicial y Procedimientos de Incapacidad Judicial[373].

(188) Las solicitudes presentadas ante el DPRC son examinadas por grupos de tres jueces, incluido el presidente, que deben actuar de conformidad con el Código de Conducta de los Jueces de Estados Unidos[374]. Cada panel cuenta con la asistencia de un Defensor Especial[375], que tiene acceso a toda la información

370 Sección 3(d)(i)(A) OE 14086 y Sección 201.3(a) y (c) Reglamento AG. Las personas nombradas para el DPRC podrán participar en actividades extrajudiciales, incluidas las empresariales, financieras, de recaudación de fondos sin ánimo de lucro y fiduciarias, así como el ejercicio de la abogacía, siempre que dichas actividades no interfieran en el desempeño imparcial de sus funciones ni en la eficacia o independencia del DPRC (Sección 201.7(c) del Reglamento del AG).

371 Secciones 3(d)(iii)-(iv) OE 14086 y Sección 201.7(d) Reglamento AG.

372 Sección 3(d)(i)(D) EO 14086 y Sección 201.9 Reglamento AG.

373 Sección 3(d)(iv) OE 14086 y Sección 201.7(d) Reglamento AG. Véase también Bumap v. United States, 252 U.S. 512, 515 (1920), que confirmó el antiguo principio de la legislación estadounidense de que la facultad de destitución es inherente a la facultad de nombramiento (como también recordó la Oficina de Asesoría Jurídica del Departamento de Justicia en The Constitutional Separation of Powers Between the President and Congress, 20 Op. O.L.C. 124, 166 (1996)).

374 Sección 3(d)(i)(B) de la OE 14086 y Sección 201.7(a)-(c) del Reglamento del GC. La Oficina de Privacidad y Libertades Civiles del Departamento de Justicia (OPCL), que es responsable de proporcionar apoyo administrativo al DPRC y a los Defensores Especiales (véase la Sección 201.5 del Reglamento AG), selecciona un panel de tres personas de forma rotatoria, tratando de garantizar que cada panel tenga al menos un juez con experiencia judicial previa (si ninguno de los jueces del panel tiene dicha experiencia, el juez presidente será el juez seleccionado en primer lugar por la OPCL).

375 Sección 201.4 Reglamento del Fiscal General. Al menos dos Defensores Especiales son nombrados por el Fiscal General, en consulta con el Secretario de Comercio, el Director de Inteligencia Nacional y la PCLOB, por períodos de dos años renovables. Los Defensores Especiales deben tener la experiencia adecuada en el ámbito de la legislación sobre privacidad y seguridad nacional, ser abogados experimentados, estar colegiados en activo y debidamente autorizados para ejercer la abogacía. Además, en el momento de su nombramiento inicial, no deben haber sido empleados del Poder Ejecutivo durante los dos años anteriores. Para cada revisión de una solicitud, el juez que preside selecciona a un Defensor Especial para asistir al panel, véase la Sección 201.8(a) del Reglamento AG.

relativa al caso, incluida la información clasificada[376]. La función del Defensor Especial es garantizar que los intereses del demandante estén representados y que el panel del DPRC esté bien informado sobre todas las cuestiones de hecho y de derecho pertinentes[377]. Para fundamentar mejor su posición sobre una solicitud de revisión ante el DPRC presentada por un particular, el Defensor Especial puede recabar información del denunciante mediante preguntas escritas[378].

(189) El DPRC revisa las decisiones tomadas por la CLPO de la ODNI (tanto si se ha producido una violación de la legislación estadounidense aplicable como en lo que respecta a las medidas correctivas apropiadas) basándose, como mínimo, en el expediente de la investigación de la CLPO de la ODNI, así como en cualquier información y presentación facilitada por el denunciante, el Defensor Especial o una agencia de inteligencia[379]. El panel del DPRC tiene acceso a toda la información necesaria para llevar a cabo la revisión, que puede obtener a través de la CLPO de la ODNI. Un panel del DPRC tiene acceso a toda la información necesaria para llevar a cabo una revisión, que puede obtener a través de la CLPO de la ODNI (el panel puede, por ejemplo, solicitar a la CLPO que complemente su expediente con información adicional o conclusiones fácticas si es necesario para llevar a cabo la revisión)[380].

(190) Al concluir su revisión, el DPRC podrá (1) decidir que no existen pruebas que indiquen que se hayan producido actividades de inteligencia de señales en relación con los datos personales del denunciante, (2) decidir que las determinaciones del CLPO de la ODNI eran jurídicamente correctas y estaban respaldadas por pruebas sustanciales, o (3) si el DPRC no está de acuerdo con las determinaciones del CLPO de la ODNI (si se ha producido una violación de la legislación estadounidense aplicable o la solución adecuada), emitir sus propias determinaciones[381].

(191) En todos los casos, el DPRC adopta una decisión por escrito por mayoría de votos. En caso de que el examen revele una violación de las normas aplicables, la decisión especificará las medidas correctoras adecuadas, entre las que se inclu-

376 Sección 201.8(c) y 201.11 del Reglamento AG.

377 Sección 3(d)(i)(C) EO 14086 y Sección 201.8(e) Reglamento AG. El Defensor Especial no actúa como agente ni tiene una relación de abogado-cliente con el denunciante.

378 Véase la sección 201.8(d)(e) del Reglamento AG. Tales preguntas son revisadas en primer lugar por la OPCL, en consulta con el elemento pertinente de la Comunidad de Inteligencia, con vistas a identificar y excluir cualquier información clasificada o privilegiada o protegida antes de remitirla al denunciante. La información adicional recibida por el Defensor Especial en respuesta a dichas preguntas se incluye en las presentaciones del Defensor Especial al DPRC.

379 Sección 3(d)(i)(D) OE 14086.

380 Sección 3(d)(iii) OE 14086 y Sección 201.9(b) Reglamento AG.

381 Sección 3(d)(i)(E) de la OE 14086 y sección 201.9(c)-(e) del Reglamento del GC. De acuerdo con la definición de "reparación adecuada" que figura en el artículo 4(a) de la OE 14086, el DPRC debe tener en cuenta "la forma en que se ha abordado habitualmente una infracción del tipo identificado" a la hora de decidir una medida de reparación para abordar plenamente una infracción, es decir, el DPRC tendrá en cuenta, entre otros factores, cómo se remediaron en el pasado problemas de cumplimiento similares para garantizar que la reparación sea eficaz y adecuada.

yen la supresión de los datos recopilados ilegalmente, la supresión de los resultados de las consultas realizadas de forma inadecuada, la restricción del acceso a los datos recopilados legalmente al personal debidamente formado, o la retirada de los informes de inteligencia que contengan datos adquiridos sin autorización legal o que se hayan difundido ilegalmente[382]. La decisión del DPRC es vinculante y definitiva con respecto a la denuncia que se le haya presentado[383]. Además, si la revisión revela una violación de cualquier autoridad sujeta a la supervisión del FISC, el DPRC también debe proporcionar un informe clasificado al Fiscal General Adjunto para la Seguridad Nacional, que a su vez tiene la obligación de informar del incumplimiento al FISC, que puede adoptar nuevas medidas coercitivas (de conformidad con el procedimiento descrito en los considerandos 173 a 174)[384].

(192) Cada decisión de un panel del DPRC se transmite a la CLPO de la ODNI[385]. En los casos en que la revisión del DPRC se inició por una solicitud del denunciante, se notifica al denunciante a través de la autoridad nacional que el DPRC completó su revisión y que "la revisión no identificó ninguna violación cubierta o el DPRC emitió una determinación que requería una remediación apropiada"[386]. La Oficina de Privacidad y Libertades Civiles del DoJ mantiene un registro de toda la información revisada por el DPRC y de todas las decisiones emitidas, que se pone a disposición para su consideración como precedente no vinculante para futuros paneles del DPRC[387].

(193) El DoC también está obligado a mantener un registro de cada denunciante que haya presentado una denuncia[388]. Para aumentar la transparencia, el DoC debe, al menos cada cinco años, ponerse en contacto con las agencias de inteligencia pertinentes para verificar si la información relativa a una revisión del DPRC ha sido desclasificada[389]. En caso afirmativo, se notificará a la persona que dicha información puede estar disponible en virtud de la legislación aplicable (es decir, a la que puede solicitar acceso en virtud de la Ley de Libertad de Información, véase el considerando 199).

(194) Por último, el correcto funcionamiento de este mecanismo de recurso será objeto de una evaluación periódica e independiente. Más concretamente, de conformidad con la OE nº 14086, el funcionamiento del mecanismo de recurso

382 Sección 4(a) OE 14086.

383 Sección 3(d)(ii) OE 14086 y Sección 201.9(g) Reglamento AG. Dado que la decisión del DPRC es definitiva y vinculante, ninguna otra institución u organismo ejecutivo o administrativo (incluido el Presidente de los Estados Unidos) puede anular la decisión del DPRC. Así lo ha confirmado también la jurisprudencia del Tribunal Supremo, que ha aclarado que, al delegar en un órgano independiente la autoridad única del Fiscal General dentro del Poder Ejecutivo para emitir decisiones vinculantes, el Fiscal General se niega a sí mismo la capacidad de dictar la decisión de dicho órgano en modo alguno (véase *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954).

384 Sección 3(d)(i)(F) OE 14086 y Sección 201.9(i) Reglamento AG.

385 Sección 201.9(h) del Reglamento AG.

386 Sección 3(d)(i)(H) OE 14086 y Sección 201.9(h) Reglamento AG. Por lo que respecta a la naturaleza de la notificación, véase la sección 2 0 1 . 9 (h)(3) del Reglamento AG.

387 Sección 201.9(j) del Reglamento Ag.

388 Sección 3(d)(v)(A) OE 14086.

389 Sección 3(d)(v) OE 14086.

está sujeto a una revisión anual por parte del PCLOB, un órgano independiente (véase el considerando 110)[390]. Como parte de esta revisión, el PCLOB evaluará, entre otras cosas, si el ODNI CLPO y el DPRC han tramitado las reclamaciones a su debido tiempo; si han obtenido pleno acceso a la información necesaria; si las salvaguardias sustantivas de la OE 14086 se han tenido debidamente en cuenta en el proceso de revisión; y si la Comunidad de Inteligencia ha cumplido plenamente las determinaciones adoptadas por el ODNI CLPO y el DPRC. El PCLOB elaborará un informe sobre el resultado de su revisión para el Presidente, el Fiscal General, el Director de Inteligencia Nacional, los jefes de las agencias de inteligencia, el ODNI CLPO y los comités de inteligencia del Congreso, que también se hará público en una versión no clasificada - y que a su vez alimentará la revisión periódica del funcionamiento de la presente Decisión que llevará a cabo la Comisión. El Fiscal General, el Director de Inteligencia Nacional, el CLPO de la ODNI y los jefes de las agencias de inteligencia están obligados a aplicar o a abordar de otro modo todas las recomendaciones incluidas en dichos informes. Además, el PCLOB realizará una certificación pública anual sobre si el mecanismo de reparación está tramitando las denuncias de conformidad con los requisitos de la OE 14086.

(195) Además del mecanismo de recurso específico establecido en la OE 14086, todas las personas (independientemente de su nacionalidad o lugar de residencia) disponen de vías de recurso ante los tribunales ordinarios estadounidenses[391].

(196) En concreto, la FISA y una ley conexa ofrecen a los particulares la posibilidad de interponer una demanda civil por daños y perjuicios contra Estados Unidos cuando se haya utilizado o revelado información sobre ellos de forma ilícita y deliberada[392]; demandar a funcionarios del Gobierno estadounidense actuando a título personal por daños y perjuicios monetarios[393]; y para impugnar la legalidad de la vigilancia (y solicitar la supresión de la información) en caso de que el Gobierno de EE.UU. pretenda utilizar o revelar cualquier información obtenida o derivada de la vigilancia electrónica contra el individuo en procedimientos judiciales o administrativos en EE.UU.[394]. En términos más generales, si el Gobierno pretende utilizar información obtenida durante operaciones de inteligencia contra un sospechoso en un caso penal, los requisitos constitucionales y legales[395]

---

390 Sección 3(e) OE 14086. Véase también https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e- 2687b14ed9b9/Trans- Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

391 El acceso a estas vías está sujeto a la demostración de "legitimación". Esta norma, que se aplica a cualquier persona con independencia de su nacionalidad, se deriva del requisito de "caso o controversia" del artículo III de la Constitución estadounidense. Según el Tribunal Supremo, esto requiere que (1) el individuo haya sufrido un "perjuicio de hecho" (es decir, un perjuicio de un interés jurídicamente protegido que sea concreto y particularizado y real o inminente), (2) exista una conexión causal entre el perjuicio y la conducta impugnada ante el tribunal, y (3) sea probable, y no especulativo, que una decisión favorable del tribunal resuelva el perjuicio (véase Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).

392 18 U.S.C. § 2712.

393 50 U.S.C. § 1810.

394 50 U.S.C. § 1806.

395 Véase, respectivamente, Brady contra Maryland, 373 U.S. 83 (1963) y la Ley Jencks, 18

imponen la obligación de revelar determinada información para que el acusado pueda impugnar la legalidad de la obtención y utilización de las pruebas por parte del Gobierno.

(197) Además, existen varias vías específicas para interponer recursos legales contra funcionarios públicos por el acceso o uso ilícitos de datos personales por parte del Gobierno, incluso con fines supuestamente de seguridad nacional (por ejemplo, la Ley de Fraude y Abuso Informático[396]; la Ley de Privacidad de las Comunicaciones Electrónicas[397]; y la Ley de Derecho a la Privacidad Financiera[398]). Todas estas acciones legales se refieren a datos específicos, objetivos y/o tipos de acceso (por ejemplo, acceso remoto a un ordenador a través de Internet) y están disponibles bajo ciertas condiciones (por ejemplo, conducta intencionada/voluntaria, conducta fuera de la capacidad oficial, daño sufrido).

(198) Una posibilidad de reparación más general la ofrece la APA[399], según la cual "cualquier persona que sufra un agravio legal debido a la actuación de un organismo, o que se vea perjudicada o agraviada por la actuación de un organismo", tiene derecho a solicitar una revisión judicial[400]. Ello incluye la posibilidad de solicitar al tribunal que "declare ilegales y anule la actuación, los resultados y las conclusiones del organismo que se consideren [...] arbitrarios, caprichosos, constitutivos de un abuso de poder discrecional o no conformes a derecho"[401]. Por ejemplo, un tribunal federal de apelación dictaminó en 2015 sobre una demanda APA que la recopilación masiva de metadatos de telefonía por parte del gobierno de Estados Unidos no estaba autorizada por la Sección 501 FISA[402].

(199) Por último, además de las vías de recurso mencionadas en los considerandos 176 a 198, toda persona tiene derecho a solicitar el acceso a los registros existentes de los organismos federales en virtud de la FOIA, incluso cuando éstos contengan datos personales de la persona[403]. Obtener dicho acceso también puede facilitar la interposición de recursos ante los tribunales ordinarios, incluso para demostrar la legitimación. Los organismos pueden retener información que entre dentro de ciertas excepciones enumeradas, incluido el acceso a información clasificada de seguridad nacional y a información relativa a investigaciones policiales[404], pero los denunciantes que no están satisfechos con la respuesta

---

U.S.C. § 3500.

396 18 U.S.C. § 1030.

397 18 U.S.C. §§ 2701-2712.

398 12 U.S.C. § 3417.

399 5 U.S.C. § 702.

400 En general, sólo la acción "final" de un organismo -en lugar de la acción "preliminar, procesal o intermedia"- está sujeta a revisión judicial. Véase 5 U.S.C. § 704.

401 5 U.S.C. § 706(2)(A).

402 ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015), El programa de recolección de telefonía masiva impugnado en estos casos fue terminado por la Ley USA FREEDOM en 2015.

403 5 U.S.C. § 552. Existen leyes similares a nivel estatal.

404 Si este es el caso, la persona normalmente solo recibirá una respuesta estándar por la que la agencia se niega a confirmar o negar la existencia de cualquier registro. Véase ACLU c. CIA, 710 F.3d 422 (D.C. Cir. 2014). Los criterios y la duración de la clasificación se establecen en la Orden Ejecutiva 13526, que dispone, como norma general, que debe establecerse una fecha o un evento específico para la desclasificación en función de la

tienen la posibilidad de impugnarla solicitando una revisión administrativa y, posteriormente, judicial (ante los tribunales federales)[405].

(200) De lo anterior se desprende que cuando las autoridades policiales y de seguridad nacional de Estados Unidos acceden a datos personales que entran en el ámbito de aplicación de la presente Decisión, dicho acceso se rige por un marco jurídico que establece las condiciones en las que puede tener lugar el acceso y garantiza que el acceso y el uso posterior de los datos se limitan a lo necesario y proporcionado al objetivo de interés público perseguido. Estas salvaguardias pueden ser invocadas por particulares que disfruten de derechos efectivos de recurso.

4. CONCLUSIÓN

(201) La Comisión considera que los Estados Unidos -a través de los Principios publicados por el DoC estadounidense- garantizan un nivel de protección de los datos personales transferidos desde la Unión a organizaciones certificadas en los Estados Unidos en virtud del Marco de Privacidad de Datos UE-EE.UU. que es esencialmente equivalente al garantizado por el Reglamento (UE) 2016/679.

(202) Por otra parte, la Comisión considera que la aplicación efectiva de los Principios está garantizada por las obligaciones de transparencia y la administración del DPF por el DoC. Además, en su conjunto, los mecanismos de supervisión y las vías de recurso de la legislación estadounidense permiten identificar y sancionar en la práctica las infracciones de las normas de protección de datos y ofrecen recursos jurídicos al interesado para obtener el acceso a los datos personales que le conciernen y, en su caso, la rectificación o supresión de dichos datos.

(203) Por último, sobre la base de la información disponible sobre el ordenamiento jurídico de los Estados Unidos, incluida la información contenida en los anexos VI y VII, la Comisión considera que cualquier injerencia de interés público, en particular con fines de aplicación de la ley penal y de seguridad nacional, por parte de las autoridades públicas de los Estados Unidos en los derechos fundamentales de las personas cuyos datos personales se transfieren de la Unión a los Estados Unidos en virtud del Marco de Privacidad de Datos UE-EE.UU., se limitará a lo estrictamente necesario para alcanzar el objetivo legítimo en cuestión, y que existe una protección jurídica efectiva contra dicha injerencia. Por consiguiente, a la luz de las constataciones anteriores, debe decidirse que los Estados Unidos garantizan un nivel de protección adecuado en el sentido del artículo 45 del Reglamento (UE) 2016/679, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, para los datos personales transferidos desde la Unión Europea a organizaciones certificadas con arreglo al Marco de Privacidad de Datos UE-EE.UU.

(204) Dado que las limitaciones, las salvaguardias y el mecanismo de recurso establecidos por la OE 14086 son elementos esenciales del marco jurídico esta-

duración de la sensibilidad de la información para la seguridad nacional, momento en el que la información debe desclasificarse automáticamente (véase la sección 1.5 de la OE 13526).

405 El tribunal determina de novo si los registros están legalmente retenidos y puede obligar al gobierno a proporcionar acceso a los registros (5 U.S.C. § 552(a)(4)(B)).

dounidense en los que se basa la evaluación de la Comisión, la adopción de la presente Decisión se basa especialmente en la adopción de políticas y procedimientos actualizados para aplicar la OE 14086 por parte de todas las agencias de inteligencia estadounidenses y en la designación de la Unión como organización habilitada a efectos del mecanismo de recurso que han tenido lugar, respectivamente, el 3 de julio de 2023 (véase el considerando 126) y el 30 de junio de 2023 (véase el considerando 176).

5. EFECTOS DE ESTA DECISIÓN Y ACTUACIÓN DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

(205) Los Estados miembros y sus órganos están obligados a adoptar las medidas necesarias para dar cumplimiento a los actos de las instituciones de la Unión, ya que éstos se presumen legales y, por tanto, producen efectos jurídicos mientras no sean retirados, anulados en un recurso de anulación o declarados nulos a raíz de una cuestión prejudicial o de una excepción de ilegalidad.

(206) En consecuencia, una decisión de adecuación de la Comisión adoptada de conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679 es vinculante para todos los órganos de los Estados miembros a los que se dirige, incluidas sus autoridades de control independientes. En particular, las transferencias de un responsable o encargado del tratamiento en la Unión a organizaciones certificadas en los Estados Unidos pueden tener lugar sin necesidad de obtener ninguna otra autorización.

(207) Debe recordarse que, de conformidad con el artículo 58, apartado 5, del Reglamento (UE) 2016/679 y como explicó el Tribunal de Justicia en la sentencia *Schrems*[406], cuando una autoridad nacional de protección de datos cuestione, incluso mediante una denuncia, la compatibilidad de una decisión de adecuación de la Comisión con los derechos fundamentales de la persona a la intimidad y a la protección de datos, el Derecho nacional debe proporcionarle un recurso legal para plantear esas objeciones ante un órgano jurisdiccional nacional, que puede verse obligado a plantear una cuestión prejudicial al Tribunal de Justicia[407].

6. SEGUIMIENTO Y REVISIÓN DE ESTA DECISIÓN

(208) Según la jurisprudencia del Tribunal de Justicia[408], y tal como se reconoce en el artículo 45, apartado 4, del Reglamento (UE) 2016/679, la Comisión debe supervisar continuamente la evolución pertinente en el tercer país tras la adopción de una decisión de adecuación con el fin de evaluar si el tercer país sigue garantizando un

406 *Schrems*, apartado 65.

407 *Schrems*, apartado 65: "Incumbe al legislador nacional prever vías de recurso que permitan a la autoridad nacional de control de que se trate formular las objeciones que considere fundadas ante los órganos jurisdiccionales nacionales para que éstos, si comparten sus dudas sobre la validez de la decisión de la Comisión, planteen una cuestión prejudicial a efectos del examen de la validez de la decisión."

408 *Schrems*, apartado 76.

nivel de protección esencialmente equivalente. Dicha comprobación es necesaria, en cualquier caso, cuando la Comisión reciba información que suscite una duda justificada al respecto.

(209) Por lo tanto, la Comisión debe supervisar de forma continua la situación en Estados Unidos en lo que respecta al marco jurídico y la práctica real del tratamiento de datos personales evaluados en la presente Decisión. Para facilitar este proceso, las autoridades de Estados Unidos deben informar sin demora a la Comisión de la evolución material del ordenamiento jurídico estadounidense que tengan incidencia en el marco jurídico objeto de la presente Decisión, así como cualquier evolución en las prácticas relacionadas con el tratamiento de los datos personales evaluados en la presente Decisión, tanto en lo que se refiere al tratamiento de datos personales por parte de organizaciones certificadas en Estados Unidos como a las limitaciones y garantías aplicables al acceso a los datos personales por parte de las autoridades públicas.

(210) Por otra parte, para que la Comisión pueda desempeñar eficazmente su función de control, los Estados miembros deben informar a la Comisión de cualquier acción pertinente emprendida por las autoridades nacionales de protección de datos, en particular en relación con las consultas o denuncias de los interesados de la Unión sobre la transferencia de datos personales de la Unión a organizaciones certificadas de Estados Unidos. También deberá informarse a la Comisión de cualquier indicio de que la actuación de las autoridades públicas estadounidenses responsables de la prevención, investigación, detección o enjuiciamiento de infracciones penales, o de seguridad nacional, incluidos los organismos de supervisión, no garantizan el nivel de protección requerido.

(211) En aplicación del artículo 45, apartado 3, del Reglamento (UE) 2016/679[409], la Comisión, tras la adopción de la presente Decisión, debe revisar periódicamente si las conclusiones relativas a la adecuación del nivel de protección garantizado por los Estados Unidos en el marco del FPD UE-EE.UU. siguen estando justificadas desde el punto de vista fáctico y jurídico. Dado que, en particular, la OE 14086 y el Reglamento AG exigen la creación de nuevos mecanismos y la aplicación de nuevas salvaguardias, la presente Decisión debe someterse a una primera revisión en el plazo de un año tras su entrada en vigor, para comprobar si todos los elementos pertinentes se han aplicado plenamente y funcionan eficazmente en la práctica. Tras esa primera revisión, y en función de su resultado, la Comisión decidirá, en estrecha consulta con el Comité establecido en virtud del artículo 93, apartado 1, del Reglamento (UE) 2016/679 y el Consejo Europeo de Protección de Datos, la periodicidad de las futuras revisiones[410].

(212) Para llevar a cabo las revisiones, la Comisión debería reunirse con el DoC, la FTC y el DoT acompañados, si procede, por otros departamentos y organismos implicados en la aplicación del DPF UE-EE.UU., así como, para los asuntos relativos al acceso gubernamental a los datos, por representantes del DoJ, el ODNI (incluida la CLPO), otros elementos de la Comunidad de Inteligencia, el DPRC, así como los Defensores Especiales. La participación en esta reunión debería estar abierta a los representantes de los miembros del Consejo Europeo de Protección de Datos.

---

409 De conformidad con el artículo 45, apartado 3, del Reglamento (UE) 2016/679, "[e]l acto de ejecución establecerá un mecanismo de revisión periódica, [...] que tendrá en cuenta todos los acontecimientos pertinentes en el tercer país u organización internacional."

410 El artículo 45, apartado 3, del Reglamento (UE) 2016/679 establece que debe realizarse una revisión periódica "al menos cada cuatro años". Véase también Consejo Europeo de Protección de Datos, Adequacy Referential, WP 254 rev. 01.

(213) Las revisiones deben abarcar todos los aspectos del funcionamiento de la presente Decisión con respecto al tratamiento de datos personales en Estados Unidos, y en particular la aplicación y ejecución de los Principios, prestando especial atención a las protecciones ofrecidas en caso de transferencias ulteriores; la evolución de la jurisprudencia pertinente; la eficacia del ejercicio de los derechos individuales; el control y la ejecución del cumplimiento de los Principios; así como las limitaciones y salvaguardias con respecto al acceso gubernamental, en particular la implantación y aplicación de las salvaguardias introducidas por la OE 14086, incluso mediante políticas y procedimientos elaborados por los organismos de inteligencia; la interacción entre la OE 14086 y la Sección 702 de la FISA y la OE 12333; y la eficacia de los mecanismos de supervisión y las vías de recurso (incluido el funcionamiento del nuevo mecanismo de recurso establecido en virtud de la OE 14086). En el contexto de dichas revisiones, también se prestará atención a la cooperación entre las APD y las autoridades competentes de los Estados Unidos, incluida la elaboración de orientaciones y otros instrumentos interpretativos sobre la aplicación de los Principios, así como sobre otros aspectos del funcionamiento del Marco.

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

7. SUSPENSIÓN, DEROGACIÓN O MODIFICACIÓN DE LA PRESENTE DECISIÓN

(215) Cuando la información disponible, en particular la resultante de la supervisión de la presente Decisión o la facilitada por las autoridades de los EE.UU. o de los Estados miembros, revele que el nivel de protección concedido a los datos transferidos en virtud de la presente Decisión ya no puede ser adecuada, la Comisión debe informar de ello sin demora a las autoridades estadounidenses competentes y solicitar que se adopten las medidas apropiadas en un plazo determinado y razonable.

(216) Si, transcurrido ese plazo especificado, las autoridades competentes de los Estados Unidos no adoptan esas medidas o no demuestran de otro modo satisfactoriamente que la presente Decisión sigue basándose en un nivel de protección adecuado, la Comisión iniciará el procedimiento contemplado en el artículo 93, apartado 2, del Reglamento (UE) 2016/679 con vistas a suspender parcial o totalmente o derogar la presente Decisión.

(217) Alternativamente, la Comisión iniciará dicho procedimiento con vistas a modificar la Decisión, en particular sometiendo las transferencias de datos a condiciones adicionales o limitando el alcance de la conclusión de adecuación únicamente a las transferencias de datos para las que siga garantizándose un nivel de protección adecuado.

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

(a) indicios de que las organizaciones que han recibido datos personales de la Unión en virtud de la presente Decisión no cumplen los Principios y de que dicho incumplimiento no es abordado eficazmente por los organismos competentes de supervisión y ejecución;

(b) indicios de que las autoridades estadounidenses no cumplen las condiciones y limitaciones aplicables al acceso de las autoridades públicas estadounidenses con fines policiales y de seguridad nacional a los datos personales transferidos en virtud del DPF UE-EE.UU.; o

(c) no atender eficazmente las reclamaciones de los interesados de la Unión, incluso por parte del CLPO de la ODNI y/o el DPRC.

(219) La Comisión también debe considerar la posibilidad de iniciar el procedimiento conducente a la modificación, suspensión o derogación de la presente Decisión si las autoridades competentes de los Estados Unidos no facilitan la información o las aclaraciones necesarias para evaluar el nivel de protección de los datos personales transferidos de la Unión a los Estados Unidos, o en lo que respecta al cumplimiento de la presente Decisión. A este respecto, la Comisión debe tener en cuenta en qué medida la información pertinente puede obtenerse de otras fuentes.

(220) Por razones imperiosas de urgencia debidamente justificadas, por ejemplo, si la OE 14086 o el Reglamento AG se modificaran de manera que socavaran el nivel de protección descrito en la presente Decisión o si se retirara la designación por el Fiscal General de la Unión como organización habilitada a efectos del mecanismo de recurso, la Comisión hará uso de la posibilidad de adoptar, de conformidad con el procedimiento contemplado en el artículo 93, apartado 3, del Reglamento (UE) 2016/679, actos de ejecución inmediatamente aplicables por los que se suspenda, derogue o modifique la presente Decisión.

8. CONSIDERACIONES FINALES

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

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

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

HA ADOPTADO ESTA DECISIÓN:

Artículo 1

A efectos del artículo 45 del Reglamento (UE) 2016/679, los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a organizaciones de los Estados Unidos que estén incluidas en la "Data Privacy Framework List", mantenida y puesta a disposición del público por el Departamento de Comercio de los Estados Unidos, de conformidad con la sección I.3 del anexo I.

Artículo 2

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

411 Dictamen 5/2023 sobre el proyecto de Decisión de Ejecución de la Comisión Europea relativa al carácter adecuado de la protección de los datos personales en el marco de la protección de datos entre la UE y los EE.UU., de 28 de febrero de 2023.

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

Artículo 3

1. La Comisión supervisará continuamente la aplicación del marco jurídico objeto de la presente Decisión, incluidas las condiciones en que se llevan a cabo las transferencias ulteriores, se ejercen los derechos individuales y las autoridades públicas de los Estados Unidos tienen acceso a los datos transferidos en virtud de la presente Decisión, con el fin de evaluar si los Estados Unidos siguen garantizando un nivel de protección adecuado según lo dispuesto en el artículo 1.
2. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que se ponga de manifiesto que los organismos de los Estados Unidos con competencias legales para hacer cumplir los Principios establecidos en el Anexo I no proporcionan mecanismos eficaces de detección y supervisión que permitan identificar y sancionar en la práctica las infracciones de los Principios establecidos en el Anexo I.
3. Los Estados miembros y la Comisión se informarán mutuamente de cualquier indicio de que las injerencias de las autoridades públicas estadounidenses responsables de la persecución de la seguridad nacional, la aplicación de la ley u otros intereses públicos en el derecho de las personas a la protección de sus datos personales van más allá de lo necesario y proporcionado, y/o de que no existe una protección jurídica eficaz contra dichas injerencias.
4. Transcurrido un año desde la fecha de notificación de la presente Decisión a los Estados miembros y, posteriormente, con una periodicidad que se decidirá en estrecha consulta con el Comité creado en virtud del artículo 93, apartado 1, del Reglamento (UE) 2016/679 y el Consejo Europeo de Protección de Datos, la Comisión evaluará la constatación a que se refiere el artículo 1, apartado 1, sobre la base de toda la información disponible, incluida la información obtenida a través de la revisión llevada a cabo junto con las autoridades competentes de Estados Unidos .
5. Cuando la Comisión tenga indicios de que ya no se garantiza un nivel de protección adecuado, informará a las autoridades competentes de los Estados Unidos. En caso necesario, decidirá suspender, modificar o derogar la presente Decisión, o limitar su ámbito de aplicación, de conformidad con el artículo 45, apartado 5, del Reglamento (UE) 2016/679. La Comisión también podrá adoptar una decisión de este tipo si la falta de cooperación del Gobierno estadounidense impide a la Comisión determinar si los Estados Unidos siguen garantizando un nivel de protección adecuado.

Artículo 4

Los destinatarios de la presente Decisión serán los Estados miembros. Hecho en Bruselas, el 10.7.2023

Por la Comisión Didier REYNDERS
Miembro de la Comisión

CERTIFIES COPY For the Secretary-General
Martine DEPREZ
Director
Decision-making & Collegiality
EUROPEAN COMISSION

NOTA PARA EL LECTOR: todos los anexos que se reproducirán a partir de aquí forman parte de la precitada Decisión del 10 de julio de 2023.



Bruselas, 10.7.2023
C(2023) 4745 final
ANEXOS 1 a 7

ANEXOS

a la

DECISIÓN DE APLICACIÓN DE LA COMISIÓN

de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre la UE y los EE.UU.

ANEXO I

PRINCIPIOS MARCO DE PRIVACIDAD DE DATOS UE-EE.UU. PUBLICADOS POR EL DEPARTAMENTO DE COMERCIO DE LOS EE.UU.

I. Visión general

1. Aunque Estados Unidos y la Unión Europea (la "UE") comparten el compromiso de mejorar la protección de la intimidad, el Estado de Derecho y el reconocimiento de la importancia de los flujos transatlánticos de datos para nuestros respectivos ciudadanos, economías y sociedades, Estados Unidos adopta un planteamiento de la protección de la intimidad distinto del de la UE. Estados Unidos utiliza un enfoque sectorial que se basa en una combinación de legislación, regulación y autorregulación. El Departamento de Comercio de EE.UU. ("el Departamento") publica los Principios Marco de Protección de Datos UE-EE.UU., incluidos los Principios Complementarios (denominados colectivamente "los Principios") y el Anexo I de los Principios ("Anexo I"), en virtud de su autoridad legal para fomentar, promover y desarrollar el comercio internacional (15 U.S.C. § 1512). Los Principios se elaboraron en consulta con la Comisión Europea ("la Comisión"), la industria y otras partes interesadas para facilitar el comercio entre Estados Unidos y la UE. Los Principios, un componente clave del Acuerdo UE-EE. U.S. Data Privacy Framework ("EU-U.S. DPF"), proporcionan a las organizaciones de Estados Unidos un mecanismo fiable para las transferencias de datos personales a Estados Unidos desde la UE, garantizando al mismo tiempo que los interesados de la UE sigan beneficiándose de las salvaguardias y la protección efectivas exigidas por la legislación europea con respecto al tratamiento de sus datos personales cuando hayan sido transferidos a países no pertenecientes a la UE. Los Principios están destinados a ser utilizados exclusivamente por las organizaciones elegibles de Estados Unidos que reciban datos personales de la UE con el fin de acogerse al DPF UE-EE.UU. y beneficiarse así de la decisión de adecuación de la Comisión[1]. Los Principios no afectan a la aplicación del Regla-

1 Siempre que la Decisión de la Comisión sobre la adecuación de la protección proporcionada por el DPF UE- EE.UU. se aplique a Islandia, Liechtenstein y Noruega, el DPF UE-EE. UU. cubrirá tanto a la UE como a estos tres países. Por consiguiente, las referencias a la UE y sus Estados miembros se entenderán como inclusivas de Islandia, Liechtenstein y Noruega.

mento (UE) 2016/679 ("Reglamento general de protección de datos" o "RGPD")[2] que se aplica al tratamiento de datos personales en los Estados miembros de la UE. Los Principios tampoco limitan las obligaciones de privacidad que de otro modo se aplicarían en virtud de la legislación estadounidense.

2. Para poder acogerse al DPF UE-EE.UU. para efectuar transferencias de datos personales desde la UE, una organización debe autocertificar su adhesión a los Principios ante el Departamento (o su representante). Si bien la decisión de las organizaciones de entrar así en el DPF UE-EE.UU. es totalmente voluntaria, su cumplimiento efectivo es obligatorio: las organizaciones que autocertifiquen al Departamento y declaren públicamente su compromiso de adherirse a los Principios deben cumplirlos plenamente. Para entrar en el DPF UE-EE.UU., una organización debe (a) estar sujeta a los poderes de investigación y ejecución de la Comisión Federal de Comercio (la "FTC"), el Departamento de Transporte de EE.UU. (el "DOT") u otro organismo estatutario que garantice efectivamente el cumplimiento de los Principios *(en el futuro podrán incluirse como anexo otros organismos estatutarios estadounidenses reconocidos por la UE)*; (b) declare públicamente su compromiso de cumplir con los Principios; (c) divulgue públicamente sus políticas de privacidad en línea con estos Principios; y (d) aplique plenamente[3]. El incumplimiento por parte de una organización puede ser ejecutado por la FTC en virtud del artículo 5 de la Ley de la Comisión Federal de Comercio (FTC), que prohíbe los actos desleales o engañosos en el comercio o que afecten a éste (15 U.S.C. § 45); por el Departamento de Transporte en virtud del artículo 49 del Tratado de la Unión Europea, que prohíbe los actos desleales o engañosos en el comercio o que afecten a éste. U.S.C. § 41712 que prohíbe a un transportista o agente de venta de billetes realizar prácticas desleales o engañosas en el transporte aéreo o en la venta de transporte aéreo; o en virtud de otras leyes o reglamentos que prohíben tales actos.

3. El Departamento mantendrá y pondrá a disposición del público una lista autorizada de organizaciones estadounidenses que se han autocertificado ante el Departamento y han declarado su compromiso de adherirse a los Principios ("la Lista del Marco de Privacidad de Datos"). Los beneficios del DPF de EE.UU. están garantizados a partir de la fecha en que el Departamento incluya a la organización en la Lista del Marco de Privacidad de Datos. El Departamento retirará de la Lista del Marco de Privacidad de Datos a las organizaciones que se retiren voluntariamente del DPF UE-EE.UU. o que no completen su recertificación anual ante el Departamento; estas organizaciones deben seguir aplicando los Principios a la información personal que recibieron en virtud del DPF UE-EE. UU. y afirmar anualmente ante el Departamento su compromiso de hacerlo (es decir, mientras conserven dicha información), proporcionar una protección "adecuada" de la información por otro medio autorizado (por ejemplo, utilizando un contrato que refleje plenamente los requisitos de las cláusulas contractuales tipo pertinentes adoptadas por la Comisión), o devolver o eliminar la información. El Departamento también eliminará de la Lista del Marco de Privacidad de Datos a aquellas organizaciones que hayan incumplido de forma persistente los Princi-

2 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por la que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

3 Los Principios Marco del Escudo de Privacidad UE-EE.UU. han sido modificados como "Principios Marco de Privacidad de Datos UE-EE.UU.". (*Véase* el Principio Suplementario sobre Autocertificación).

pios; estas organizaciones deberán devolver o eliminar la información personal que recibieron en virtud del DPF UE-EE.UU.. La eliminación de una organización de la Lista del Marco de Privacidad de Datos significa que ya no tiene derecho a beneficiarse de la decisión de adecuación de la Comisión para recibir información personal de la UE.

4. El Departamento también mantendrá y pondrá a disposición del público un registro fidedigno de las organizaciones estadounidenses que anteriormente se habían autocertificado ante el Departamento, pero que han sido eliminadas de la Lista del Marco de Privacidad de Datos. El Departamento advertirá claramente de que estas organizaciones no son participantes en el DPF UE-EE.UU.; de que la eliminación de la Lista del Marco de Privacidad de Datos significa que dichas organizaciones no pueden afirmar que cumplen el DPF UE-EE.UU. y deben evitar cualquier declaración o práctica engañosa que implique que participan en el DPF UE-EE.UU.; y de que dichas organizaciones ya no tienen derecho a beneficiarse de la decisión de adecuación de la Comisión para recibir información personal de la UE. Una organización que siga afirmando que participa en el DPF UE-EE.UU. o que haga otras declaraciones engañosas relacionadas con el DPF UE-EE.UU. después de haber sido eliminada de la Lista Marco de Privacidad de Datos puede estar sujeta a medidas coercitivas por parte de la FTC, el DOT u otras autoridades encargadas de hacer cumplir la ley.

5. La adhesión a estos Principios puede verse limitada (a) en la medida en que sea necesario para cumplir una orden judicial o satisfacer requisitos de interés público, de aplicación de la ley o de seguridad nacional, incluso cuando la ley o la regulación gubernamental creen obligaciones contradictorias; (b) por ley, orden judicial o reglamento gubernamental que cree autorizaciones explícitas, siempre que, al ejercer cualquier autorización de este tipo, una organización pueda demostrar que su incumplimiento de los Principios se limita a lo necesario para satisfacer los intereses legítimos primordiales promovidos por dicha autorización; o (c) si el efecto del GDPR es permitir excepciones o derogaciones, en las condiciones establecidas en el mismo, siempre que dichas excepciones o derogaciones se apliquen en contextos comparables. En este contexto, las salvaguardias de la legislación estadounidense para proteger privacidad y las libertades civiles incluyen las exigidas por el Decreto 14086[4] en las condiciones establecidas en el mismo (incluidos sus requisitos sobre necesidad y proporcionalidad). En consonancia con el objetivo de mejorar la protección de la privacidad, las organizaciones deben esforzarse por aplicar estos Principios de forma completa y transparente, incluso procurando indicar en sus políticas de privacidad en qué casos se aplicarán las excepciones a los Principios permitidas por la letra b) anterior. Por la misma razón, cuando la opción esté permitida por los Principios y/o la legislación estadounidense, se espera que las organizaciones opten por la mayor protección siempre que sea posible.

6. Las organizaciones están obligadas a aplicar los Principios a todos los datos personales transferidos en virtud del DPF UE-EE.UU. después de su entrada en el DPF UE-EE.UU.. Una organización que opte por ampliar los beneficios del DPF UE-EE.UU. a la información personal de recursos humanos transferida desde la UE para su uso en el contexto de una relación laboral debe indicarlo cuando se autocertifique ante el Departamento y ajustarse a los requisitos establecidos en el Principio Suplementario sobre Autocertificación.

4 Orden Ejecutiva del 7 de octubre de 2022, "Enhancing Safeguards for United States Signals Intelligence Activities".

7. La legislación estadounidense se aplicará a las cuestiones de interpretación y cumplimiento de los Principios y de las políticas de privacidad pertinentes por parte de las organizaciones que participen en la iniciativa EU-DPF de EE.UU., excepto cuando dichas organizaciones se hayan comprometido a cooperar con las autoridades de protección de datos de la UE ("DPA"). Salvo que se indique lo contrario, todas las disposiciones de los Principios se aplican cuando son pertinentes.
8. Definiciones:
   a) "Datos personales" e "información personal" son datos sobre un individuo identificado o identificable que están dentro del ámbito de aplicación del GDPR, recibidos por una organización en los Estados Unidos desde la UE y registrados en cualquier forma.
   b) Por "tratamiento" de datos personales se entenderá cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación o difusión, así como su supresión o destrucción.
   c) "Responsable del tratamiento": persona u organización que, sola o conjuntamente con otras, determina los fines y medios del tratamiento de datos personales.
9. La fecha efectiva de los Principios y de su Anexo I es la fecha de entrada en vigor de la decisión de adecuación de la Comisión Europea.

II. Principios

1. Aviso

a) Una organización debe informar a las personas sobre:

   i. su participación en el DPF UE-EE.UU. y proporcionar un enlace o la dirección web de la Lista del Marco de Privacidad de Datos,
   ii. los tipos de datos personales recogidos y, en su caso, las entidades estadounidenses o filiales estadounidenses de la organización que también se adhieren a los Principios,
   iii. su compromiso de someter a los Principios todos los datos personales recibidos de la UE en virtud del DPF UE-EE.UU,
   iv. los fines para los que recoge y utiliza información personal sobre ellos,
   v. cómo ponerse en contacto con la organización para cualquier consulta o reclamación, incluido cualquier establecimiento pertinente en la UE que pueda responder a dichas consultas o reclamaciones,
   vi. el tipo o la identidad de los terceros a los que revela información personal, y los fines para los que lo hace,
   vii. el derecho de las personas a acceder a sus datos personales,
   viii. las opciones y los medios que la organización ofrece a las personas para limitar el uso y la divulgación de sus datos personales,
   ix. el organismo independiente de resolución de litigios designado para tratar las reclamaciones y proporcionar el recurso adecuado de forma gratuita al par-

ticular, y si se trata de: (1) el panel establecido por las APD, (2) un proveedor de resolución alternativa de litigios con sede en la UE, o (3) un proveedor de resolución alternativa de litigios con sede en Estados Unidos,

x. estar sujeto a los poderes de investigación y aplicación de la FTC, el DOT o cualquier otro organismo legal autorizado de EE.UU,

xi. la posibilidad, en determinadas condiciones, de que el particular invoque un arbitraje vinculante[5],

xii. la obligación de revelar información personal en respuesta a solicitudes legítimas de las autoridades públicas, por ejemplo para cumplir requisitos de seguridad nacional o de aplicación de la ley, y

xiii. su responsabilidad en caso de transferencia a terceros.

b) Este aviso debe facilitarse en un lenguaje claro y visible cuando se pida por primera vez a los individuos que proporcionen información personal a la organización o tan pronto como sea posible, pero en cualquier caso antes de que la organización utilice dicha información para un fin distinto de aquel para el que fue originalmente recopilada o procesada por la organización que la transfiere o la revele por primera vez a un tercero.

2. Elección

a) Una entidad debe ofrecer a las personas la oportunidad de elegir (es decir, excluirse voluntariamente) si su información personal (i) se va a revelar a un tercero o (ii) se va a utilizar para un fin materialmente distinto del fin o fines para los que se recogió originalmente o se autorizó posteriormente por parte de los individuos. Las personas deben disponer de mecanismos claros, visibles y fácilmente accesibles para ejercer su derecho de elección.

b) No obstante lo dispuesto en el apartado anterior, no es necesario proporcionar una opción cuando la divulgación se realiza a un tercero que actúa como agente para realizar tareas en nombre y bajo las instrucciones de la organización. No obstante, la organización deberá celebrar siempre un contrato con el agente.

c) En el caso de la información sensible (es decir, información personal que especifique condiciones médicas o sanitarias, origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical o información que especifique la vida sexual de la persona), las entidades deben obtener el consentimiento expreso afirmativo (es decir, la opción de inclusión) de las personas si dicha información va a ser (i) revelada a un tercero o (ii) utilizada para un fin distinto de aquellos para los que se recopiló originalmente o autorizados posteriormente por las personas mediante el ejercicio de la opción de inclusión. Además, una entidad debe tratar como sensible cualquier información personal recibida de un tercero cuando éste la identifique y trate como tal.

3. Responsabilidad de la transferencia

a) Para transferir información personal a un tercero que actúe como responsable del tratamiento, las organizaciones deben cumplir los Principios de notificación y elección. Las organizaciones también deben suscribir un contrato con el tercero responsable del tratamiento que establezca que dichos datos sólo podrán tratarse para fines limitados y especificados coherentes con el consentimiento proporcio-

5 Véase, por ejemplo, la sección (c) del Principio de recurso, ejecución y responsabilidad.

nado por la persona y que el receptor proporcionará el mismo nivel de protección que los Principios y notificará a la organización si toma la determinación de que ya no puede cumplir esta obligación. El contrato establecerá que, cuando se llegue a tal determinación, el tercero responsable del tratamiento cese el tratamiento o adopte otras medidas razonables y adecuadas para remediarlo.

b) Para transferir datos personales a un tercero que actúe como agente, las organizaciones deben (i) transferir dichos datos sólo para fines limitados y especificados; (ii) asegurarse de que el agente está obligado a proporcionar al menos el mismo nivel de protección de la privacidad que exigen los Principios; (iii) tomar medidas razonables y adecuadas para garantizar que el agente procesa efectivamente la información personal transferida de forma coherente con las obligaciones de la organización en virtud de los Principios; (iv) exigir al agente que notifique a la entidad si llega a la conclusión de que ya no puede cumplir su obligación de proporcionar el mismo nivel de protección que exigen los Principios; v) previa notificación, incluso en virtud del punto iv), tomar medidas razonables y adecuadas para detener y corregir el tratamiento no autorizado; y vi) proporcionar al Departamento, previa solicitud, un resumen o una copia representativa de las disposiciones pertinentes sobre privacidad de su contrato con dicho agente.

4. Seguridad

a) Las organizaciones que creen, mantengan, utilicen o difundan información personal deben adoptar medidas razonables y adecuadas para protegerla de la pérdida, el uso indebido y el acceso no autorizado, la revelación, la alteración y la destrucción, teniendo debidamente en cuenta los riesgos que entraña el tratamiento y la naturaleza de los datos personales.

5. Integridad de los datos y limitación de su finalidad

a) De conformidad con los Principios, la información personal debe limitarse a la información pertinente para los fines del tratamiento[6] Una organización no puede procesar información personal de forma incompatible con los fines para los que ha sido recopilada o posteriormente autorizada por el individuo. En la medida en que sea necesario para esos fines, una organización debe tomar medidas razonables para garantizar que los datos personales son fiables para el uso previsto, exactos, completos y actuales. Las entidades deben respetar los Principios mientras conserven dicha información.

b) La información sólo podrá conservarse en una forma que identifique o haga identificable[7] a la persona mientras sirva a un fin de tratamiento en el sentido del artículo 5(a). Esta obligación no impide que las organizaciones traten la información

6 Dependiendo de las circunstancias, algunos ejemplos de fines de tratamiento compatibles pueden ser los que sirven razonablemente a las relaciones con los clientes, el cumplimiento y las consideraciones jurídicas, la auditoría, la seguridad y la prevención del fraude, la preservación o defensa de los derechos legales de la organización, u otros fines coherentes con las expectativas de una persona razonable dado el contexto de la recogida.

7 En este contexto, si, dados los medios de identificación razonablemente probables (considerando, entre otras cosas, los costes y el tiempo necesarios para la identificación y la tecnología disponible en el momento del tratamiento) y la forma en que se conservan los datos, una persona puede ser razonablemente identificada por la organización, o por un tercero si tuviera acceso a los datos, entonces la persona es "identificable".

personal durante períodos más largos por el tiempo y en la medida en que dicho tratamiento sirva razonablemente a los fines del archivo en interés público, el periodismo, la literatura y el arte, la investigación científica o histórica y el análisis estadístico. En estos casos, dicho tratamiento estará sujeto a los demás principios y disposiciones del DPF UE- EE.UU.. Las organizaciones deberán adoptar medidas razonables y adecuadas para cumplir esta disposición.

6. Acceso

a) Las personas deben tener acceso a la información personal sobre ellas que posea una entidad y poder corregirla, modificarla o eliminarla cuando sea inexacta o se haya procesado infringiendo los Principios, excepto cuando la carga o el gasto de proporcionar acceso sea desproporcionado con respecto a los riesgos para la privacidad de la persona en el caso en cuestión, o cuando se violen los derechos de otras personas.

7. Recurso, ejecución y responsabilidad

a) Una protección eficaz de la privacidad debe incluir mecanismos sólidos para garantizar el cumplimiento de los Principios, recursos para las personas que se vean afectadas por el incumplimiento de los Principios y consecuencias para la organización cuando no se respeten los Principios. Como mínimo, dichos mecanismos deben incluir:

   i. mecanismos de recurso independientes y fácilmente disponibles mediante los cuales se investiguen y resuelvan rápidamente las quejas y disputas de cada individuo, sin coste alguno para el individuo y haciendo referencia a los Principios, y se concedan indemnizaciones por daños y perjuicios cuando la legislación aplicable o las iniciativas del sector privado así lo prevean;

   ii. procedimientos de seguimiento para verificar la veracidad de las declaraciones y afirmaciones que hacen las organizaciones sobre sus prácticas de protección de la vida privada y que las prácticas de protección de la intimidad se han aplicado tal como se presentaron y, en particular, con respecto a los casos de incumplimiento; y

   iii. obligaciones para remediar los problemas derivados del incumplimiento de los Principios por parte de las organizaciones que anuncian su adhesión a los mismos y consecuencias para dichas organizaciones. Las sanciones deben ser suficientemente rigurosas para garantizar el cumplimiento por parte de las organizaciones.

b) Las organizaciones y sus mecanismos independientes de recurso seleccionados responderán con prontitud a las consultas y solicitudes de información del Departamento en relación con el DPF UE-EEUU. Todas las organizaciones deben responder con prontitud a las reclamaciones relativas al cumplimiento de los Principios remitidas por las autoridades de los Estados miembros de la UE a través del Departamento. Las organizaciones que hayan optado por cooperar con las APD, incluidas las organizaciones que procesan datos de recursos humanos, deben responder directamente a dichas autoridades en lo que respecta a la investigación y resolución de reclamaciones.

c) Las organizaciones están obligadas a arbitrar las reclamaciones y seguir los términos establecidos en el Anexo I, siempre que un particular haya invocado el arbitraje vinculante mediante la entrega de una notificación a la organización en cuestión y siguiendo los procedimientos y con sujeción a las condiciones establecidos en el Anexo I.

d) En el contexto de una transferencia ulterior, una organización participante es responsable del tratamiento de la información personal que recibe en virtud del DPF UE-EE.UU. y que posteriormente transfiere a un tercero que actúa como agente en su nombre. La organización participante seguirá siendo responsable en virtud de los Principios si su agente procesa dicha información personal de forma incompatible con los Principios, a menos que la organización demuestre que no es responsable del hecho que dio lugar al daño.

e) Cuando una organización esté sujeta a una orden judicial basada en el incumplimiento o a una orden de un organismo legal estadounidense (por ejemplo, la FTC o el DOT) enumerado en los Principios o en un futuro anexo a los Principios basado en el incumplimiento, la organización hará públicas todas las secciones pertinentes relacionadas con DPF de la UE y EE.UU. de cualquier informe de cumplimiento o evaluación presentado al tribunal o al organismo legal estadounidense e n la medida en que sea compatible con los requisitos de confidencialidad. El Departamento ha establecido un punto de contacto específico para las APD para cualquier problema de cumplimiento por parte de las organizaciones participantes. La FTC y el DOT darán consideración prioritaria a las remisiones de incumplimiento de los Principios procedentes del Departamento y de las autoridades de los Estados miembros de la UE, e intercambiarán información relativa a las remisiones con las autoridades estatales remitentes de forma oportuna, con sujeción a las restricciones de confidencialidad existentes.

III. Principios complementarios

1. Datos sensibles

a) Una organización no está obligada a obtener el consentimiento afirmativo y expreso (es decir, la inclusión voluntaria) con respecto a los datos sensibles cuando el tratamiento es:

   i. en interés vital del interesado o de otra persona;

   ii. necesarias para el establecimiento de reclamaciones o defensas legales;

   iii. necesarios para proporcionar atención médica o diagnóstico;

   iv. efectuado en el marco de las actividades legítimas de una fundación, asociación o cualquier otro organismo sin ánimo de lucro con fines políticos, filosóficos, religiosos o sindicales, y a condición de que el tratamiento se refiera únicamente a los miembros del organismo o a las personas que mantengan contactos regulares con él en relación con sus fines y de que los datos no se comuniquen a terceros sin el consentimiento de los interesados;

   v. necesarios para cumplir las obligaciones de la organización en el ámbito de la legislación laboral; o

   vi. relacionados con datos que el particular haya hecho manifiestamente públicos.

2. Excepciones periodísticas

a) Dadas las protecciones constitucionales de EE.UU. para la libertad de prensa, cuando los derechos de una prensa libre consagrados en la Primera Enmienda de la Constitución de EE.UU. se cruzan con los intereses de protección de la privacidad, la Primera Enmienda debe regir el equilibrio de estos intereses con respecto a las actividades de las personas u organizaciones estadounidenses.

b) La información personal que se recopile para la publicación, emisión u otras formas de comunicación pública de material periodístico, se utilice o no, así como la información que se encuentre en material publicado previamente y difundido desde archivos de medios de comunicación, no está sujeta a los requisitos de los Principios.

3. Responsabilidad secundaria

a) Los proveedores de servicios de Internet ("PSI"), los operadores de telecomunicaciones y otras organizaciones no son responsables en virtud de los Principios cuando, en nombre de otra organización, se limitan a transmitir, encaminar, conmutar o almacenar en caché información. El DPF UE-EE.UU. no crea una responsabilidad secundaria. En la medida en que una organización actúe como mero conducto de datos transmitidos por terceros y no determine los fines y medios del tratamiento de esos datos personales, no sería responsable.

4. Realizar la diligencia debida y llevar a cabo auditorías

a) Las actividades de los auditores y banqueros de inversión pueden implicar el tratamiento de datos personales sin el consentimiento o el conocimiento de la persona. Esto está permitido por los principios de notificación, elección y acceso en las circunstancias que se describen a continuación.

b) Las sociedades anónimas y las sociedades cerradas, incluidas las organizaciones participantes, se someten regularmente a auditorías. Dichas auditorías, especialmente los que investigan posibles irregularidades, pueden verse en peligro si se divulgan prematuramente. Del mismo modo, una organización participante en una posible fusión o adquisición tendrá que realizar, o ser objeto de, un examen de "diligencia debida". Esto implicará a menudo la recogida y el tratamiento de datos personales, como información sobre altos ejecutivos y otro personal clave. Una revelación prematura podría obstaculizar la transacción o incluso infringir la normativa aplicable en materia de valores. Los banqueros de inversión y los abogados encargados de la diligencia debida, o los auditores que llevan a cabo una auditoría, pueden tratar información sin conocimiento de la persona sólo en la medida y durante el periodo necesarios para cumplir los requisitos legales o de interés público y en otras circunstancias en las que la aplicación de estos Principios perjudicaría los intereses legítimos de la organización. Estos intereses legítimos incluyen la supervisión del cumplimiento por parte de las organizaciones de sus obligaciones legales y actividades contables legítimas, así como la necesidad de confidencialidad relacionada con posibles adquisiciones, fusiones, empresas conjuntas u otras transacciones similares llevadas a cabo por banqueros de inversión o auditores.

5. El papel de las autoridades de protección de datos

a) Las organizaciones pondrán en práctica su compromiso de cooperar con las APD tal como se describe a continuación. En virtud del DPF UE- EE.UU., las organizaciones estadounidenses que reciban datos personales de la UE deben comprometerse a emplear mecanismos eficaces para garantizar el cumplimiento de los Principios. Más concretamente, tal como se establece en el Principio de recurso, ejecución y responsabilidad, las organizaciones participantes deben proporcionar: (a)(i) recurso para los individuos a los que se refieren los datos; (a)(ii) procedimientos de seguimiento para verificar que las atestaciones y afirmaciones que han hecho sobre sus prácticas de privacidad son ciertas; y (a)(iii) obligaciones para remediar los problemas derivados del incumplimiento de los Principios y consecuencias para dichas organizaciones. Una organización puede satisfacer los pun-

tos (a)(i) y (a)(iii) del Principio de Recurso, Cumplimiento y Responsabilidad si se adhiere a los requisitos establecidos aquí para cooperar con las APD.

b) Una organización se compromete a cooperar con las APD declarando en su presentación de autocertificación DPF UE-EE.UU. al Departamento (véase el Principio Suplementario sobre Autocertificación) que la organización:

   i. opta por cumplir el requisito de los puntos (a)(i) y (a)(iii) del Principio de recurso, ejecución y responsabilidad comprometiéndose a cooperar con las APD;

   ii. cooperará con las APD en la investigación y resolución de las denuncias presentadas en virtud de los Principios; y

   iii. acatará cualquier consejo dado por las APD cuando éstas consideren que la organización necesita tomar medidas específicas para cumplir con los Principios, incluidas medidas correctoras o compensatorias en beneficio de las personas afectadas por cualquier incumplimiento de los Principios, y proporcionará a las APD una confirmación por escrito de que se han tomado dichas medidas.

c) Funcionamiento de los paneles DPA

   i. La cooperación de las APD se prestará en forma de información y asesoramiento de la siguiente manera:

      1. El asesoramiento de las APD se prestará a través de un grupo informal de APD establecido a escala de la UE, que, entre otras cosas, contribuirá a garantizar un enfoque armonizado y coherente.

      2. El grupo asesorará a las organizaciones estadounidenses afectadas sobre las reclamaciones no resueltas de particulares acerca del tratamiento de información personal que haya sido transferida desde la UE en el marco del DPF UE-EE.UU.. Este asesoramiento tendrá por objeto garantizar la correcta aplicación de los principios e incluirá las soluciones que las APD consideren adecuadas para las personas afectadas.

      3. El panel proporcionará dicho asesoramiento en respuesta a las remisiones de las organizaciones afectadas y/o a las reclamaciones recibidas directamente de particulares contra organizaciones que se hayan comprometido a cooperar con las APD a efectos de la DPF UE-EE.UU., al tiempo que animará y, si es necesario, ayudará a dichos particulares en primera instancia a utilizar los mecanismos internos de tramitación de reclamaciones que pueda ofrecer la organización.

      4. El dictamen sólo se emitirá después de que ambas partes en litigio hayan tenido una oportunidad razonable de comentar y aportar las pruebas que deseen. El panel tratará de emitir su dictamen tan pronto como lo permita este requisito del debido proceso. Por regla general, el panel tratará de proporcionar asesoramiento en un plazo de 60 días a partir de la recepción de una reclamación o remisión, y más rápidamente siempre que sea posible.

      5. El panel hará públicos los resultados de su examen de las quejas que se le presenten, si lo considera oportuno.

      6. La prestación de asesoramiento a través del panel no dará lugar a responsabilidad alguna para el panel ni para las APD individuales.

   vii. Como ya se ha indicado, las organizaciones que elijan esta opción para la resolución de litigios deben comprometerse a cumplir el asesoramiento de los APD. Si una organización no cumple en un plazo de 25 días a partir de la entrega del asesoramiento y no ha ofrecido ninguna explicación satisfactoria

por el retraso, el panel notificará su intención de remitir el asunto a la FTC, el DOT u otro organismo federal o estatal de EE.UU. con poderes legales para tomar medidas coercitivas en casos de engaño o tergiversación, o de concluir que el acuerdo de cooperación se ha incumplido gravemente y, por lo tanto, debe considerarse nulo y sin efecto. En este último caso, el panel informará al Departamento para que la Lista Marco de Privacidad de Datos pueda ser debidamente modificada. Cualquier incumplimiento del compromiso de cooperar con las APD, así como los incumplimientos de los Principios, será perseguible como práctica engañosa en virtud del artículo 5 de la Ley FTC (15 U.S.C. § 45), 49 U.S.C. § 41712 u otra ley similar.

d) Una organización que desee que sus beneficios de DPF UE-EE.UU. cubran los datos de recursos humanos transferidos desde la UE en el contexto de la relación laboral debe comprometerse a cooperar con las DPA con respecto a dichos datos (véase el Principio Suplementario sobre Datos de Recursos Humanos).cubran los datos de recursos humanos transferidos desde la UE en el contexto de la relación laboral debe comprometerse a cooperar con las DPA con respecto a dichos datos (véase el Principio Suplementario sobre Datos de Recursos Humanos).

e) Las organizaciones que elijan esta opción deberán abonar una cuota anual destinada a cubrir los gastos de funcionamiento del panel. Además, se les podrá pedir que sufraguen todos los gastos de traducción necesarios derivados del examen por parte del panel de las remisiones o denuncias presentadas contra ellas. El importe de la tasa será determinado por el Departamento previa consulta con la Comisión. La recaudación de la tasa podrá ser llevada a cabo por un tercero seleccionado por el Departamento para que actúe como depositario de los fondos recaudados con este fin. El Departamento cooperará estrechamente con la Comisión y las APD en el establecimiento de procedimientos adecuados para la distribución de los fondos recaudados mediante la tasa, así como en otros aspectos procedimentales y administrativos del panel. El Departamento y la Comisión podrán acordar modificar la periodicidad de la recaudación de la tasa.

6. Autocertificación

a) Los beneficios del DPF UE-EE.UU. están garantizados a partir de la fecha en que el Departamento incluya a la organización en la Lista del Marco de Privacidad de Datos. El Departamento sólo incluirá a una organización en la Lista Marco de Privacidad de Datos después de haber determinado que la presentación inicial de autocertificación de la organización está completa, y retirará a la organización de esa lista si se retira voluntariamente, no completa su recertificación anual, o si incumple persistentemente los Principios (véase el Principio Suplementario sobre Resolución de Conflictos y Aplicación).

b) Para autocertificarse inicialmente o volver a certificarse posteriormente para el DPF UE-EE.UU., una organización debe proporcionar en cada ocasión al Departamento una presentación realizada por un directivo de la empresa en nombre de la organización que está autocertificando o volviendo a certificar (según corresponda) su adhesión a los Principios[8], que contenga al menos la siguiente información:

8 La presentación debe ser realizada a través del sitio web del Marco de Privacidad de Datos del Departamento por una persona de la organización que esté autorizada a hacer declaraciones en nombre de la organización y de cualquiera de sus entidades cubiertas en relación con su adhesión a los Principios.

i. el nombre de la organización estadounidense autocertificante o recertificante, así como el nombre o nombres de cualquiera de sus entidades o filiales estadounidenses que también se adhieran a los Principios que la organización desee cubrir;

ii. una descripción de las actividades de la entidad con respecto a la información personal que se recibiría de la UE en virtud del DPF UE-EE.UU;

iii. una descripción de la política o políticas de privacidad pertinentes de la organización para dicha información personal, incluyendo:

1. si la organización tiene un sitio web público, la dirección web pertinente en la que está disponible la política de privacidad, o si la organización no tiene un sitio web público, en la que la política de privacidad está disponible para su consulta por el público; y

2. su fecha efectiva de aplicación;

iv. una oficina de contacto dentro de la organización para la tramitación de reclamaciones, solicitudes de acceso y cualquier otra cuestión que surja en virtud de los Principios[9], incluyendo:

1. nombre(s), cargo(s) (si procede), dirección(es) de correo electrónico y número(s) de teléfono de la(s) persona(s) u oficina(s) de contacto pertinente(s) dentro de la organización; y

2. la dirección postal de la organización en Estados Unidos;

v. el órgano estatutario específico que tiene jurisdicción para conocer de cualquier reclamación contra la organización en relación con posibles prácticas desleales o engañosas y violaciones de las leyes o reglamentos que rigen la privacidad (y que figura en los Principios o en un futuro anexo a los Principios);

vi. el nombre de cualquier programa de privacidad al que pertenezca la organización;

vii. el método de verificación (es decir, autoevaluación; o revisiones externas del cumplimiento, incluido el tercero que realiza dichas revisiones)[10]; y

viii. el mecanismo o mecanismos independientes de recurso disponibles para investigar las quejas no resueltas relacionadas con los Principios[11].

c) Cuando la organización desee que sus prestaciones de DPF UE-EE.UU. cubran la información sobre recursos humanos transferida desde la UE para su uso en el contexto de la relación laboral, podrá hacerlo cuando un órgano estatutario enumerado en los Principios o en un futuro anexo a los Principios tenga jurisdicción para conocer de reclamaciones contra la organización derivadas del tratamiento de información sobre recursos humanos. Además, la organización debe indicarlo en su presentación inicial de autocertificación, así como en cualquier presentación de recertificación, y declarar su compromiso de cooperar con la autoridad o autoridades de la UE afectadas de conformidad con los Principios complementarios sobre los datos de recursos humanos y la función de las autoridades de protección de datos (según proceda) y que cumplirá con el asesoramiento prestado por

9 El "contacto principal de la organización" o el "responsable corporativo de la organización" no puede ser externo a la organización (por ejemplo, un abogado externo o un consultor externo).

10 Véase el principio complementario sobre verificación.

11 Véase el Principio Complementario sobre Resolución de Litigios y Ejecución.

dichas autoridades. La organización también debe facilitar al Departamento una copia de su política de privacidad en materia de recursos humanos y proporcionar información sobre el lugar en el que la política de privacidad está disponible para su consulta por parte de los empleados afectados.

d) El Departamento mantendrá y pondrá a disposición del público la lista del marco de protección de la intimidad de los datos de las organizaciones que hayan presentado una autocertificación inicial completa y actualizará dicha lista sobre la base de las presentaciones anuales de recertificación completadas, así como de las notificaciones recibidas de conformidad con el principio complementario sobre resolución de litigios y ejecución. Dichos informes de recertificación deberán presentarse al menos una vez al año; de lo contrario, la organización será eliminada de la Lista del Marco de Privacidad de Datos y dejará de disfrutar de las ventajas del DPF UE-EE.UU.. Todas las organizaciones que sean incluidas en la Lista Marco de Privacidad de Datos por el Departamento deben tener políticas de privacidad pertinentes que cumplan con el Principio de Notificación y declarar en esas políticas de privacidad que adherirse a los Principios[12]. Si está disponible en línea, la política de privacidad de una organización debe incluir un hipervínculo al sitio web del Marco de Privacidad de Datos del Departamento y un hipervínculo al sitio web o al formulario de presentación de quejas del mecanismo de recurso independiente que está disponible para investigar las quejas no resueltas relacionadas con los Principios de forma gratuita para el individuo.

e) Los Principios se aplican inmediatamente después de la autocertificación. Las organizaciones participantes que anteriormente se autocertificaron conforme a los Principios del Marco del Escudo de Privacidad UE- EE.UU. deberán actualizar sus políticas de privacidad para hacer referencia a los "Principios del Marco de Privacidad de Datos UE- EE.UU.". Dichas organizaciones deberán incluir esta referencia lo antes posible y, en cualquier caso, en un plazo máximo de tres meses a partir de la fecha de entrada en vigor de los Principios del Marco de Protección de la Privacidad de Datos entre la UE y Estados Unidos.

f) Una organización debe someter a los Principios todos los datos personales recibidos de la UE en virtud del DPF UE-EE.UU.. El compromiso de adherirse a los Principios no está limitado en el tiempo en lo que respecta a los datos personales recibidos durante el periodo en el que la organización disfruta de los beneficios del DPF UE-EE.UU.; su compromiso significa que seguirá aplicando los Principios a dichos datos mientras la organización los almacene, utilice o divulgue, incluso si posteriormente abandona el DPF UE-EE.UU. por cualquier motivo. Una organización que desee retirarse del DPF UE-EE.UU. debe notificarlo al Departamento con antelación. Esta notificación también debe indicar lo que la organización hará con los datos personales que recibió en virtud del DPF UE-EE.UU. (es decir, retener, devolver o suprimir los datos, y si los retiene, los medios autorizados por

12 Una organización que se autocertifique por primera vez no podrá alegar la participación en el DPF UE-EE.UU. en su política de privacidad definitiva hasta que el Departamento notifique a la organización que puede hacerlo. La organización debe proporcionar al Departamento un borrador de política de privacidad, que sea coherente con los Principios, cuando presente su autocertificación inicial. Una vez que el Departamento haya determinado que la presentación de la autocertificación inicial de la organización está completa, el Departamento notificará a la organización que debe finalizar (por ejemplo, publicar cuando proceda) su política de privacidad coherente con los DPF UE-EE.UU.. La organización debe notificar inmediatamente al Departamento tan pronto como finalice la política de privacidad pertinente, momento en el que el Departamento incluirá a la organización en la Lista del Marco de Privacidad de Datos.

los que proporcionará protección a los datos). Una organización que se retire del DPF UE-EE.UU., pero que desee conservar dichos datos, deberá afirmar anualmente ante el Departamento su compromiso de seguir aplicando los Principios a los datos o proporcionar una protección "adecuada" a los datos por otro medio autorizado (por ejemplo, utilizando un contrato que refleje plenamente los requisitos de las cláusulas contractuales tipo pertinentes adoptadas por la Comisión); de lo contrario, la organización deberá devolver o suprimir la información[13]. Una entidad que se retire del DPF UE-EE.UU. debe eliminar de cualquier política de privacidad pertinente cualquier referencia al DPF UE-EE.UU. que implique que la entidad sigue participando en el DPF UE-EE.UU. y tiene derecho a sus beneficios.

g) Una organización que vaya a dejar de existir como entidad jurídica independiente debido a un cambio en su estatus corporativo, como resultado de una fusión, absorción, quiebra o disolución, debe notificarlo al Departamento con antelación. La notificación también debe indicar si la entidad resultante del cambio en el estado corporativo (i) sigue participando en el DPF UE-EE.UU. a través de una autocertificación existente; (ii) autocertificarse como nuevo participante en el DPF UE-EE.UU. (por ejemplo, cuando la nueva entidad o la entidad superviviente no disponga ya de una autocertificación a través de la cual pueda participar en el DPF UE-EE.UU.); o (iii) establecer otras salvaguardias, como un acuerdo por escrito que garantice la aplicación continuada de los Principios a cualquier dato personal que la organización haya recibido en el marco del DPF UE-EE.UU.).U.S. DPF y se conservarán. Cuando no se apliquen ni (i), ni (ii), ni (iii), los datos personales que se hayan recibido en virtud del DPF UE-EE.UU. deberán devolverse o suprimirse sin demora.

h) Cuando una organización abandona el DPF UE-EE.UU. por cualquier motivo, debe eliminar todas las declaraciones que impliquen que la organización sigue participando en el DPF UE-EE.UU. o que tiene derecho a los beneficios del DPF UE-EE. UU.. La marca de certificación DPF UE-EE.UU., si se utiliza, también debe ser eliminada. Cualquier tergiversación al público en general sobre la adhesión de una organización a los Principios puede ser perseguida por la FTC, el DOT u otro organismo gubernamental pertinente. Las declaraciones falsas al Departamento pueden ser procesables bajo la Ley de Declaraciones Falsas (18 U.S.C. § 1001).

7. Verificación

a) Las organizaciones deben proporcionar procedimientos de seguimiento para verificar que las declaraciones y afirmaciones que hacen sobre sus prácticas de privacidad DPF UE-EE.UU. son ciertas y que dichas prácticas de privacidad se han aplicado según lo representado y de conformidad con los Principios.

b) Para cumplir los requisitos de verificación del Principio de Recurso, Ejecución y Responsabilidad, una organización debe verificar tales declaraciones y afirmaciones mediante autoevaluación o revisiones externas del cumplimiento.

---

13 Si una organización opta en el momento de su retirada por conservar los datos personales que recibió en virtud del DPF UE-EE.UU. y afirmar anualmente al Departamento que sigue aplicando los Principios a dichos datos, la organización deberá verificar al Departamento una vez al año tras su retirada (es decir, a menos que y hasta que el la organización proporciona una protección "adecuada" de dichos datos por otro medio autorizado, o devuelve o suprime todos esos datos y notifica esta acción al Departamento) qué ha hecho con esos datos personales, qué hará con cualquiera de esos datos personales que siga conservando, y quién servirá de punto de contacto permanente para cuestiones relacionadas con los Principios.

c) Cuando la organización haya optado por la autoevaluación, dicha verificación deberá demostrar que su política de privacidad relativa a la información personal recibida de la UE es precisa, exhaustiva, fácilmente disponible, conforme a los Principios y se aplica en su totalidad (es decir, se cumple). También debe indicar que las personas están informadas de los acuerdos internos para la gestión de reclamaciones y de los mecanismos de recurso independientes a través de los cuales pueden presentar reclamaciones; que dispone de procedimientos para formar a los empleados en su aplicación y sancionarlos en caso de incumplimiento; y que dispone de procedimientos internos para realizar periódicamente revisiones objetivas del cumplimiento de lo anterior. Un directivo de la empresa u otro representante autorizado de la organización debe firmar al menos una vez al año una declaración en la que se verifique que se ha completado la autoevaluación, y esta declaración debe estar disponible a petición de particulares o en el contexto de una investigación o una denuncia por incumplimiento.

d) Cuando la organización haya optado por una verificación externa del cumplimiento, dicha verificación debe demostrar que su política de privacidad relativa a la información personal recibida de la UE es exacta, exhaustiva, fácilmente disponible, conforme a los Principios y se aplica en su totalidad (es decir, se cumple). También debe indicar que los particulares están informados de los mecanismos a través de los cuales pueden presentar reclamaciones. Los métodos de revisión pueden incluir, entre otros, auditorías, revisiones aleatorias, el uso de "señuelos" o el uso de herramientas tecnológicas, según proceda. Una declaración que verifique que se ha llevado a cabo con éxito una revisión externa del cumplimentados debe ser firmada por el revisor o por el responsable corporativo u otro representante autorizado de la organización al menos una vez al año y estar disponibles a petición de particulares o en el contexto de una investigación o una reclamación sobre cumplimiento.

e) Las organizaciones deben conservar sus registros sobre la aplicación de las normas de la UE-.DPF de EE.UU. y ponerlos a disposición, previa solicitud, en el contexto de una investigación o de una reclamación por incumplimiento, del organismo independiente de resolución de litigios encargado de investigar las reclamaciones o de la agencia competente en materia de prácticas desleales y engañosas. Las organizaciones también deben responder con prontitud a las consultas y otras solicitudes de información del Departamento relacionadas con la adhesión de la organización a los Principios.

8. Acceso

a) El principio de acceso en la práctica

i. Según los Principios, el derecho de acceso es fundamental para la protección de la intimidad. En concreto, permite a las personas verificar la exactitud de la información que se tiene sobre ellas. El Principio de Acceso significa que las personas tienen derecho a:

1. obtener de una organización la confirmación de si ésta está tratando o no datos personales que le conciernen[14];

2. haberles comunicado dichos datos para que pudieran comprobar su exactitud y la licitud del tratamiento; y

14 La organización debe responder a las solicitudes de una persona en relación con los fines del tratamiento, las categorías de datos personales afectadas y los destinatarios o categorías de destinatarios a los que se revelan los datos personales.

3. hacer rectificar, modificar o suprimir los datos cuando sean inexactos o se hayan tratado infringiendo los Principios.

ii. Las personas no tienen que justificar las solicitudes de acceso a sus datos personales. Al responder a las solicitudes de acceso de los particulares, las organizaciones deben guiarse en primer lugar por la preocupación o preocupaciones que dieron lugar a las solicitudes. Por ejemplo, si una solicitud de acceso es vaga o de amplio alcance, una organización puede entablar un diálogo con la persona para comprender mejor la motivación de la solicitud y localizar la información pertinente. La entidad puede preguntar con qué parte o partes de la organización ha interactuado la persona o sobre la naturaleza de la información o su uso que es objeto de la solicitud de acceso.

iii. En consonancia con la naturaleza fundamental del acceso, las entidades siempre deben esforzarse de buena fe por facilitar el acceso. Por ejemplo, cuando determinada información deba protegerse y pueda separarse fácilmente de otra información personal sujeta a una solicitud de acceso, la entidad deberá redactar la información protegida y facilitar el resto de la información. Si una entidad determina que el acceso debe restringirse en un caso concreto, deberá proporcionar a la persona que lo solicite una explicación de por qué ha tomado esa decisión y un punto de contacto para cualquier otra consulta.

b) Carga o coste de facilitar el acceso

i. El derecho de acceso a los datos personales puede restringirse en circunstancias excepcionales en las que se violen los derechos legítimos de otras personas o en las que la carga o el coste de facilitar el acceso sean desproporcionados en relación con los riesgos para la intimidad de la persona en el caso en cuestión. Los gastos y la carga son factores importantes que deben tenerse en cuenta, pero no son factores determinantes a la hora de determinar si el acceso es razonable.

ii. Por ejemplo, si la información personal se utiliza para tomar decisiones que afectarán significativamente a la persona (por ejemplo, la denegación o concesión de prestaciones importantes, como un seguro, una hipoteca o un puesto de trabajo), entonces, en consonancia con las demás disposiciones de estos Principios complementarios, la entidad tendría que revelar esa información aunque sea relativamente difícil o costosa de proporcionar. Si la información personal solicitada no es sensible o no se utiliza para tomar decisiones que afecten significativamente a la persona, pero se puede obtener fácilmente y no es costoso proporcionarla, la entidad tendría que facilitar el acceso a dicha información.

c) Información comercial confidencial

i. La información comercial confidencial es información que una organización ha tomado medidas para proteger de la divulgación, cuando ésta ayudaría a un competidor en el mercado. Las organizaciones pueden denegar o limitar el acceso en la medida en que conceder pleno acceso revelaría su propia información comercial confidencial, como inferencias de marketing o clasificaciones generadas por la organización, o la información comercial confidencial de otra que esté sujeta a una obligación contractual de confidencialidad.

ii. Cuando la información comercial confidencial pueda separarse fácilmente de otra información personal sujeta a una solicitud de acceso, la entidad deberá redactar la información comercial confidencial y poner a disposición la información no confidencial.

d) Organización de bases de datos

i. El acceso puede facilitarse en forma de divulgación de la información personal pertinente por parte de una organización al individuo y no requiere el acceso del individuo a la base de datos de una organización.

ii. El acceso sólo debe facilitarse en la medida en que una organización almacene la información personal. El principio de acceso no crea por sí mismo ninguna obligación de conservar, mantener, reorganizar o reestructurar los ficheros de información personal.

e) Cuándo puede restringirse el acceso

i. Dado que las organizaciones siempre deben hacer esfuerzos de buena fe para proporcionar a las personas acceso a sus datospersonales, las circunstancias en las que las organizaciones pueden restringir dicho acceso son limitadas, y cualquier motivo para restringir el acceso debe ser específico. Como en el caso del RGPD, una organización puede restringir el acceso a la información en la medida en que sea probable que su divulgación interfiera con la salvaguarda de importantes intereses públicos compensatorios, como la seguridad nacional, la defensa o la seguridad pública. Además, cuando la información personal se procesa únicamente con fines de investigación o estadísticos, puede denegarse el acceso. Otras razones para denegar o limitar el acceso son:

1. interferencia con la ejecución o el cumplimiento de la ley o con causas privadas, incluida la prevención, investigación o detección de delitos o el derecho a un juicio justo;
2. divulgación cuando se vulneren los derechos legítimos o intereses importantes de terceros;
3. violar un privilegio u obligación legal o profesional;
4. perjudicar las investigaciones de seguridad de los empleados o los procedimientos de reclamación o en relación con la planificación de la sucesión de los empleados y las reorganizaciones corporativas; o
5. perjudicar la confidencialidad necesaria en funciones de control, inspección o reglamentación relacionadas con la buena gestión, o en negociaciones futuras o en curso en las que participe la organización.

ii. Una organización que alegue una excepción tiene la carga de demostrar su necesidad, y deben darse a los particulares las razones para restringir el acceso y un punto de contacto para consultas posteriores.

f) Derecho a obtener confirmación y cobro de una tasa para cubrir los costes de acceso

i. Toda persona tiene derecho a obtener confirmación sobre si esta organización dispone o no de datos personales que le conciernan. También tiene derecho a que se le comuniquen sus datos personales. Una organización puede cobrar una tasa que no sea excesiva.

ii. El cobro de una tasa puede estar justificado, por ejemplo, cuando las solicitudes de acceso son manifiestamente excesivas, en particular por su carácter repetitivo.

iii. No puede denegarse el acceso por razones de coste si el interesado se ofrece a pagar los gastos.

g) Solicitudes de acceso repetitivas o infundadas

i. Una entidad puede establecer límites razonables al número de veces dentro de un período determinado que se atenderán las solicitudes de acceso de una persona concreta. A la hora de establecer dichas limitaciones, la entidad deberá tener en cuenta factores como la frecuencia con la que se actualiza la información, la finalidad para la que se utilizan los datos y la naturaleza de la información.

h) Solicitudes de acceso fraudulentas

i. Una organización no está obligada a facilitar el acceso a menos que se le proporcione información suficiente que le permita confirmar la identidad de la persona que presenta la solicitud.

i) Plazos de respuesta

i. Las entidades deben responder a las solicitudes de acceso en un plazo razonable, de manera razonable y de forma fácilmente inteligible para el interesado. Una entidad que proporcione información a los interesados a intervalos regulares podrá satisfacer una solicitud de acceso individual con su divulgación regular si ello no constituye un retraso excesivo.

9. Datos sobre recursos humanos

a) Cobertura del DPF UE-EE.UU.

i. Cuando una organización de la UE transfiere información personal sobre sus empleados (pasados o presentes) recopilada en el contexto de la relación laboral, a una empresa matriz, filial o proveedor de servicios no afiliado de Estados Unidos que participa en el DPF UE-EE.UU., la transferencia goza de los beneficios del DPF UE-EE.UU.. En tales casos, la recogida de la información y su tratamiento previo a la transferencia habrán estado sujetos a la legislación nacional del Estado miembro de la UE en el que se recogió, y deberán respetarse todas las condiciones o restricciones para su transferencia con arreglo a dicha legislación.

ii. Los Principios sólo son pertinentes cuando se transfieren o se accede a registros identificados o identificables individualmente. Los informes estadísticos que se basan en datos de empleo agregados y no contienen datos personales o el uso de datos anónimos no plantean problemas de privacidad.

b) Aplicación de los principios de notificación y elección

i. Una organización estadounidense que haya recibido información de empleados de la UE en virtud del DPF UE-EE.UU. podrá revelarla a terceros o utilizarla para fines distintos únicamente de conformidad con los principios de notificación y elección. Por ejemplo, cuando una entidad pretenda utilizar la información personal recopilada a través de la relación laboral para fines no relacionados con el empleo, como comunicaciones de marketing, la entidad estadounidense deberá proporcionar a las personas afectadas la opción requerida antes de hacerlo, a menos que ya hayan autorizado el uso de la información para tales fines. Este uso no debe ser incompatible con los fines para los que se recogió la información personal o para los que la persona la autorizó posteriormente. Además, estas opciones no deben utilizarse para restringir las oportunidades de empleo o tomar medidas punitivas contra los empleados.

ii. Debe tenerse en cuenta que determinadas condiciones de aplicación general para la transferencia desde algunos Estados miembros de la UE pueden impedir

otros usos de dicha información incluso después de su transferencia fuera de la UE, y dichas condiciones deberán respetarse.

iii. Además, los empresarios deben hacer esfuerzos razonables para adaptarse a las preferencias de privacidad de los empleados. Esto podría incluir, por ejemplo, restringiendo el acceso a los datos personales, anonimizando determinados datos o asignando códigos o seudónimos cuando los nombres reales no sean necesarios para los fines de gestión de que se trate.

iv. En la medida y durante el periodo necesarios para evitar perjudicar la capacidad de la organización a la hora de tomar promociones, nombramientos u otras decisiones laborales similares, una organización no necesita ofrecer preaviso y elección.

c) Aplicación del principio de acceso

i. El Principio complementario sobre el acceso ofrece orientación sobre las razones que pueden justificar la denegación o limitación del acceso previa solicitud en el contexto de los recursos humanos. Por supuesto, los empresarios de la UE deben cumplir la normativa local y garantizar que los empleados de la UE tengan acceso a la información exigida por la ley en sus países de origen, independientemente del lugar de tratamiento y almacenamiento de los datos. El DPF UE-EE.UU. exige que una organización que procese dichos datos en Estados Unidos coopere para proporcionar dicho acceso, ya sea directamente o a través del empleador de la UE.

d) Ejecución

i. En la medida en que la información personal se utilice únicamente en el contexto de la relación laboral, la responsabilidad principal de los datos frente al empleado sigue recayendo en la organización de la UE. De ello se deduce que, cuando los empleados europeos presenten reclamaciones sobre violaciones de sus derechos de protección de datos y no estén satisfechos con los resultados de los procedimientos internos de revisión, reclamación y recurso (o de cualquier procedimiento de reclamación aplicable en virtud de un contrato con un sindicato), deberán dirigirse a la autoridad laboral o de protección de datos estatal o nacional de la jurisdicción en la que trabajen los empleados. Esto incluye los casos en los que el presunto tratamiento incorrecto de su información personal sea responsabilidad de la organización estadounidense que ha recibido la información del empleador y, por tanto, implique una presunta infracción de los Principios. Esta será la forma más eficaz de abordar los derechos y obligaciones, a menudo solapados, que imponen la legislación laboral y los convenios laborales locales, así como la legislación sobre protección de datos.

ii. Una organización estadounidense que participe en el DPF UE- EE.UU. que utilice datos de recursos humanos de la UE transferidos desde la UE en el contexto de la relación laboral y que desee que dichas transferencias queden cubiertas por el DPF UE-EE.UU. deberá, por tanto, comprometerse a cooperar en las investigaciones de las autoridades competentes de la UE en tales casos y a seguir sus consejos.

e) Aplicación del principio de responsabilidad por las transferencias ulteriores

i. Para necesidades operativas ocasionales relacionadas con el empleo de la organización participante con respecto a los datos personales transferidos en virtud del DPF UE-EE.UU., como la reserva de un vuelo, una habitación de hotel o la cobertura de un seguro, las transferencias de datos personales de un pequeño número de empleados pueden tener lugar a los responsables del

tratamiento sin aplicación del Principio de Acceso ni celebración de un contrato con el responsable del tratamiento tercero, como se exigiría en virtud del Principio de Responsabilidad de las Transferencias Ulteriores, siempre que la organización participante haya cumplido los Principios de Notificación y de Elección.

10. Contratos obligatorios para transferencias ulteriores

a) Contratos de tratamiento de datos

i. Cuando los datos personales se transfieran de la UE a Estados Unidos sólo con fines de tratamiento, será necesario un contrato, independientemente de la participación del encargado del tratamiento en el DPF UE-EE.UU.

ii. Los responsables del tratamiento de datos en la UE siempre están obligados a celebrar un contrato cuando se realiza una transferencia por mero tratamiento, tanto si la operación de tratamiento se lleva a cabo dentro como fuera de la UE, y tanto si el encargado del tratamiento participa en el DPF UE-EE. UU. como si no. La finalidad del contrato es garantizar que el encargado del tratamiento:

1. actúa sólo bajo las instrucciones del controlador;
2. proporciona las medidas técnicas y organizativas adecuadas para proteger los datos personales contra la destrucción accidental o ilícita o la pérdida accidental, la alteración, la difusión o el acceso no autorizados, y comprende si se permite la transferencia ulterior; y
3. teniendo en cuenta la naturaleza del tratamiento, ayuda al responsable del tratamiento a responder a las personas que ejercen sus derechos en virtud de los Principios.

iii. Dado que las organizaciones participantes ofrecen una protección adecuada, los contratos con dichas organizaciones para el mero tratamiento no requieren autorización previa.

b) Transferencias dentro de un grupo controlado de sociedades o entidades

i. Cuando la información personal se transfiere entre dos responsables del tratamiento dentro de un grupo controlado de sociedades o entidades, no siempre es necesario un contrato en virtud del Principio de responsabilidad de las transferencias ulteriores. Los responsables del tratamiento dentro de un grupo controlado de corporaciones o entidades pueden basar dichas transferencias en otros instrumentos, como las Normas Corporativas Vinculantes de la UE u otros instrumentos intragrupo (por ejemplo, programas de cumplimiento y control), garantizando la continuidad de la protección de la información personal en virtud de los Principios. En caso de tales transferencias, la organización participante seguirá siendo responsable del cumplimiento de los Principios.

c) Transferencias entre controladores

i. Para las transferencias entre responsables del tratamiento, no es necesario que el responsable del tratamiento receptor sea una organización participante o disponga de un mecanismo de recurso independiente. La organización participante debe celebrar un contrato con el tercero responsable del tratamiento destinatario que establezca el mismo nivel de protección que el disponible en virtud del DPF UE-EE.UU., sin incluir el requisito de que el tercero responsable del tratamiento sea una organización participante o disponga de un mecanismo de recurso independiente, siempre que ponga a disposición un mecanismo equivalente.

11. Resolución de litigios y ejecución

a) El Principio de Recurso, Ejecución y Responsabilidad establece los requisitos para la aplicacióndel DPF UE-EE.UU. Cómo cumplir los requisitos del punto (a)(ii) del Principio se establecen en el Principio Suplementario sobre Verificación. Este Principio complementario aborda los puntos (a)(i) y (a)(iii), que exigen mecanismos de recurso independientes. Estos mecanismos pueden adoptar diferentes formas, pero deben cumplir los requisitos del Principio de recurso, ejecución y responsabilidad. Las organizaciones satisfacen los requisitos mediante lo siguiente (i) el cumplimiento de programas de privacidad desarrollados por el sector privado que incorporen los Principios en sus normas y que incluyan mecanismos de aplicación efectivos del tipo descrito en el Principio de recurso, aplicación y responsabilidad; (ii) el cumplimiento de las autoridades supervisoras legales o reglamentarias que prevean la gestión de reclamaciones individuales y la resolución de conflictos; o (iii) el compromiso de cooperar con las APD ubicadas en la UE o sus representantes autorizados.

b) Esta lista pretende ser ilustrativa y no limitativa. El sector privado puede diseñar mecanismos adicionales para garantizar el cumplimiento, siempre que cumplan los requisitos del Principio de recurso, cumplimiento y responsabilidad y los Principios complementarios. Tenga en cuenta que los requisitos del principio de recurso, aplicación y responsabilidad son adicionales al requisito de que los esfuerzos de autorregulación deben ser ejecutables en virtud de la Sección 5 de la Ley FTC (15 U.S.C. § 45) que prohíbe los actos desleales o engañosos, 49 U.S.C. § 41712 que prohíbe a un transportista o agente de venta de billetes realizar prácticas desleales o engañosas en el transporte aéreo o en la venta de transporte aéreo, u otra ley o reglamento que prohíba tales actos.

c) Para ayudar a garantizar el cumplimiento de sus compromisos con el DPF UE-EE. UU. y apoyar la administración del programa, las organizaciones, así como sus mecanismos de recurso independientes, deben proporcionar información relativa al DPF UE-EE.UU. cuando lo solicite el Departamento. Además, las organizaciones deben responder con rapidez a las reclamaciones relativas a su cumplimiento de los Principios remitidas a través del Departamento por las APD. La respuesta debe abordar si la queja tiene fundamento y, en caso afirmativo, cómo rectificará la organización el problema. El Departamento protegerá la confidencialidad de la información que reciba de conformidad con la legislación estadounidense.

d) Mecanismos de recurso

   i. Se debe animar a los particulares a plantear cualquier queja que puedan tener ante la organización pertinente antes de acudir a mecanismos de recurso independientes. Las organizaciones deben responder a los particulares en un plazo de 45 días a partir de la recepción de la queja. La independencia de un mecanismo de recurso es una cuestión de hecho que puede demostrarse, en particular, por su imparcialidad, su composición y financiación transparentes y un historial probado. Como exige el Principio de recurso, ejecución y responsabilidad, el recurso a disposición de los particulares debe ser de fácil acceso y gratuito para los particulares. Los organismos independientes de resolución de litigios deben examinar todas las reclamaciones recibidas de los particulares, a menos que sean manifiestamente infundadas o frívolas. Esto no impide que el organismo independiente de resolución de litigios que gestione el mecanismo de recurso establezca requisitos de admisibilidad, pero dichos requisitos deben ser transparentes y estar justificados (por ejemplo, para excluir las reclamaciones que queden fuera del ámbito del programa o que deban examinarse en otro foro), y no deben tener el efecto de socavar el

compromiso de examinar las reclamaciones legítimas. Además, los mecanismos de recurso deben proporcionar a las personas información completa y fácilmente disponible sobre el funcionamiento del procedimiento de resolución de litigios cuando presenten una reclamación. Dicha información debe incluir un aviso sobre las prácticas de privacidad del mecanismo, de conformidad con los Principios. También deben cooperar en el desarrollo de herramientas, como formularios de reclamación estándar para facilitar el proceso de resolución de reclamaciones.

ii. Los mecanismos de recurso independientes deben incluir en sus sitios web públicos información relativa a los Principios y a los servicios que prestan en el marco del DPF UE-EE.UU.. Esta información debe incluir (1) información o un enlace a los requisitos de los Principios para los mecanismos de recurso independientes; (2) un enlace al sitio web del Marco de Privacidad de Datos del Departamento; (3) una explicación de que sus servicios de resolución de litigios en virtud del DPF UE-EE.UU. son gratuitos para los particulares; (4) una descripción de cómo se puede presentar una reclamación relacionada con los Principios; (5) el plazo en el que se tramitan las reclamaciones relacionadas con los Principios; y (6) una descripción de la gama de posibles soluciones.

iii. Los mecanismos de recurso independientes deben publicar un informe anual con estadísticas agregadas sobre sus servicios de resolución de litigios. El informe anual debe incluir: (1) el número total de reclamaciones relacionadas con los Principios recibidas durante el año del informe; (2) los tipos de reclamaciones recibidas; (3) las medidas de calidad de la resolución de conflictos, como el tiempo que se tarda en tramitar las reclamaciones; y (4) los resultados de las reclamaciones recibidas, en particular el número y los tipos de soluciones o sanciones impuestas.

iv. Tal y como se establece en el Anexo I, una persona tiene a su disposición una opción de arbitraje para determinar, en el caso de reclamaciones residuales, si una organización participante ha incumplido sus obligaciones en virtud de los Principios en lo que respecta a dicha persona, y si dicho incumplimiento sigue total o parcialmente sin subsanarse. Esta opción sólo está disponible para estos fines. Esta opción no está disponible, por ejemplo, con respecto a las excepciones a los Principios[15] o con respecto a una alegación sobre la adecuación del DPF UE-EEUU. En virtud de esta opción de arbitraje, el "Panel del Marco de Privacidad de Datos UE-EE.UU." (compuesto por uno o tres árbitros, según acuerden las partes) está facultado para imponer medidas equitativas no pecuniarias específicas para cada persona (como el acceso, la corrección, la supresión o la devolución de los datos de la persona en cuestión) necesarias para remediar la violación de los Principios únicamente con respecto a la persona. Los particulares y las organizaciones participantes podrán solicitar la revisión judicial y la ejecución de las decisiones arbitrales de conformidad con la legislación estadounidense en virtud de la Ley Federal de Arbitraje.

e) Recursos y sanciones

i. El resultado de cualquier reparación proporcionada por el organismo independiente de resolución de litigios debe ser que los efectos del incumplimiento sean revertidos o corregidos por la organización, en la medida de lo posible, y que el tratamiento futuro por parte de la organización sea conforme con los Principios y, en su caso, que el tratamiento de los datos personales de la persona que presentó la reclamación sea cesado. Las sanciones deben ser lo sufi-

15 Los Principios, Visión general, párr. 5.

cientemente rigurosas como para garantizar el cumplimiento de los Principios por parte de la organización. Una gama de sanciones de distintos grados de severidad permitirá a los organismos de resolución de litigios responder adecuadamente a los distintos grados de incumplimiento. Las sanciones deben incluir tanto la publicidad de los incumplimientos constatados como la obligación de suprimir los datos en determinadas circunstancias[16]. Otras sanciones podrían incluir la suspensión y retirada de un sello, la indemnización a los particulares por las pérdidas sufridas como consecuencia del incumplimiento y la imposición de medidas cautelares. Los organismos independientes de resolución de litigios del sector privado y los organismos de autorregulación deben notificar los incumplimientos de sus resoluciones por parte de las organizaciones participantes al organismo gubernamental con jurisdicción aplicable o a los tribunales, según proceda, y al Departamento.

f) Acción de la FTC

i. La FTC se ha comprometido a revisar con carácter prioritario las denuncias de incumplimiento de los Principios recibidas de: (i) organismos de autorregulación de la privacidad y otros organismos independientes de resolución de litigios; (ii) Estados miembros de la UE; y (iii) el Departamento, para determinar si se ha infringido el artículo 5 de la Ley FTC, que prohíbe los actos o prácticas desleales o engañosos en el comercio. Si la FTC llega a la conclusión de que tiene motivos para creer que se ha infringido el artículo 5, puede resolver el asunto solicitando una orden administrativa de cese y desistimiento que prohíba las prácticas impugnadas o presentando una denuncia ante un tribunal federal de distrito, que en caso de prosperar podría dar lugar a una orden judicial federal en el mismo sentido. Esto incluye afirmaciones falsas de adhesión a los Principios o de participación en el DPF UE-EE.UU. por parte de organizaciones que ya no figuran en la Lista del Marco de Privacidad de Datos o que nunca se han autocertificado ante el Departamento. La FTC puede obtener sanciones civiles por incumplimiento de una orden administrativa de cese y desistimiento y puede perseguir el desacato civil o penal por incumplimiento de una orden de un tribunal federal. La FTC notificará al Departamento cualquier acción de este tipo que emprenda. El Departamento anima a otros organismos gubernamentales a que le notifiquen la disposición final de cualquiera de dichas remisiones u otras resoluciones que determinen la adhesión a los Principios.

g) Incumplimiento persistente

i. Si una organización incumple persistentemente los Principios, ya no tendrá derecho a beneficiarse del DPF UE-EE.UU. Las organizaciones que hayan incumplido de forma persistente los Principios serán eliminadas de la Lista del Marco de Privacidad de Datos por el Departamento y deberán devolver o eliminar la información personal que hayan recibido en virtud del DPF UE- EE.UU.

ii. El incumplimiento persistente se produce cuando una organización que se ha autocertificado ante el Departamento se niega a cumplir una resolución definitiva de cualquier organismo de autorregulación de la privacidad, de resolución independiente de litigios o gubernamental, o cuando dicho organismo, incluido

16 Los organismos independientes de resolución de litigios tienen discreción sobre las circunstancias en las que utilizan estas sanciones. La sensibilidad de los datos en cuestión es un factor que debe tenerse en cuenta a la hora de decidir si debe exigirse la supresión de los datos, al igual que si una organización ha recopilado, utilizado o divulgado información contraviniendo flagrantemente los Principios.

el Departamento, determina que una organización incumple con frecuencia los Principios hasta el punto de que su pretensión de cumplirlos deje de ser creíble. En los casos en que tal determinación sea realizada por un organismo distinto del Departamento, la organización deberá notificar sin demora tales hechos al Departamento. El incumplimiento de esta obligación puede ser perseguible en virtud de la Ley de Declaraciones Falsas (18 U.S.C. § 1001). La retirada de una organización de un programa de autorregulación de la privacidad del sector privado o de un mecanismo independiente de resolución de litigios no la exime de su obligación de cumplir los Principios y constituiría un incumplimiento persistente.

iii. El Departamento retirará a una organización de la Lista Marco de Privacidad de Datos por incumplimiento persistente, incluso en respuesta a cualquier notificación que reciba de dicho incumplimiento por parte de la propia organización, un organismo autorregulador de la privacidad u otro organismo independiente de resolución de litigios, o un organismo gubernamental, pero sólo después de avisar previamente a la organización con 30 días de antelación y darle la oportunidad de responder[17]. En consecuencia, la Lista del Marco de Privacidad de Datos que mantiene el Departamento dejará claro qué organizaciones tienen garantizados los beneficios del DPF UE-EE.UU. y qué organizaciones han dejado de tenerlos.

iv. Una organización que solicite participar en un organismo de autorregulación a efectos de recalificación para el DPF UE- EE.UU. debe facilitar a dicho organismo información completa sobre su participación previa en el DPF UE-EE. UU. DPF ESTADOUNIDENSE.

12. Elección - Momento de la exclusión voluntaria

a) En general, el objetivo del principio de elección es garantizar que la información personal se utilice y divulgue de forma coherente con las expectativas y elecciones de la persona. En consecuencia, una persona debe poder ejercer la opción de "exclusión voluntaria" de la utilización de información personal para mercadotecnia directa en cualquier momento, con sujeción a límites razonables establecidos por la entidad, como dar tiempo a la entidad para hacer efectiva la exclusión voluntaria. Una organización también puede requerir información suficiente para confirmar la identidad del individuo que solicita la "exclusión voluntaria". En Estados Unidos, las personas pueden ejercer esta opción mediante el uso de un programa central de "exclusión voluntaria". En cualquier caso, la persona debe disponer de un mecanismo fácilmente accesible y asequible para ejercer esta opción.

b) Del mismo modo, una entidad puede utilizar información para determinados fines de marketing directo cuando no sea posible ofrecer a la persona la oportunidad de renunciar antes de utilizar la información, siempre que la entidad le ofrezca al mismo tiempo (y previa solicitud en cualquier momento) la oportunidad de negarse (sin coste alguno para la persona) a recibir más comunicaciones de marketing directo y la entidad cumpla los deseos de la persona.

13. Información sobre viajes

a) La información sobre reservas de pasajeros de líneas aéreas y otros datos de viaje, como la información sobre viajeros frecuentes o reservas de hotel y necesidades

17 El Departamento indicará en la notificación el plazo, que necesariamente será inferior a 30 días, de que dispone la organización para responder a la notificación.

especiales de gestión, como comidas para cumplir requisitos religiosos o asistencia física, puede transferirse a organizaciones situadas fuera de la UE en varias formas diferentes circunstancias. En virtud del RGPD, los datos personales pueden transferirse a un tercer país, en ausencia de una decisión de adecuación, si se proporcionan las garantías de protección de datos apropiadas de conformidad con el artículo 46 del RGPD o, en situaciones específicas, si se cumple una de las condiciones del artículo 49 del RGPD (por ejemplo, cuando el interesado haya consentido explícitamente la transferencia). Las organizaciones estadounidenses suscritas al DPF UE-EE.UU. proporcionan una protección adecuada de los datos personales y, por tanto, pueden recibir transferencias de datos de la UE sobre la base del artículo 45 del GDPR, sin tener que establecer un instrumento de transferencia de conformidad con el artículo 46 del GDPR o cumplir las condiciones del artículo 49 del GDPR. Dado que el DPF UE-EE.UU. incluye normas específicas para la información sensible, dicha información (que puede ser necesario recopilar, por ejemplo, en relación con las necesidades de asistencia física de los clientes) puede incluirse en las transferencias a las organizaciones participantes. En todos los casos, sin embargo, la organización que transfiere la información tiene que respetar la legislación del Estado miembro de la UE en el que opera, que puede, entre otras cosas, imponer condiciones especiales para el tratamiento de datos sensibles.

14. Productos farmacéuticos y médicos

a) Aplicación de la legislación de la UE/Estados miembros o de los Principios

i. La legislación de la UE/Estado miembro se aplica a la recogida de los datos personales y a cualquier tratamiento que tenga lugar antes de la transferencia a Estados Unidos. Los Principios se aplican a los datos una vez transferidos a Estados Unidos. Los datos utilizados para la investigación farmacéutica y otros fines deben ser anónimos cuando proceda.

b) Futura investigación científica

i. Los datos personales obtenidos en estudios específicos de investigación médica o farmacéutica suelen desempeñar un valioso papel en futuras investigaciones científicas. Cuando los datos personales recogidos para un estudio de investigación se transfieren a una organización de EE.UU. en el DPF UE-EE.UU., la organización puede utilizar los datos para una nueva actividad de investigación científica si se ha proporcionado la notificación y la opción adecuadas en primera instancia. Dicha notificación debe proporcionar información sobre cualquier uso específico futuro de los datos, como seguimiento periódico, estudios relacionados o comercialización.

ii. Se entiende que no se pueden especificar todos los usos futuros de los datos, ya que podría surgir un nuevo uso de investigación a partir de nuevos conocimientos sobre los datos originales, nuevos descubrimientos y avances médicos y novedades en materia de salud pública y reglamentación. Por lo tanto, cuando proceda, la notificación deberá incluir una explicación de que los datos personales pueden utilizarse en futuras actividades de investigación médica y farmacéutica no previstas. Si el uso no es coherente con la finalidad o finalidades generales de investigación para las que se recogieron originalmente los datos personales, o para las que la persona ha dado su consentimiento posteriormente, deberá obtenerse un nuevo consentimiento.

c) Retirada de un ensayo clínico

i. Los participantes pueden decidir retirarse de un ensayo clínico o se les puede pedir que lo hagan en cualquier momento. Los datos personales recogidos antes de la retirada podrán seguir tratándose junto con otros datos recogidos

como parte del ensayo clínico, sin embargo, si esto se dejó claro al participante en el aviso en el momento en que aceptó participar.

d) Transferencias con fines de regulación y supervisión

i. Las empresas farmacéuticas y de productos sanitarios están autorizadas a facilitar datos personales de ensayos clínicos realizados en la UE a los organismos reguladores de Estados Unidos con fines de regulación y supervisión. Se permiten transferencias similares a partes distintas de los reguladores, como sedes de empresas y otros investigadores, en consonancia con los Principios de Notificación y Elección.

e) Estudios "a ciegas

i. Para garantizar la objetividad en muchos ensayos clínicos, los participantes, y a menudo también los investigadores, no pueden tener acceso a información sobre qué tratamiento puede estar recibiendo cada participante. Hacerlo pondría en peligro la validez del estudio de investigación y sus resultados. Los participantes en dichos ensayos clínicos (denominados estudios "ciegos") no tienen que tener acceso a los datos sobre su tratamiento durante el ensayo si esta restricción se ha explicado cuando el participante entró en el ensayo y la divulgación de dicha información pondría en peligro la integridad de la investigación.

ii. Aceptar participar en el ensayo en estas condiciones es una renuncia razonable al derecho de acceso. Tras la conclusión del ensayo y el análisis de los resultados, los participantes deben tener acceso a sus datos si lo solicitan. Deben solicitarlo en primer lugar al médico u otro proveedor de atención sanitaria del que recibieron tratamiento dentro del ensayo clínico o, en segundo lugar, a la organización patrocinadora.

f) Control de la seguridad y eficacia de los productos

i. Una empresa farmacéutica o de productos sanitarios no está obligada a aplicar los Principios relativos a los Principios de Notificación, Elección, Responsabilidad por la Transferencia ulterior y Acceso en sus actividades de supervisión de la seguridad y eficacia de sus productos, incluida la notificación de acontecimientos adversos y el seguimiento de pacientes/sujetos que utilicen determinados medicamentos o productos sanitarios, en la medida en que la adhesión a los Principios interfiera con el cumplimiento de los requisitos reglamentarios. Esto es cierto tanto con respecto a los informes de, por ejemplo, los proveedores de atención sanitaria a las empresas farmacéuticas y de productos sanitarios, como con respecto a los informes de las empresas farmacéuticas y de productos sanitarios a organismos gubernamentales como la Administración de Alimentos y Medicamentos.

g) Datos codificados

i. Invariablemente, los datos de la investigación son codificados con una clave única en su origen por el investigador principal para no revelar la identidad de los sujetos individuales de los datos. Las empresas farmacéuticas que patrocinan estas investigaciones no reciben la clave. El investigador es el único que posee el código clave único para poder identificar al sujeto de la investigación en circunstancias especiales (por ejemplo, si se requiere atención médica de seguimiento). Una transferencia de la UE a Estados Unidos de datos codificados de esta manera que sean datos personales de la UE según la legislación de la UE estaría cubierta por los Principios.

15. Registros públicos e información de dominio público

a) Una organización debe aplicar los Principios de Seguridad, Integridad de los Datos y Limitación de Finalidad, y Recurso, Cumplimiento y Responsabilidad a los datos personales procedentes de fuentes de acceso público. Estos Principios se aplicarán también a los datos personales recogidos de registros públicos (es decir, aquellos registros conservados por organismos o entidades gubernamentales de cualquier nivel que estén abiertos a la consulta del público en general).

b) No es necesario aplicar los Principios de notificación, elección o responsabilidad en las transferencias ulteriores a la información de dominio público, siempre que no se combine con información de dominio no público y se respeten las condiciones de consulta establecidas por la jurisdicción pertinente. Asimismo, por lo general no es necesario aplicar los Principios de notificación, elección o responsabilidad en las transferencias ulteriores a la información de dominio público, a menos que el cedente europeo indique que dicha información está sujeta a restricciones que exigen la aplicación de dichos Principios por parte de la entidad para los usos que pretende. Las entidades no serán responsables del uso que hagan de dicha información quienes la obtengan a partir de material publicado.

c) Si se descubre que una organización ha hecho pública intencionadamente información personal contraviniendo los Principios para que ella u otros puedan beneficiarse de estas excepciones, dejará de poder acogerse a los beneficios del DPF UE-EE.UU.

d) No es necesario aplicar el Principio de Acceso a la información de los registros públicos siempre que no se combine con otra información personal (aparte de las pequeñas cantidades utilizadas para indexar u organizar la información de los registros públicos); sin embargo, deben respetarse todas las condiciones de consulta establecidas por la jurisdicción pertinente. Por el contrario, cuando la información de los registros públicos se combina con otra información de registros no públicos (distinta de la indicada específicamente más arriba), una entidad debe proporcionar acceso a toda esa información, suponiendo que no esté sujeta a otras excepciones permitidas.

e) Al igual que ocurre con la información de los registros públicos, no es necesario facilitar el acceso a la información que ya está a disposición del público en general, siempre que no se combine con información no disponible públicamente. Las organizaciones que se dedican a la venta de información de acceso público pueden cobrar la tarifa habitual de la organización para responder a las solicitudes de acceso. Alternativamente, los particulares pueden solicitar el acceso a su información a la organización que recopiló originalmente los datos.

16. Solicitudes de acceso de las autoridades públicas

– Con el fin de proporcionar transparencia con respecto a las solicitudes legales de acceso a información personal por parte de las autoridades públicas, las organizaciones participantes podrán emitir voluntariamente informes periódicos de transparencia sobre el número de solicitudes de información personal que reciban por parte de las autoridades públicas por motivos policiales o de seguridad nacional, en la medida en que dichas divulgaciones estén permitidas por la legislación aplicable.

– La información proporcionada por las organizaciones participantes en estos informes junto con la información que ha sido publicada por la comunidad de inteligencia, junto con otra información, puede ser utilizada para la revisión periódica conjunta del funcionamiento del DPF UE-EE.UU. de conformidad con los Principios.

– La ausencia de notificación de conformidad con el punto (a)(xii) del Principio de Notificación no impedirá ni menoscabará la capacidad de una organización para responder a cualquier solicitud lícita.

ANEXO I: MODELO ARBITRAL

El presente Anexo I establece las condiciones en las que las organizaciones que participan en el DPF UE-EE.UU. están obligadas a arbitrar las reclamaciones, de conformidad con el principio de recurso, ejecución y responsabilidad. La opción de arbitraje vinculante que se describe a continuación se aplica a determinadas reclamaciones "residuales" relativas a datos cubiertos por el DPF UE-EE.UU.. El propósito de esta opción es proporcionar un mecanismo rápido, independiente y justo, a elección de los particulares, para la resolución de cualquier reclamación por violación de los Principios que no haya sido resuelta por ninguno de los otros mecanismos del DPF UE-EE.UU.

A. Alcance

Esta opción de arbitraje está a disposición de una persona para determinar, en el caso de reclamaciones residuales, si una organización participante ha incumplido sus obligaciones en virtud de los Principios en lo que respecta a dicha persona, y si dicho incumplimiento sigue total o parcialmente sin subsanarse. Esta opción sólo está disponible para estos fines. Esta opción no está disponible, por ejemplo, con respecto a las excepciones a los Principios[18] o con respecto a una alegación sobre la adecuación del DPF UE-EEUU.

B. Remedios disponibles

Con arreglo a esta opción de arbitraje, el "Panel del Marco de Privacidad de Datos UE-EE.UU." (el panel de arbitraje compuesto por uno o tres árbitros, según acuerden las partes) está facultado para imponer reparaciones equitativas no monetarias y específicas para cada persona (como el acceso, la corrección, la supresión o la devolución de los datos de la persona en cuestión) necesarias para remediar la violación de los Principios sólo con respecto a la persona. Éstas son las únicas competencias del Grupo de expertos UE-EE.UU. sobre privacidad de los datos en materia de recursos. Al considerar las soluciones, el Panel del Marco de Privacidad de Datos UE-EE. UU. está obligado a considerar otras soluciones que ya hayan sido impuestas por otros mecanismos en virtud del DPF UE-EE.UU.. No se impondrán indemnizaciones por daños y perjuicios, costas, honorarios u otros recursos disponibles. Cada parte se hace cargo de sus propios honorarios de abogado.

C. Requisitos previos al arbitraje

Una persona que decida acogerse a esta opción de arbitraje debe dar los siguientes pasos antes de iniciar una reclamación de arbitraje: (1) plantear la infracción reclamada directamente a la organización y dar a ésta la oportunidad de resolver la cuestión dentro del plazo establecido en la sección (d)(i) del Principio Complementario sobre Resolución de Litigios y Ejecución; (2) hacer uso del mecanismo de recurso independiente previsto en los Principios, sin coste alguno para el particular; y (3) plantear la cuestión al Departamento a través del APD del particular y dar al Departamento la oportunidad de hacer todo lo posible por resolver la cuestión dentro de los plazos establecidos en la carta de la Administración de Comercio Internacional del Departamento, sin coste alguno para el particular.

18 Los Principios, Visión general, párr. 5.

Esta opción de arbitraje no podrá invocarse si la misma infracción de los Principios alegada por el particular (1) ha sido previamente objeto de arbitraje vinculante; (2) fue objeto de una sentencia firme dictada en una acción judicial en la que el particular era parte; o (3) fue previamente resuelta por las partes. Además, esta opción no podrá invocarse si un APD (1) tiene autoridad en virtud del Principio Suplementario sobre la Función de las Autoridades de Protección de Datos o del Principio Suplementario sobre Datos de Recursos Humanos; o (2) tiene autoridad para resolver la violación reclamada directamente con la organización. La autoridad de una APD para resolver la misma reclamación contra un responsable del tratamiento de datos de la UE no impide por sí sola invocar esta opción de arbitraje contra una entidad jurídica diferente no vinculada por la autoridad de la APD.

D. Carácter vinculante de las decisiones

La decisión de una persona de acogerse a esta opción de arbitraje vinculante es totalmente voluntaria. Las decisiones arbitrales serán vinculantes para todas las partes del arbitraje. Una vez invocada, la persona renuncia a la opción de solicitar reparación por la misma infracción alegada en otro foro, excepto si no se ha invocado la opción de arbitraje.

Si la compensación monetaria equitativa no remedia completamente la violación reclamada, la invocación del arbitraje por parte del particular no impedirá una reclamación por daños y perjuicios que, de otro modo, estaría disponible en los tribunales.

E. Revisión y aplicación

Los particulares y las organizaciones participantes podrán solicitar la revisión judicial y la ejecución de las decisiones arbitrales de conformidad con la legislación estadounidense, en virtud de la Ley Federal de Arbitraje[19] Dichos casos deberán presentarse ante el tribunal federal de distrito cuyo ámbito territorial incluya la sede principal de la organización participante.

---

19 El capítulo 2 de la Ley Federal de Arbitraje ("FAA") establece que "[u]n acuerdo de arbitraje o laudo arbitral derivado de una relación jurídica, contractual o no, que se considere comercial, incluida una transacción, contrato o acuerdo descrito en [el artículo 2 de la FAA], entra dentro del ámbito de aplicación de la Convención [sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras de 10 de junio de 1958, 21 U.S.T. 2519, T.I.A.S. nº 6997 ("Convención de Nueva York")]". 9 U.S.C. § 202. La FAA establece además que "[s]e considerará que un acuerdo o laudo derivado de dicha relación que se celebre íntegramente entre ciudadanos de los Estados Unidos no está comprendido en el ámbito de aplicación de la Convención [de Nueva York], a menos que dicha relación afecte a bienes situados en el extranjero, prevea su cumplimiento o ejecución en el extranjero, o tenga alguna otra relación razonable con uno o más Estados extranjeros". Id. Conforme al Capítulo 2, "cualquiera de las partes en el arbitraje podrá solicitar a cualquier tribunal competente en virtud de este capítulo una orden que confirme el laudo frente a cualquier otra parte en el arbitraje. El tribunal confirmará el laudo a menos que encuentre uno de los motivos para denegar o aplazar el reconocimiento o la ejecución del laudo especificados en dicha Convención [de Nueva York]." Id. § 207. El Capítulo 2 dispone además que "[l]os tribunales de distrito de los Estados Unidos . . tendrán jurisdicción original sobre ... una acción o procedimiento [bajo la Convención de Nueva York], independientemente del monto en controversia". Id. § 203. El capítulo 2 también establece que "el capítulo 1 se aplica a las acciones y procedimientos iniciados en virtud de este capítulo en la medida en que dicho capítulo no esté en conflicto con este capítulo o con la Convención [de Nueva York] ratificada por Estados Unidos". Id. § 208. El Capítulo 1, a su vez, establece que "[una] disposición escrita en ...

Esta opción de arbitraje está pensada para resolver disputas individuales, y las decisiones arbitrales no pretenden funcionar como precedente persuasivo o vinculante en asuntos que impliquen a otras partes, incluidos futuros arbitrajes o en tribunales de la UE o EE.UU., o procedimientos de la FTC.

F. El panel arbitral

Las partes seleccionarán a los árbitros del Grupo de expertos UE-EE.UU. sobre protección de datos de la lista de árbitros que se expone a continuación.

De conformidad con la legislación aplicable, el Departamento y la Comisión elaborarán una lista de al menos 10 árbitros, elegidos en función de su independencia, integridad y experiencia. En relación con este proceso se aplicará lo siguiente:

Árbitros:

1. permanecerán en la lista por un periodo de 3 años, salvo circunstancias excepcionales o cese por causa justificada, renovable por el Departamento, previa notificación a la Comisión, por periodos adicionales de 3 años;
2. no estará sujeta a instrucciones de ninguna de las partes, ni de ninguna organización participante, ni de EE.UU., la UE o cualquier Estado miembro de la UE, ni de ninguna otra autoridad gubernamental, autoridad pública o autoridad encargada de hacer cumplir la ley, ni estará afiliada a ninguna de ellas; y
3. deben estar habilitados para ejercer la abogacía en Estados Unidos y ser expertos en la legislación estadounidense sobre privacidad, con conocimientos especializados en la legislación de la UE sobre protección de datos.

G. Procedimientos de arbitraje

El Departamento y la Comisión han acordado, de conformidad con la legislación aplicable, la adopción de las normas de arbitraje que rigen los procedimientos ante el Panel Marco de Privacidad de Datos UE-EE.UU.[20]. En caso de que sea necesario modificar las normas que rigen los procedimientos, el Departamento y la Comisión

---

un contrato que evidencie una transacción que involucre comercio para resolver mediante arbitraje una controversia que surja posteriormente de dicho contrato o transacción, o la negativa a cumplir la totalidad o cualquier parte del mismo, o un acuerdo por escrito para someter a arbitraje una controversia existente que surja de dicho contrato, transacción o negativa, será válido, irrevocable y exigible, salvo por las causales que existan en derecho o en equidad para la revocación de cualquier contrato". Id. § 2. El capítulo 1 establece además que "cualquiera de las partes en el arbitraje puede solicitar al tribunal así especificado una orden que confirme el laudo, y a partir de ese momento el tribunal debe conceder dicha orden a menos que el laudo sea anulado, modificado o corregido según lo prescrito en las secciones 10 y 11 de [la FAA]". Id. § 9.

20 El Centro Internacional para la Resolución de Disputas ("ICDR", por sus siglas en inglés), la división internacional de la Asociación Americana de Arbitraje ("AAA", por sus siglas en inglés) (colectivamente "ICDR- AAA"), fue seleccionado por el Departamento para administrar arbitrajes de conformidad con y gestionar el fondo arbitral identificado en el Anexo I de los Principios. El 15 de septiembre de 2017, el Departamento y la Comisión acordaron la adopción de un conjunto de reglas de arbitraje para regir los procedimientos de arbitraje vinculante descritos en el Anexo I de los Principios, así como un código de conducta para los árbitros que es coherente con las normas éticas generalmente aceptadas para los árbitros comerciales y el Anexo I de los Principios. El Departamento y la Comisión acordaron

acordarán modificar dichas normas o adoptar un conjunto diferente de procedimientos de arbitraje existentes y bien establecidos en EE.UU., según proceda, con sujeción a cada una de las siguientes consideraciones:

1. Un particular puede iniciar un arbitraje vinculante, sujeto a la disposición sobre los requisitos previos al arbitraje, mediante la entrega de una "Notificación" a la organización. La notificación contendrá un resumen de las medidas adoptadas en virtud del apartado C para resolver la reclamación, una descripción de la supuesta infracción y, a elección del interesado, los documentos y materiales justificativos y/o un análisis de la legislación relativa a la supuesta reclamación.
2. Se desarrollarán procedimientos para garantizar que la misma infracción alegada por un individuo no reciba remedios o procedimientos duplicados.
3. La acción de la FTC puede proceder paralelamente al arbitraje.
4. Ningún representante de los EE.UU., la UE o cualquier Estado miembro de la UE o cualquier otra autoridad gubernamental, autoridad pública o autoridad de aplicación podrá participar en estos arbitrajes, siempre que, a petición de un particular de la UE, los APD puedan prestar asistencia en la preparación únicamente de la Notificación, pero los APD no podrán tener acceso a la proposición de prueba ni a ningún otro material relacionado con estos arbitrajes.
5. La sede del arbitraje será Estados Unidos, y la persona podrá optar por la participación por vídeo o teléfono, que se facilitará sin coste alguno para la persona. No será necesaria la participación en persona.
6. El idioma del arbitraje será el inglés, salvo acuerdo en contrario de las partes. Previa solicitud motivada, y teniendo en cuenta si el particular está representado por un abogado, se proporcionará interpretación en la audiencia arbitral, así como traducción de los materiales arbitrales, sin coste alguno para el particular, a menos que el Panel del Marco de Privacidad de Datos UE-EE.UU. considere que, en las circunstancias del arbitraje específico, ello daría lugar a costes injustificados o desproporcionados.
7. Los materiales presentados a los árbitros se tratarán confidencialmente y sólo se utilizarán en relación con el arbitraje.
8. En caso necesario, se autorizará la presentación de pruebas específicas individuales, que las partes tratarán confidencialmente y sólo se utilizarán en relación con el arbitraje.
9. Los arbitrajes deben completarse en un plazo de 90 días a partir de la entrega de la Notificación a la organización en cuestión, salvo que las partes acuerden otra cosa.

H. Costes

Los árbitros deben tomar medidas razonables para minimizar los costes u honorarios de los arbitrajes.

El Departamento, en consonancia con la legislación aplicable, facilitará el mantenimiento de un fondo, al que las organizaciones participantes deberán contribuir, basándose en parte en el tamaño de la organización, que cubrirá el coste del arbi-

adaptar el reglamento de arbitraje y el código de conducta para reflejar las actualizaciones en el marco de la UE-UE. UU, y el Departamento trabajará con la ICDR-AAA para realizar esas actualizaciones.

traje, incluidos los honorarios del árbitro, hasta unos importes máximos ("topes"). El fondo será gestionado por un tercero, que informará periódicamente al Departamento sobre las operaciones del fondo. El Departamento trabajará con el tercero para revisar periódicamente el funcionamiento del fondo, incluida la necesidad de ajustar el importe de las contribuciones o de los topes del coste arbitral, y considerar, entre otras cosas, el número de arbitrajes y los costes y el calendario de los arbitrajes, en el entendimiento de que no se impondrá una carga financiera excesiva a las organizaciones participantes. El Departamento notificará a la Comisión el resultado de dichas revisiones con el tercero y le comunicará previamente cualquier ajuste del importe de las contribuciones. Los honorarios de los abogados no están cubiertos por esta disposición ni por ningún fondo de esta disposición.

ANEXO II



DEPARTAMENTO DE COMERCIO
DE LOS ESTADOS UNIDOS
Secretario de Comercio
Washington, D.C. 20230

6 de julio de 2023

Honorable Didier Reynders
Comisario de Justicia Comisión Europea
Rue de la Loi/ Westraat 200 1049 Bruselas
Bélgica

Estimado Comisario Reynders:

En nombre de los Estados Unidos, me complace transmitir adjunto un paquete de materiales del Marco de Privacidad de Datos UE-EE.UU. que, combinado con la Orden Ejecutiva 14086, "Mejora de las Salvaguardias para las Actividades de Inteligencia de Señales de los Estados Unidos" y 28 CFR parte 201 que modifica los reglamentos del Departamento de Justicia para establecer el "Tribunal de Revisión de Protección de Datos", refleja negociaciones importantes y detalladas para reforzar la protección de la privacidad y las libertades civiles.

Estas negociaciones han dado lugar a nuevas salvaguardias para garantizar que las actividades de inteligencia de señales de EE.UU. sean necesarias y proporcionadas para la consecución de los objetivos de seguridad nacional definidos y a un nuevo mecanismo para que las personas de la Unión Europea ("UE") puedan obtener reparación si creen que son objeto ilegal de actividades de inteligencia de señales, lo que en conjunto garantizará la privacidad de los datos personales de la UE. El marco de privacidad de datos UE-EE.UU. sustentará una economía digital integradora y competitiva. Ambos debemos estar orgullosos de las mejoras reflejadas en dicho Marco, que mejorará la protección de la privacidad en todo el mundo. Este paquete, junto con la Orden Ejecutiva, los Reglamentos y otros materiales disponibles en fuentes públicas, proporciona una base muy sólida para una nueva constatación de adecuación por parte de la Comisión Europea[1].

Se adjunta el siguiente material:

- Los Principios Marco de Privacidad de Datos UE-EE.UU., incluidos los Principios Suplementarios (colectivamente "los Principios") y el Anexo I de los Principios (es decir, un anexo que establece los términos en los que las orga-

1 Siempre que la Decisión de la Comisión sobre la adecuación de la protección proporcionada por el Marco de Protección de Datos UE-EE.UU. se aplique a Islandia, Liechtenstein y Noruega, el Paquete Marco de Protección de Datos de UE-EE.UU. abarcará tanto a la Unión Europea como a estos tres países.

nizaciones del Marco de Privacidad de Datos están obligadas a arbitrar ciertas reclamaciones residuales en cuanto a datos personales cubiertos por los Principios);

- Una carta de la Administración de Comercio Internacional del Departamento, que administra el programa del Marco de Privacidad de Datos, en la que se describen los compromisos que nuestro Departamento ha asumido para garantizar que el Marco de Privacidad de Datos UE-EE.UU. funcione eficazmente;
- Una carta de la Comisión Federal de Comercio en la que se describe su aplicación de los Principios;
- Una carta del Departamento de Transporte en la que se describe su aplicación de los Principios;
- Una carta preparada por la Oficina del Director de Inteligencia Nacional sobre las salvaguardias y limitaciones aplicables a las autoridades de seguridad nacional de EE.UU.; y
- Una carta preparada por el Departamento de Justicia en relación con las salvaguardias y limitaciones sobre acceso del Gobierno de EE.UU. con fines policiales y de interés público.

El paquete completo del Marco de Privacidad de Datos UE-EE.UU. se publicará en el sitio web del Marco de Privacidad de Datos del Departamento y los Principios y el Anexo I de los Principios serán efectivos en la fecha de entrada en vigor de la decisión de adecuación de la Comisión Europea.

Puede estar seguro de que Estados Unidos se toma en serio estos compromisos. Estamos deseando trabajar con ustedes en la aplicación del Marco de Privacidad de Datos UE-EE.UU. y embarcarnos juntos en la siguiente fase de este proceso.

Atentamente,

Gina M. Raimondo

ANEXO III



UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D.C. 20230

12 de diciembre de 2022

Honorable Didier Reynders
Comisario de Justicia Comisión Europea
Rue de la Loi/Westraat 200 1049 Bruselas
Bélgica

Estimado Comisario Reynders:

En nombre de la Administración de Comercio Internacional ("ACI"), me complace describir los compromisos que el Departamento de Comercio ("el Departamento") ha asumido para garantizar la protección de los datos personales a través de su administración y supervisión del programa Marco de Privacidad de Datos. La finalización del Marco de Privacidad de Datos UE-EE.UU. ("MPD UE-EE.UU.") es un logro importante para la privacidad y para las empresas de ambos lados del Atlántico, ya que ofrecerá confianza a las personas de la UE de que sus datos estarán protegidos y de que dispondrán de recursos legales para abordar las preocupaciones relacionadas con sus datos, y permitirá a miles de empresas seguir invirtiendo y participando en el comercio a través del Atlántico en beneficio de nuestras respectivas economías y ciudadanos. El DPF UE-EE.UU. refleja años de duro trabajo y colaboración con usted y sus colegas de la Comisión Europea ("la Comisión"). Esperamos seguir trabajando con la Comisión para garantizar que este esfuerzo de colaboración funcione eficazmente.

El DPF UE-EE.UU. reportará importantes beneficios tanto a los particulares como a las empresas. En primer lugar, proporciona un importante conjunto de protecciones de la intimidad para los datos de las personas de la UE transferidos a Estados Unidos. Exige que las organizaciones estadounidenses participantes desarrollen una política de privacidad conforme; se comprometan públicamente a cumplir los "Principios del Marco de Privacidad de Datos UE-EE.UU.", incluidos los Principios Suplementarios (colectivamente "los Principios"), y el Anexo I de los Principios (es decir, un anexo en el que se establecen las condiciones en las que los Estados miembros de la UE podrán aplicar los Principios). Las organizaciones de DPF de EE.UU. están obligadas a arbitrar ciertas reclamaciones residuales en relación con los datos personales cubiertos por los Principios), de modo que el compromiso sea exigible en virtud de la legislación estadounidense[1]; volver a certificar anualmente su cumplimiento ante

1 Las organizaciones que autocertificaron su compromiso de cumplir los Principios del Marco del Escudo de Privacidad UE-EE.UU. y desean disfrutar de las ventajas de par-

el Departamento; proporcionar un servicio gratuito e independiente de resolución de conflictos a particulares de la UE; y estar sujetos a la autoridad de investigación y ejecución de un Organismo legal estadounidense enumerado en los Principios (por ejemplo, la Comisión Federal de Comercio (la "FTC") y el Departamento de Transporte (el "DOT")), o un organismo legal estadounidense enumerado en un futuro anexo a los Principios. Si bien la decisión de una organización de autocertificarse es voluntaria, una vez que una organización se compromete públicamente con el DPF UE-EE. UU., su compromiso es exigible en virtud de la legislación estadounidense por la FTC, el DOT u otro organismo legal de EE.UU., dependiendo de qué organismo tenga jurisdicción sobre la organización participante. En segundo lugar, el DPF UE- EE.UU. permitirá a las empresas de Estados Unidos, incluidas las filiales de empresas europeas ubicadas en Estados Unidos, recibir datos personales de la Unión Europea para facilitar los flujos de datos que apoyan el comercio transatlántico. Los flujos de datos entre Estados Unidos y la Unión Europea son los mayores del mundo y sustentan la relación económica de 7,1 billones de dólares entre Estados Unidos y la UE, que mantiene millones de puestos de trabajo a ambos lados del Atlántico. Las empresas que dependen de los flujos de datos transatlánticos proceden de todos los sectores industriales e incluyen a las principales empresas de Fortune 500, así como a muchas pequeñas y medianas empresas. Los flujos de datos transatlánticos permiten a las organizaciones estadounidenses procesar los datos necesarios para ofrecer bienes, servicios y oportunidades de empleo a las personas europeas.

El Departamento se ha comprometido a colaborar estrecha y productivamente con nuestros homólogos de la UE para administrar y supervisar eficazmente el programa del Marco de Protección de Datos. Este compromiso se refleja en el desarrollo y perfeccionamiento continuo por parte del Departamento de una serie de recursos para ayudar a las organizaciones con el proceso de autocertificación, la creación de un sitio web para proporcionar información específica a las partes interesadas, la colaboración con la Comisión y las autoridades europeas de protección de datos ("DPA") para desarrollar directrices que aclaren elementos importantes del DPF UE-EE.UU., la divulgación para facilitar una mayor comprensión de las obligaciones de protección de datos de las organizaciones, y la supervisión y el seguimiento del cumplimiento de los requisitos del programa por parte de las organizaciones.

Nuestra cooperación permanente con nuestros valiosos homólogos de la UE permitirá al Departamento garantizar que el DPF UE-EE.UU. funcione eficazmente. El Gobierno de los Estados Unidos tiene un largo historial de colaboración con la Comisión para promover principios comunes de protección de datos, salvando las diferencias entre nuestros respectivos enfoques jurídicos y fomentando al mismo tiempo el comercio y el crecimiento económico en la Unión Europea y los Estados Unidos. Creemos que el DPF UE-EE.UU., que es un ejemplo de esta cooperación, permitirá a la Comisión emitir una nueva decisión de adecuación que permitirá a las organizaciones utilizar el DPF UE-EE.UU. para transferir datos personales de la Unión Europea a Estados Unidos de forma coherente con la legislación de la UE.

---

ticipar en el DPF UE-EE.UU. deben cumplir los "Principios del Marco de Privacidad de Datos UE-EE.UU.". Este compromiso de cumplimiento de los "Principios del marco de privacidad de datos UE-EE.UU. Principios" se reflejarán en las políticas de privacidad de dichas organizaciones participantes lo antes posible y, en cualquier caso, a más tardar tres meses después de la fecha de entrada en vigor de los "Principios del Marco de Privacidad de Datos UE-EE.UU.". (Véase la sección (e) del Principio Suplementario sobre Autocertificación).

Administración y supervisión del Programa Marco de Privacidad de Datos por el Departamento de Comercio

El Departamento está firmemente comprometido con la administración y supervisión efectivas del programa Marco de Privacidad de Datos y emprenderá los esfuerzos y dedicará los recursos adecuados para garantizar ese resultado. El Departamento mantendrá y pondrá a disposición del público una lista autorizada de organizaciones estadounidenses que se han autocertificado ante el Departamento y han declarado su compromiso de adherirse a los Principios ("la Lista del Marco de Privacidad de Datos"), que actualizará sobre la base de las presentaciones anuales de recertificación realizadas por las organizaciones participantes y mediante la eliminación de organizaciones cuando se retiren voluntariamente, no completen la recertificación anual de conformidad con los procedimientos del Departamento, o se compruebe que incumplen persistentemente. El Departamento también mantendrá y pondrá a disposición del público un registro autorizado de las organizaciones estadounidenses que hayan sido eliminadas de la Lista Marco de Privacidad de Datos e identificará la razón por la que cada organización fue eliminada. La lista autorizada y el registro mencionados permanecerán a disposición del público en el sitio web de la Comisión Europea.

El sitio web del Marco de Privacidad de Datos del Departamento. El sitio web del Marco de protección de la intimidad de los datos incluirá una explicación en un lugar destacado en la que se indicará que cualquier organización eliminada de la Lista del Marco de protección de la intimidad de los datos debe dejar de afirmar que participa en el DPF UE-EE.UU. o que lo cumple, y que puede recibir información personal en virtud del DPF UE-EE.UU.. No obstante, dicha organización deberá seguir aplicando los Principios a la información personal que haya recibido mientras participaba en el DPF UE-EE.UU. mientras conserve dicha información. El Departamento, en cumplimiento de su compromiso global y permanente con la administración y supervisión eficaces del programa del Marco de Privacidad de Datos, se compromete específicamente a hacer lo siguiente:

Verificar los requisitos de autocertificación

- El Departamento, antes de finalizar la autocertificación inicial o la recertificación anual de una organización (colectivamente "autocertificación") y de incluir o mantener a una organización en la Lista Marco de Privacidad de Datos, verificará que la organización ha cumplido, como mínimo, los requisitos pertinentes establecidos en el Principio Suplementario sobre Autocertificación relativos a la información que una organización debe proporcionar en su presentación de autocertificación al Departamento y ha proporcionado en el momento oportuno una política de privacidad pertinente que informa a las personas sobre los 13 elementos enumerados establecidos en el Principio de Notificación. El Departamento verificará que la organización
  - identificó a la organización que presenta su autocertificación, así como a cualquier entidad estadounidense o filial estadounidense de la organización autocertificante que también se adhiera a los Principios que la organización desea que queden cubiertos por su autocertificación;
  - proporcionó la información de contacto de la organización requerida (por ejemplo, información de contacto de la(s) persona(s) y/o oficina(s) específica(s) dentro de la organización autocertificante responsable(s) de tramitar las reclamaciones, las solicitudes de acceso y cualquier otra cuestión que surja en el marco del DPF UE-EE.UU.);
  - describió la finalidad o finalidades para las que la organización recogería y utilizaría la información personal recibida de la Unión Europea;

- indicó qué información personal recibiría de la Unión Europea en virtud del DPF UE-EE.UU. y, por tanto, estaría cubierta por su autocertificación;
- si la organización tiene un sitio web público, facilitó la dirección web en la que la política de privacidad pertinente está fácilmente disponible en ese sitio web, o si la organización no tiene un sitio web público, facilitó al Departamento una copia de la política de privacidad pertinente y el lugar en el que esa política de privacidad está disponible para que la consulten las personas afectadas (es decir, los empleados afectados si la política de privacidad pertinente es una política de privacidad de recursos humanos o el público si la política de privacidad pertinente no es una política de privacidad de recursos humanos);
- incluir en su política de privacidad pertinente en el momento adecuado (es decir, inicialmente sólo en un borrador de política de privacidad proporcionado junto con la presentación si dicha presentación es una autocertificación inicial; de lo contrario, en una política de privacidad final y, en su caso, publicada) una declaración de que se adhiere a los Principios y un hipervínculo o la dirección web del sitio web del Marco de Privacidad de Datos del Departamento (por ejemplo, la página de inicio o la página web de la Lista del Marco de Privacidad de Datos);
- incluyó en su política de privacidad pertinente, en el momento oportuno, todos los otros 12 elementos enumerados establecidos en el Principio de Notificación (por ejemplo, la posibilidad, en determinadas condiciones, de que la persona afectada de la UE invoque un arbitraje vinculante; el requisito de revelar información personal en respuesta a solicitudes legales de las autoridades públicas, incluso para cumplir requisitos de seguridad nacional o de aplicación de la ley; y su responsabilidad en casos de transferencias ulteriores a terceros);
- identificó el órgano estatutario específico que tiene jurisdicción para conocer de cualquier reclamación contra la organización en relación con posibles prácticas desleales o engañosas y violaciones de leyes o normativas que regulen la privacidad (y que figure en los Principios o en un futuro anexo a los Principios);
- identificado cualquier programa de privacidad en el que la organización sea miembro;
- identificó si el método pertinente (es decir, los procedimientos de seguimiento que debe proporcionar) para verificar su cumplimiento de los Principios es la "autoevaluación" (es decir, la verificación interna) o la "revisión externa del cumplimiento" (es decir, la verificación por terceros) y, si identificó el método pertinente como revisión externa del cumplimiento, también identificó al tercero que ha completado esa revisión;
- identificó el mecanismo de recurso independiente adecuado que está disponible para tratar las quejas presentadas en virtud de los Principios y proporcionar el recurso adecuado de forma gratuita a la persona afectada.
  - » Si la organización ha seleccionado un mecanismo de recurso independiente proporcionado por un organismo de resolución alternativa de litigios del sector privado, ha incluido en su política de privacidad pertinente un hipervínculo o la dirección web del sitio web correspondiente o del formulario de presentación de reclamaciones del mecanismo que está disponible para investigar las reclamaciones no resueltas presentadas en virtud de los Principios.

» Si la organización está obligada (es decir, con respecto a los datos de recursos humanos transferidos desde la Unión Europea en el contexto de la relación laboral) o ha optado por cooperar con las APD adecuadas en la investigación y resolución de las reclamaciones presentadas en virtud de los Principios, declaró su compromiso con dicha cooperación con las APD y el cumplimiento de sus consejos relacionados para tomar medidas específicas para cumplir con los Principios.

- El Departamento también verificará que la presentación de autocertificación de la organización sea coherente con su política o políticas de privacidad pertinentes. Cuando una organización que se autocertifica desee cubrir cualquiera de sus entidades o filiales estadounidenses que tengan políticas de privacidad independientes y pertinentes, el Departamento también revisará las políticas de privacidad pertinentes de dichas entidades o filiales cubiertas para asegurarse de que incluyen todos los elementos requeridos establecidos en el Principio de Notificación.
- El Departamento colaborará con los organismos legales (por ejemplo, la FTC y el DOT) para verificar que las organizaciones están sujetas a la jurisdicción del organismo legal pertinente identificado en sus presentaciones de autocertificación, cuando el Departamento tenga motivos para dudar de que estén sujetas a dicha jurisdicción.
- El Departamento trabajará con organismos de resolución alternativa de conflictos del sector privado para verificar que las organizaciones están registradas activamente para el mecanismo de recurso independiente identificado en sus presentaciones de autocertificación; y trabajará con dichos organismos para verificar que las organizaciones están registradas activamente para la revisión externa del cumplimiento identificada en sus presentaciones de autocertificación, cuando dichos organismos puedan ofrecer ambos tipos de servicios.
- El Departamento trabajará con el tercero seleccionado por el Departamento para actuar como depositario de los fondos recaudados a través de la tasa del panel de APD (es decir, la tasa anual destinada a cubrir los costes de funcionamiento del panel de APD) para verificar que las organizaciones han abonado dicha tasa para el año correspondiente, cuando las organizaciones hayan identificado las APD como el mecanismo de recurso independiente pertinente.
- El Departamento colaborará con el tercero seleccionado por el Departamento para administrar los arbitrajes de conformidad con el fondo arbitral identificado en el Anexo I de los Principios y gestionarlo, a fin de verificar que las organizaciones han contribuido a dicho fondo arbitral.
- Cuando el Departamento detecte algún problema durante su revisión de las presentaciones de autocertificación de las organizaciones, les informará de que deben resolver todos esos problemas en el plazo adecuado designado por el Departamento[2]. El Departamento también les informará de que si no responden en los plazos establecidos por el Departamento o no completan su autocertificación de acuerdo con los procedimientos del Departamento, se considerará que han abandonado la solicitud de autocertificación, y de

2 Por ejemplo, en lo que respecta a la recertificación, se espera que las organizaciones aborden todas estas cuestiones en un plazo de 45 días, sin perjuicio de que el Departamento designe un plazo diferente y adecuado.

que cualquier solicitud de autocertificación que no se haya completado se considerará abandonada la tergiversación sobre la participación de una organización en el DPF UE-EE.UU. o su cumplimiento del mismo puede ser objeto de medidas coercitivas por parte de la FTC, el DOT u otro organismo gubernamental pertinente. El Departamento informará a las organizaciones a través de los medios de contacto que las organizaciones facilitaron al Departamento.

Facilitar la cooperación con organismos de resolución alternativa de litigios que presten servicios relacionados con los principios

- El Departamento colaborará con los organismos de resolución alternativa de litigios del sector privado que ofrezcan mecanismos de recurso independientes, disponibles para investigar las reclamaciones no resueltas presentadas en virtud de los Principios, para verificar que cumplen, como mínimo, los requisitos establecidos en el Principio complementario sobre resolución de litigios y ejecución. El Departamento verificará que
  - incluir información en sus sitios web públicos sobre los Principios y los servicios que prestan en virtud del DPF UE-EE.UU., que debe incluir: (1) información o un hipervínculo a los requisitos de los Principios para los mecanismos de recurso independientes; (2) un hipervínculo al sitio web del Marco de Privacidad de Datos del Departamento; (3) una explicación de que sus servicios de resolución de litigios en virtud del DPF UE-EE.UU. son gratuitos para las personas; (4) una descripción de cómo se puede presentar una reclamación relacionada con los Principios; (5) el plazo en el que se procesan las reclamaciones relacionadas con los Principios; y (6) una descripción de la gama de posibles soluciones. El Departamento notificará oportunamente a los organismos los cambios materiales que se produzcan en la supervisión y administración por parte del Departamento del programa del Marco de Privacidad de los Datos, cuando dichos cambios sean inminentes o ya se hayan producido y sean pertinentes para el papel que desempeñan los organismos en el marco del DPF UE-EE.UU.;
  - publicar un informe anual con estadísticas agregadas relativas a sus servicios de resolución de litigios, que deben incluir: (1) el número total de reclamaciones relacionadas con los Principios recibidas durante el año del informe; (2) los tipos de reclamaciones recibidas; (3) medidas de calidad de la resolución de conflictos, como el tiempo que se tarda en tramitar las reclamaciones; y (4) los resultados de las reclamaciones recibidas, en particular el número y los tipos de soluciones o sanciones impuestas. El Departamento proporcionará a los organismos orientaciones específicas y complementarias sobre la información que deben proporcionar en esos informes anuales, desarrollando esos requisitos (por ejemplo, enumerando los criterios específicos que debe cumplir una reclamación para ser considerada una reclamación relacionada con los Principios a efectos del informe anual), así como identificando otros tipos de información que deben proporcionar (por ejemplo, si el organismo también proporciona un servicio de verificación relacionado con los Principios, una descripción de cómo el organismo evita cualquier conflicto de intereses real o potencial en situaciones en las que proporciona a una organización tanto servicios de verificación como servicios de resolución de disputas). La orientación adicional proporcionada por el Departamento también especificará la fecha en la que deben publicarse los informes anuales de los organismos para el periodo de referencia correspondiente.

Seguimiento de las organizaciones que desean ser o han sido retiradas de la lista del marco de privacidad de datos

- Si una organización desea retirarse del DPF UE-EE.UU., el Departamento exigirá que la organización elimine de cualquier política de privacidad pertinente cualquier referencia al DPF UE-EE.UU. que implique que sigue participando en el DPF UE-EE.UU. y que puede recibir datos personales de conformidad con el DPF UE-EE.UU. (véase la descripción del compromiso del Departamento de buscar falsas declaraciones de participación). El Departamento también exigirá que la organización cumplimente y envíe al Departamento un cuestionario adecuado para verificar:
  - su deseo de retirarse;
  - cuál de las siguientes medidas adoptará con los datos personales que recibió en virtud del DPF UE-EE.UU. mientras participaba en el DPF UE-EE.UU.: (a) conservar dichos datos, seguir aplicando los Principios a dichos datos y afirmar anualmente ante el Departamento su compromiso de aplicar los Principios a dichos datos; (b) conservar dichos datos y proporcionar una protección "adecuada" a dichos datos por otro medio autorizado; o (c) devolver o eliminar todos dichos datos en una fecha determinada; y
  - quién dentro de la organización servirá como punto de contacto permanente para cuestiones relacionadas con los Principios.
- Si una organización opta por (a), tal y como se describe más arriba, el Departamento también le exigirá que rellene y envíe al Departamento todos los años tras su retirada (es decir en el primer aniversario de su retirada, así como en cada aniversario posterior, a menos y hasta que la organización proporcione una protección "adecuada" de dichos datos por otro medio autorizado o devuelva o elimine todos esos datos y notifique al Departamento de esta acción) un cuestionario adecuado para verificar lo que ha hecho con esos datos personales, lo que hará con cualquiera de esos datos personales que siga conservando, y quién dentro de la organización servirá como punto de contacto permanente para preguntas relacionadas con los Principios.
- Si una organización ha dejado caducar su autocertificación (es decir, no ha completado su recertificación anual de adhesión a los Principios ni ha sido eliminada de la Lista Marco de Privacidad de Datos por algún otro motivo, como la retirada), el Departamento le indicará que cumplimente y envíe al Departamento un cuestionario adecuado para verificar si desea retirarse o volver a certificarse:
  - y si desea retirarse, verificar además qué hará con los datos personales que recibió en virtud del DPF UE-EE.UU. mientras participaba en el DPF UE-EE.UU. (véase la descripción anterior de lo que una organización debe verificar si desea retirarse);
  - y si tiene intención de volver a certificarse, verificar además que durante el lapso de su estatus de certificación aplicó los Principios a los datos personales recibidos en virtud del DPF UE-EE.UU. y aclarar qué medidas tomará para abordar las cuestiones pendientes que han retrasado su recertificación.
- Si una organización es eliminada de la Lista del Marco de Privacidad de Datos por alguna de las siguientes razones: (a) retirada del DPF UE-EE.UU., (b) no completar la recertificación anual de su adhesión a los Principios (es decir, (c) "incumplimiento persistente", el Departamento enviará una notificación al contacto o contactos identificados en la presentación de autocertificación de

la organización especificando el motivo de la retirada y explicando que debe dejar de hacer afirmaciones explícitas o implícitas de que participa en el DPF UE-EE.UU. o lo cumple y que puede recibir datos personales de conformidad con el DPF UE-EE.UU.. La notificación, que también podrá incluir otros contenidos adaptados al motivo de la supresión, indicará que las organizaciones que falseen su participación en el DPF UE-EE.UU. o su cumplimiento del mismo, incluso cuando afirmen que participan en el DPF UE-EE.UU. después de haber sido suprimidas de la Lista Marco de Privacidad de Datos, podrán ser objeto de medidas coercitivas por parte de la FTC, el DOT u otro organismo gubernamental pertinente.

Búsqueda y tratamiento de las declaraciones falsas de participación

- De forma continua, cuando una organización: (a) se retira de la participación en el DPF UE- EE.UU., (b) no completa la recertificación anual de su adhesión a los Principios (es decir, (b) no completa la recertificación anual de su adhesión a los Principios (es decir, comenzó pero no completó el proceso de recertificación anual a su debido tiempo o ni siquiera comenzó el proceso de recertificación anual), (c) es eliminada como participante en el DPF UE-EE. UU. especialmente por "incumplimiento persistente", o (d) no completa una autocertificación inicial de su adhesión a los Principios (es decir, comenzó pero no completó el proceso de autocertificación inicial de manera oportuna), el Departamento emprenderá, de oficio, acciones para verificar que ninguna política de privacidad pertinente publicada por la organización contenga referencias al DPF UE-EE.UU. que impliquen que la organización participa en el DPF UE-EE.UU. y que puede recibir datos personales de conformidad con el DPF UE-EE.UU.. Cuando el Departamento encuentre tales referencias, informará a la organización de que, si procede, remitirá el asunto a la agencia pertinente para la posible adopción de medidas coercitivas si la organización sigue tergiversando su participación en el DPF UE-EE. El Departamento informará a la organización a través de los medios de contacto que la organización haya facilitado al Departamento o, en caso necesario, por otros medios adecuados. Si la organización no elimina las referencias ni autocertifica su conformidad con el DPF de la UE-U.S. DPF de acuerdo con los procedimientos del Departamento, el Departamento remitirá de oficio el asunto a la FTC, al DOT o a otro organismo de aplicación adecuado, o tomará otras medidas apropiadas para garantizar el uso correcto de la marca de certificación DPF UE-EE.UU.;
- El Departamento emprenderá otros esfuerzos para identificar falsas alegaciones de participación en el DPF UE-EE.UU. y el uso indebido de la marca de certificación DPF UE- EE.UU., incluso por parte de organizaciones que, a diferencia de las descritas anteriormente, ni siquiera han iniciado el proceso de autocertificación (por ejemplo, realizando búsquedas adecuadas en Internet para identificar referencias al DPF UE-EE.UU. en las políticas de privacidad de las organizaciones). Cuando a través de tales esfuerzos el Departamento identifique falsas afirmaciones de participación en el DPF UE-EE.UU. y uso indebido de la marca de certificación DPF UE-EE.UU., el Departamento informará a la organización de que el Departamento, según proceda, remitirá el asunto a la agencia pertinente para la posible adopción de medidas coercitivas si la organización sigue falseando su participación en el DPF UE-EE.UU., o si la organización no cumple las normas de la UE.EE.UU. DPF. El Departamento informará a la organización a través de los medios de contacto que, en su caso, la organización haya facilitado al Departamento o, cuando sea necesario, por otros medios adecuados. Si la organización no retira las referen-

cias ni autocertifica su conformidad con el DPF UE-EE.UU. de acuerdo con los procedimientos del Departamento, el Departamento remitirá de oficio el asunto a la FTC, al DOT o a otro organismo de ejecución adecuado, o tomará otras medidas apropiadas para garantizar el uso adecuado de la marca de certificación DPF UE-EE.UU.;

- El Departamento revisará y atenderá con prontitud las quejas específicas y no frívolas sobre falsas alegaciones de participación de la UE y EE.UU. en el DPF que reciba (por ejemplo, quejas recibidas de las APD, mecanismos de recurso independientes proporcionados por organismos de resolución alternativa de litigios del sector privado, interesados, empresas de la UE y EE.UU. y otros tipos de terceros); y
- El Departamento podrá adoptar otras medidas correctivas apropiadas. Las declaraciones falsas al Departamento pueden ser perseguibles en virtud de la Ley de Declaraciones Falsas (18 U.S.C. § 1001).

Realizar revisiones y evaluaciones periódicas de oficio del cumplimiento del Programa Marco de Privacidad de Datos

- De forma continuada, el Departamento se esforzará por supervisar el cumplimiento efectivo por parte de las organizaciones de DPF de la UE-EE.UU. para identificar problemas que puedan justificar medidas de seguimiento. En particular, el Departamento llevará a cabo, de oficio, inspecciones aleatorias rutinarias de organizaciones de DPF de la UE y de EE.UU. seleccionadas al azar, así como inspecciones aleatorias *ad hoc* de organizaciones de DPF de la UE y de EE.UU. específicas cuando se identifiquen posibles deficiencias de cumplimiento (por ejemplo, (a) que el punto o puntos de contacto responsables de la tramitación de reclamaciones, solicitudes de acceso y otras cuestiones que surjan en el marco del DPF UE-EE.UU. están disponibles; (b) en su caso, que la política de privacidad pública de la organización está a disposición del público, tanto en el sitio web público de la organización como a través de un hipervínculo en la lista del marco de privacidad de los datos b) en su caso, que la política de privacidad de la organización está a disposición del público tanto en el sitio web público de la organización como a través de un hipervínculo en la Lista del Marco de Privacidad de Datos; c) que la política de privacidad de la organización sigue cumpliendo los requisitos de autocertificación descritos en los Principios; y d) que el mecanismo de recurso independiente identificado por la organización está disponible para tramitar las reclamaciones presentadas en virtud de los Principios del DPF UE-EE.UU. El Departamento también vigilará activamente las noticias en busca de informes que proporcionen pruebas creíbles de incumplimiento por parte de las organizaciones de DPF UE-EE.UU.;
- Como parte de la revisión del cumplimiento, el Departamento exigirá que una organización de DPF UE-EE.UU. cumplimente y presente al Departamento un cuestionario detallado cuando: (a) el Departamento haya recibido alguna queja específica, no frívola, sobre el cumplimiento de los Principios por parte de la organización, (b) la organización no responda satisfactoriamente a las solicitudes de información del Departamento relacionadas con el DPF UE-EE.UU., o (c) existan pruebas creíbles de que la organización no cumple con los compromisos adquiridos en virtud del DPF DE EE.UU. Cuando el Departamento haya enviado un cuestionario detallado de este tipo a una organización y ésta no responda satisfactoriamente al cuestionario, el Departamento informará a la organización de que, si no recibe una respuesta oportuna y satisfactoria de la organización, el Departamento remitirá el asunto, según

proceda, a la agencia pertinente para la posible adopción de medidas coercitivas. El Departamento informará a la organización a través de los medios de contacto que la organización haya facilitado al Departamento o, en caso necesario, por otros medios adecuados. Si la organización no proporciona una respuesta oportuna y satisfactoria, el Departamento remitirá de oficio el asunto a la FTC, al DOT o a otro organismo de aplicación adecuado, o tomará otras medidas apropiadas para garantizar el cumplimiento. Cuando proceda, el Departamento consultará a las autoridades competentes en materia de protección de datos acerca de tales revisiones de cumplimiento.

- El Departamento evaluará periódicamente la administración y supervisión del programa del Marco de Privacidad de Datos para garantizar que sus esfuerzos de supervisión, incluidos los realizados mediante el uso de herramientas de búsqueda (por ejemplo, para comprobar si hay enlaces rotos a las políticas de privacidad de las organizaciones del DPF de la UE y de EE.UU.), son adecuados para abordar los problemas existentes y cualquier problema nuevo que surja.

Adaptar el sitio web del marco de privacidad de datos al público destinatario

El Departamento adaptará el sitio web del Marco de privacidad de los datos para centrarse en los siguientes destinatarios: particulares de la UE, empresas de la UE, empresas estadounidenses y APD. La inclusión de material dirigido directamente a los particulares y las empresas de la UE facilitará la transparencia de varias maneras. Por lo que respecta a los particulares de la UE, el sitio web explicará claramente: (1) los derechos que el DPF UE- EE.UU. otorga a los particulares de la UE; (2) los mecanismos de recurso a disposición de los particulares de la UE cuando consideren que una organización ha incumplido su compromiso de cumplir los Principios; y (3) cómo encontrar información relativa a la autocertificación del DPF UE-EE.UU. de una organización. En lo que respecta a las empresas de la UE, facilitará la verificación de: (1) si una organización participa en el DPF UE-EE.UU.; (2) el tipo de información cubierta por la autocertificación DPF UE-EE.UU. de una organización; (3) la política de privacidad que se aplica a la información cubierta; y (4) el método que utiliza la organización para verificar su adhesión a los Principios. Por lo que respecta a las empresas estadounidenses, explicará claramente: (1) las ventajas de la participación en el DPF UE-EE.UU.; (2) cómo adherirse al DPF UE-EE.UU., así como cómo volver a certificarse en el DPF UE-EE.UU. y retirarse de él; y (3) cómo Estados Unidos administra y hace cumplir el DPF UE- EE.UU.. La inclusión de material dirigido directamente a las APD (por ejemplo, información sobre el punto de contacto específico del Departamento para las APD y un hipervínculo al contenido relacionado con los Principios en el sitio web de la FTC) facilitará tanto la cooperación como la transparencia. El Departamento también trabajará *ad hoc* con la Comisión y el Consejo Europeo de Protección de Datos ("EDPB") para desarrollar material adicional de actualidad (por ejemplo, respuestas a preguntas frecuentes) para su uso en el sitio web del Marco de Privacidad de Datos, cuando dicha información facilite la administración y supervisión eficientes del programa del Marco de Privacidad de Datos.

Facilitar la cooperación con las APD

Para aumentar las oportunidades de cooperación con las APD, el Departamento mantendrá un punto de contacto específico en el Departamento para actuar como enlace con las APD. En los casos en que una APD considere que una organización de DPF de la UE-EE.UU. no está cumpliendo los Principios, incluso a raíz de una denuncia de un particular de la UE, la APD podrá ponerse en contacto con el punto de contacto específico del Departamento para remitir a la organización a un examen

más detallado. El Departamento hará todo lo posible para facilitar la resolución de la queja con la organización DPF de la UE y Estados Unidos. En un plazo de 90 días a partir de la recepción de la denuncia, el Departamento facilitará información actualizada a la APD. El punto de contacto específico también recibirá remisiones relativas a organizaciones que afirmen falsamente participar en el DPF UE-EE.UU.. El punto de contacto específico hará un seguimiento de todas las remisiones de las APD recibidas por el Departamento, y éste facilitará en la revisión conjunta descrita más adelante un informe en el que se analicen en conjunto las denuncias que recibe cada año. El punto de contacto específico ayudará a las APD que busquen información relacionada con la autocertificación de una organización específica o con su participación previa en el DPF UE-EE.UU., y el punto de contacto específico responderá a las consultas de las APD relativas a la aplicación de requisitos específicos del DPF UE-EE. UU.. El Departamento también cooperará con la Comisión y la EDPB en los aspectos procedimentales y administrativos del panel DPA, incluido el establecimiento de procedimientos adecuados para la distribución de los fondos recaudados a través de la tasa del panel DPA. Entendemos que la Comisión colaborará con el Departamento para facilitar la resolución de cualquier problema que pueda surgir en relación con dichos procedimientos. Además, el Departamento proporcionará a las APD material relativo al DPF UE-EE.UU. para que lo incluyan en sus propios sitios web con el fin de aumentar la transparencia para los particulares y las empresas de la UE. Un mayor conocimiento del DPF UE-EE.UU. y de los derechos y responsabilidades que genera debería facilitar la identificación de los problemas a medida que surjan, de modo que puedan abordarse adecuadamente.

Cumplir sus compromisos con arreglo al Anexo I de los Principios

El Departamento cumplirá sus compromisos en virtud del Anexo I de los Principios, incluido el mantenimiento de una lista de árbitros elegidos con la Comisión sobre la base de la independencia, la integridad y la experiencia; y el apoyo, según proceda, al tercero seleccionado por el Departamento para administrar los arbitrajes de conformidad con y gestionar el fondo arbitral identificado en el Anexo I de los Principios[3] El Departamento trabajará con el tercero para, entre otras cosas, verificar que el tercero mantiene un sitio web con orientación sobre el proceso de arbitraje, incluyendo: (1) cómo iniciar procedimientos y presentar documentos; (2) la lista de árbitros mantenida por el Departamento y cómo seleccionar árbitros de esa lista; (3) los procedimientos arbitrales rectores y el código de conducta de los árbitros adoptados por el Departamento y la Comisión[4]; y (4) el cobro y pago de los honorarios de los árbitros. Además, el Departamento trabajará con el tercero para revisar periódicamente el funcionamiento del fondo arbitral, incluida la necesidad de ajustar el importe de las contribuciones o los topes (es decir, las cantidades máximas) del coste arbitral,

3 El Centro Internacional para la Resolución de Disputas ("ICDR"), la división internacional de la Asociación Americana de Arbitraje ("AAA") (colectivamente "ICDR-AAA"), fue seleccionado por el Departamento para administrar los arbitrajes de conformidad con y gestionar el fondo arbitral identificado en el Anexo I de los Principios.

4 El 15 de septiembre de 2017, el Departamento y la Comisión acordaron la adopción de un conjunto de normas de arbitraje para regir los procedimientos de arbitraje vinculante descritos en el anexo I de los Principios, así como un código de conducta para los árbitros que es coherente con las normas éticas generalmente aceptadas para los árbitros comerciales y el anexo I de los Principios. El Departamento y la Comisión acordaron adaptar el reglamento de arbitraje y el código de conducta para reflejar las actualizaciones en el marco del DPF UE-EE.UU., y el Departamento trabajará con el ICDR-AAA para realizar dichas actualizaciones.

y considerar, entre otras cosas, el número de arbitrajes y los costes y el calendario de los arbitrajes, en el entendimiento de que no habrá una carga financiera excesiva impuesta a las organizaciones DPF de la UE y Estados Unidos. El Departamento notificará a la Comisión el resultado de dichas revisiones con el tercero y le comunicará previamente cualquier ajuste del importe de las contribuciones.

Realizar revisiones conjuntas del funcionamiento del DPF UE-EE.UU.

El Departamento y otros organismos, según proceda, celebrarán reuniones periódicas con la Comisión, las autoridades de protección de datos interesadas y los representantes pertinentes de la Oficina Europea de Protección de Datos, en las que el Departamento facilitará información actualizada sobre el marco para la protección de datos entre la UE y Estados Unidos. En las reuniones se debatirán cuestiones de actualidad relacionadas con el funcionamiento, la aplicación, la supervisión y el cumplimiento del programa marco de protección de datos. Las reuniones podrán incluir, en su caso, el debate de temas relacionados, tales como otros mecanismos de transferencia de datos que se benefician de las salvaguardias previstas en el DPF UE-EE.UU.

Actualización de la legislación

El Departamento hará esfuerzos razonables para informar a la Comisión de la evolución material de la legislación en Estados Unidos en la medida en que sea pertinente para el DPF UE-EE.UU. en el ámbito de la protección de la intimidad de los datos y de las limitaciones y salvaguardias aplicables al acceso a los datos personales por parte de las autoridades estadounidenses y a su utilización posterior.

Acceso del Gobierno de EE.UU. a datos personales

Estados Unidos ha promulgado la Orden Ejecutiva 14086, "Mejora de las salvaguardias para las actividades de inteligencia de señales de Estados Unidos" y 28 CFR parte 201, que modifica la normativa del Departamento de Justicia para establecer el Tribunal de Revisión de Protección de Datos (el "DPRC"), que proporciona una fuerte protección de los datos personales con respecto al acceso del gobierno a los datos con fines de seguridad nacional. La protección proporcionada incluye: el refuerzo de las salvaguardias de la privacidad y las libertades civiles para garantizar que las actividades de inteligencia de señales de Estados Unidos son necesarias y proporcionadas para la consecución de los objetivos de seguridad nacional definidos; el establecimiento de un nuevo mecanismo de recurso con autoridad independiente y vinculante; y la mejora de la rigurosa y estratificada supervisión existente de las actividades de inteligencia de señales de Estados Unidos. A través de estas protecciones, las personas de la UE pueden solicitar reparación a un nuevo mecanismo de reparación de múltiples niveles que incluye un DPRC independiente que estaría formado por personas elegidas fuera del Gobierno de EE.UU. que tendrían plena autoridad para adjudicar reclamaciones y dirigir medidas correctivas según sea necesario. El Departamento mantendrá un registro de las personas de la UE que presenten una reclamación admisible de conformidad con la Orden ejecutiva 14086 y 28 CFR, parte 201. Cinco años después de la fecha de esta carta, y posteriormente cada cinco años, el Departamento se pondrá en contacto con los organismos pertinentes para averiguar si se ha desclasificado la información relativa a la revisión de las reclamaciones admisibles o a la revisión de las solicitudes de revisión presentadas al DPRC. Si dicha información ha sido desclasificada, el Departamento trabajará con la APD pertinente para informar a la persona de la UE. Estas mejoras confirman que los datos personales de la UE transferidos a los Estados Unidos se tratarán de forma coherente con los requisitos legales de la UE en materia de acceso de la Administración a los datos.

Sobre la base de los Principios, la Orden Ejecutiva 14086, 28 CFR parte 201, y las cartas y materiales adjuntos, incluidos los compromisos del Departamento en relación con la administración y supervisión del programa Marco de Privacidad de Datos, nuestra expectativa es que la Comisión determine que el DPF UE-EE.UU. proporciona una protección adecuada a efectos de la legislación de la UE, las transferencias de datos desde la Unión Europea seguirán realizándose a organizaciones que participen en el DPF UE-EE.UU.. También esperamos que las transferencias a organizaciones estadounidenses realizadas en virtud de cláusulas contractuales tipo de la UE o de normas corporativas vinculantes de la UE se vean facilitadas por los términos de dichos acuerdos.

Atentamente,

Marisa Lago

ANEXO IV

Office of the Chair

ESTADOS UNIDOS DE AMÉRICA
Comisión Federal de Comercio
WASHINGTON, D.C. 20580

9 de junio de 2023

Didier Reynders
Comisario de Justicia Comisión Europea
Rue de la Loi / Wetstraat 200 1049 Bruselas
Bélgica

Estimado Comisario Reynders:

La Comisión Federal de Comercio de Estados Unidos ("FTC", por sus siglas en inglés) agradece la oportunidad de referirse a su papel en la aplicación de los principios del marco de privacidad de datos UE-EE.UU. ("EU- U.S. DPF", por sus siglas en inglés). La FTC lleva mucho tiempo comprometida con la protección de los consumidores y la privacidad a través de las fronteras, y estamos comprometidos con la aplicación de los aspectos de este marco relativos al sector comercial. La FTC ha desempeñado este papel desde el año 2000, en relación con el EE.UU.-UE Safe Harbor Framework, y más recientemente, desde 2016, en relación con el EU-U.S. Privacy Shield Framework[1]. El 16 de julio de 2020, el Tribunal de Justicia de la Unión Europea ("TJUE") invalidó la decisión de adecuación de la Comisión Europea subyacente al Marco del Escudo de Privacidad UE-EE.UU., sobre la base de cuestiones distintas de

1 Letter from Chairwoman Edith Ramirez to Věra Jourová, Commissioner for Justice, Consumers and Gender Equality of the European Commission, Describing Federal Trade Commission Enforcement of the New EU-U.S. Privacy Shield Framework (29 de febrero de 2016), disponible en https://www.ftc.gov/legal-library/browse/cases- proceedings/public-statements/letter-chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers- gender-equality-european. La FTC también se comprometió anteriormente a hacer cumplir el Programa de Puerto Seguro EE.UU.-UE. Carta de Robert Pitofsky, Presidente de la FTC, a John Mogg, Director DG Mercado Interior, Comisión Europea (14 de julio de 2000), disponible en https://www.federalregister.gov/documents/2000/07/24/00-18489/issuance-of-safe-harbor- principles-and-transmission-to-european-commission. Esta carta sustituye a los compromisos anteriores.

los principios comerciales que la FTC hizo cumplir. Desde entonces, los EE.UU. y la Comisión Europea han negociado el Marco de Privacidad de Datos UE-EE.UU. para dar respuesta a la sentencia del TJUE.

Me dirijo a usted para confirmar el compromiso de la FTC con la aplicación rigurosa de los principios DPF UE-EE.UU.. En particular, reafirmamos nuestro compromiso en tres áreas clave: (1) priorización de remisiones e investigaciones; (2) búsqueda y seguimiento de órdenes; y (3) cooperación en materia de aplicación con las autoridades de protección de datos de la UE ("APD").

I. Introducción

a. Política de privacidad de la FTC

La FTC tiene amplias competencias de ejecución civil para promover la protección de los consumidores y la competencia en el ámbito comercial. Como parte de su mandato de protección de los consumidores, la FTC hace cumplir una amplia gama de leyes para proteger la privacidad y la seguridad de los consumidores y sus datos.

La principal ley aplicada por la FTC, la Ley FTC, prohíbe los actos o prácticas "desleales" o "engañosos" en el comercio o que afecten a éste[2]. La FTC también aplica leyes específicas que protegen la información relativa a la salud, el crédito y otros asuntos financieros, así como la información en línea de los niños, y ha publicado reglamentos de aplicación de cada una de estas leyes[3].

La FTC también ha emprendido recientemente numerosas iniciativas para reforzar nuestra labor en materia de privacidad. En agosto de 2022, la FTC anunció que estaba estudiando normas para acabar con la vigilancia comercial nociva y la falta de seguridad de los datos[4]. El objetivo del proyecto es crear un registro público sólido para informar sobre si la FTC debe emitir normas para abordar la vigilancia comercial y las prácticas de seguridad de datos, y cómo deberían ser potencialmente esas normas. Agradecemos los comentarios de las partes interesadas de la UE sobre esta y otras iniciativas.

---

2 15 U.S.C. § 45(a). La FTC no tiene jurisdicción sobre la aplicación de la ley penal o asuntos de seguridad nacional. La FTC tampoco puede intervenir en la mayoría de las acciones gubernamentales. Además, existen excepciones a la jurisdicción de la FTC sobre las actividades comerciales, en particular con respecto a los bancos, las compañías aéreas, el negocio de los seguros y las actividades de transporte común de los proveedores de servicios de telecomunicaciones. La FTC tampoco tiene jurisdicción sobre la mayoría de las organizaciones sin ánimo de lucro, aunque sí sobre las organizaciones benéficas ficticias u otras organizaciones sin ánimo de lucro que de hecho operan con ánimo de lucro. La FTC también tiene jurisdicción sobre las organizaciones sin ánimo de lucro que operan en beneficio de sus miembros con ánimo de lucro, incluso proporcionando beneficios económicos sustanciales a dichos miembros. En algunos casos, la jurisdicción de la FTC es concurrente con la de otros organismos encargados de hacer cumplir la ley. Hemos desarrollado sólidas relaciones de trabajo con las autoridades federales y estatales, y colaboramos estrechamente con ellas para coordinar las investigaciones o hacer remisiones cuando procede.

3 Véase FTC, Privacidad y seguridad, https://www.ftc.gov/business-guidance/privacy-security.

4 Véase el comunicado de prensa, Fed. Trade Comm'n, FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices (11 de agosto de 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data- security-practices.

Nuestras conferencias "PrivacyCon" siguen reuniendo a destacados investigadores para debatir las últimas investigaciones y tendencias relacionadas con la privacidad de los consumidores y la seguridad de los datos. También hemos aumentado la capacidad de nuestra agencia para seguir el ritmo de los avances tecnológicos que son el centro de gran parte de nuestro trabajo sobre privacidad, creando un equipo cada vez mayor de tecnólogos e investigadores interdisciplinarios. Como sabe, también hemos anunciado un diálogo conjunto con usted y sus colegas de la Comisión Europea, en el que se abordarán temas relacionados con la privacidad, como los patrones oscuros y los modelos de negocio caracterizados por la recopilación generalizada de datos[5]. También publicamos recientemente un informe para el Congreso advirtiendo sobre los daños asociados al uso de inteligencia artificial ("IA") para abordar los daños en línea identificados por el Congreso. Este informe planteaba preocupaciones en relación con la inexactitud, la parcialidad, la discriminación y la fluencia de la vigilancia comercial[6].

b. Las protecciones legales de EE.UU. benefician a los consumidores de la UE

La DPF UE-EE.UU. opera en el contexto del panorama más amplio de la privacidad en EE.UU., que también protege a los consumidores de la UE de varias maneras. La prohibición de la Ley FTC de actos o prácticas desleales o engañosos no se limita a proteger a los consumidores estadounidenses de las empresas estadounidenses, ya que incluye aquellas prácticas que (1) causen o puedan causar un perjuicio razonablemente previsible en Estados Unidos, o (2) implican una conducta material en Estados Unidos. Además, la FTC puede utilizar todos los recursos disponibles para proteger a los consumidores nacionales a la hora de proteger a los consumidores extranjeros[7].

La FTC también hace cumplir otras leyes específicas cuyas protecciones se extienden a los consumidores no estadounidenses, como la Ley de Protección de la Privacidad Infantil en Línea ("COPPA"). Entre otras cosas, la COPPA exige que los operadores de sitios web y servicios en línea dirigidos a niños, o sitios de audiencia general que recopilen a sabiendas información personal de niños menores de 13 años, proporcionen un aviso a los padres y obtengan su consentimiento verificable. Los sitios web y servicios con sede en Estados Unidos que están sujetos a la COPPA y recopilan información personal de niños extranjeros están obligados a cumplir la COPPA. Los sitios web y servicios en línea con sede en el extranjero también deben cumplir la COPPA si están dirigidos a niños en Estados Unidos, o si recopilan a sabiendas información personal de niños en Estados Unidos. Por otra parte, además de las leyes federales estadounidenses aplicadas por la FTC, otras leyes federales y estatales de protección de los consumidores, violación de datos y privacidad pueden proporcionar beneficios adicionales a los consumidores de la UE.

---

5 Véase el comunicado de prensa conjunto de Didier Reynders, Comisario de Justicia de la Comisión Europea, y Lina Khan, Presidenta de la Comisión Federal de Comercio de Estados Unidos (30 de marzo de 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

6 Véase el comunicado de prensa, Fed. Trade Comm'n, FTC Report Warns About Using Artificial Intelligence to Combat Online Problems (16 de junio de 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc- report-warns-about- using-artificial-intelligence-combat-online-problems.

7 15 U.S.C. § 45(a)(4)(B). Además, los "actos o prácticas desleales o engañosos" incluyen los actos o prácticas relacionados con el comercio exterior que (i) causen o puedan causar un perjuicio razonablemente previsible en Estados Unidos; o (ii) impliquen una conducta material que se produzca en Estados Unidos. 15 U.S.C. § 45(a)(4)(A).

c. Actividad de aplicación de la FTC

La FTC interpuso demandas tanto en el marco del Safe Harbor entre EE.UU. y la UE como en el del Escudo de la privacidad entre la UE y EE.UU., y siguió aplicando el Escudo de la privacidad entre la UE y EE.UU. incluso después de que el TJUE invalidara la decisión de adecuación en que se basaba el marco del Escudo de la privacidad entre la UE y EE.UU.[8]. Varias de las denuncias recientes de la FTC han incluido cargos en los que se alega que las empresas infringieron el marco EU disposiciones del Escudo de Privacidad de EE.UU., incluso en procedimientos contra Twitter[9], *CafePress*[10], y *Flo*[11]. En la acción de aplicación contra Twitter, la FTC obtuvo 150 millones de dólares de Twitter por su violación de una orden anterior de la FTC con prácticas que afectan a más de 140 millones de clientes, incluida la violación del Principio 5 del Escudo de Privacidad UE-EE.UU. (Integridad de los datos y limitación de la finalidad). Además, la orden de la agencia exige que Twitter permita a los usuarios emplear métodos seguros de autenticación multifactor que no requieran que los usuarios faciliten sus números de teléfono.

En el caso de *CafePress*, la FTC alegó que la empresa no protegía la información confidencial de los consumidores, encubría una importante filtración de datos e infringía los principios 2 (Elección), 4 (Seguridad) y 6 (Acceso) del Escudo de la privacidad UE-EE.UU.. La orden de la FTC exige a la empresa que sustituya las medidas de autenticación inadecuadas por una autenticación multifactorial, que limite sustancialmente la cantidad de datos que recopila y conserva, que cifre los números de la Seguridad Social y que encargue a un tercero la evaluación de sus programas de seguridad de la información y proporcione a la FTC una copia que pueda hacerse pública.

En *Flo*, la FTC alegó que la aplicación de seguimiento de la fertilidad revelaba información sobre la salud de los usuarios a terceros proveedores de análisis de datos después de haberse comprometido a mantener la privacidad de dicha información. La denuncia de la FTC señala específicamente las interacciones de la empresa con los consumidores de la UE y que Flo infringió los principios 1 (Notificación), 2 (Elección), 3 (Responsabilidad de la transferencia ulterior) y 5 (Integridad de los datos y limitación de la finalidad) del Escudo de la privacidad UE-EE.UU.. Entre otras cosas, la orden de la agencia exige a Flo que notifique a los usuarios afectados la divulgación de su información personal y que ordene a cualquier tercero que haya recibido información sanitaria de los usuarios que destruya esos datos. Es importante destacar que las órdenes de la FTC protegen a todos los consumidores del mundo que interactúan con una empresa estadounidense, no sólo a los consumidores que han presentado una denuncia.

---

8 Véase en el Apéndice A una lista de asuntos relacionados con el Safe Harbor y el Privacy Shield de la FTC.

9 Véase el comunicado de prensa, Fed. Trade Comm'n, FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads (25 de mayo de 2022), https://www.ftc.gov/news-events/news/press- releases/2022/05/ftc-charges- twitter-deceptively-using-account-security-data-sell-targeted-ads.

10 Véase el comunicado de prensa, Fed. Trade Comm'n, FTC Takes Action Against *CafePress* for Data Breach Cover Up (15 de marzo de 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action- against-cafepress-data- breach-cover.

11 Véase el comunicado de prensa, Fed. Trade Comm'n, FTC Finalizes Order with Flo Health, a Fertility- Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (22 de junio de 2021), https://www.ftc.gov/news- events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking- app-shared-sensitive-health-data-facebook-google.

Muchos de los casos anteriores de aplicación del Safe Harbor entre EE.UU. y la UE y del Privacy Shield entre la UE y EE.UU. se referían a organizaciones que completaron una autocertificación inicial a través del Departamento de Comercio.pero no mantuvieron su autocertificación anual mientras seguían presentándose como participantes actuales. Otros casos se referían a falsas declaraciones de participación por parte de organizaciones que nunca completaron una autocertificación inicial a través del Departamento de Comercio. De cara al futuro, esperamos centrar nuestros esfuerzos proactivos de aplicación en los tipos de violaciones sustantivas de los principios DPF UE-EE.UU. alegados en casos como los de Twitter, *CafePress* y *Flo*. Mientras tanto, el Departamento de Comercio administrará y supervisará el proceso de autocertificación, mantendrá la lista autorizada de participantes en el DPF UE-EE.UU. y abordará otras cuestiones relativas a las solicitudes de participación en el programa[12]. Es importante destacar que las organizaciones que reclamen la participación en el DPF UE-EE.UU. pueden estar sujetas a la aplicación sustantiva de los principios del DPF UE-EE.UU. incluso si no realizan o mantienen su autocertificación a través del Departamento de Comercio.

II. Priorización de remisiones e investigaciones

Al igual que hicimos en el Marco de Puerto Seguro EE.UU.-UE y en el Marco del Escudo de Privacidad UE-EE.UU., la FTC se compromete a dar consideración prioritaria a las remisiones de Principios DPF UE-EE.UU. procedentes del Departamento de Comercio y de los Estados miembros de la UE. También daremos prioridad a la consideración de las remisiones por incumplimiento de los Principios DPF UE-EE.UU. procedentes de organizaciones de autorregulación de la privacidad y otros organismos independientes de resolución de litigios.

Para facilitar las remisiones en virtud del DPF UE-EE.UU. desde los Estados miembros de la UE, la FTC ha creado un proceso de remisión normalizado y ha proporcionado orientación a los Estados miembros de la UE sobre el tipo de información que mejor ayudaría a la FTC en su investigación sobre una remisión. Como parte de este esfuerzo, la FTC ha designado un punto de contacto de la agencia para las remisiones de los Estados miembros de la UE. Es más útil cuando la autoridad remitente ha llevado a cabo una investigación preliminar sobre la presunta infracción y puede cooperar con la FTC en una investigación.

Al recibir una remisión de este tipo del Departamento de Comercio, de un Estado miembro de la UE o de una organización autorreguladora u otros organismos independientes de resolución de litigios, la FTC puede tomar una serie de medidas para abordar las cuestiones planteadas. Por ejemplo, podemos revisar las políticas de privacidad de la organización, obtener más información directamente de la organización o de terceros, realizar un seguimiento con la entidad remitente, evaluar si existe un patrón de violaciones o un número significativo de consumidores afectados, determinar si la remisión implica cuestiones que son competencia del Departamento de Comercio, evaluar si sería útil realizar esfuerzos adicionales para poner sobre aviso a los participantes en el mercado y, en su caso, iniciar un procedimiento de aplicación.

Además de dar prioridad a los casos remitidos por el Departamento de Comercio, los Estados miembros de la UE y las organizaciones autorreguladoras de la privacidad u otros organismos independientes de resolución de litigios[13], la FTC seguirá inves-

12 Carta de Marisa Lago, Subsecretaria de Comercio Internacional, al Honorable Didier Reynders, Comisario de Justicia de la Comisión Europea (12 de diciembre de 2022).

13 Aunque la FTC no resuelve ni media en las reclamaciones individuales de los consumi-

tigando las infracciones significativas de los principios DPF UE-EE.UU. por iniciativa propia cuando proceda, utilizando una serie de herramientas. Como parte del programa de la FTC de investigación de cuestiones de privacidad y seguridad que implican a organizaciones comerciales, la agencia ha examinado de forma rutinaria si la entidad en cuestión estaba realizando actividades de protección de la privacidad y la intimidad en la UE. Declaraciones del Escudo de la privacidad UE-EE.UU. Si la entidad hacía tales declaraciones y la investigación revelaba aparentes violaciones de los Principios del Escudo de Privacidad UE- EE.UU., la FTC incluía alegaciones de violaciones del Escudo de Privacidad UE-EE.UU. en sus acciones de aplicación. Continuaremos con este enfoque proactivo, ahora con respecto a los Principios del Escudo de Privacidad UE-EE.UU.

III. Órdenes de búsqueda y seguimiento

La FTC también afirma su compromiso de buscar y supervisar órdenes de ejecución para garantizar el cumplimiento de los Principios DPF UE-EE.UU.. Exigiremos el cumplimiento de los Principios DPF UE-EE.UU. mediante una serie de disposiciones cautelares apropiadas en futuras órdenes de la FTC sobre los Principios DPF UE-EE. UU.. Las infracciones de las órdenes administrativas de la FTC pueden dar lugar a sanciones civiles de hasta 50.120 dólares por infracción, o 50.120 dólares por día en caso de infracción continuada[14], que, en el caso de prácticas que afecten a muchos consumidores, pueden ascender a millones de dólares. Cada orden de consentimiento contiene también disposiciones en materia de información y cumplimiento. Las entidades objeto de la orden deben conservar los documentos que demuestren su cumplimiento durante un número determinado de años. Las órdenes también deben difundirse entre los empleados responsables de garantizar su cumplimiento.

La FTC supervisa sistemáticamente el cumplimiento de las órdenes existentes sobre los Principios del Escudo de Privacidad UE-EE.UU., como hace con todas sus órdenes, y emprende acciones para hacerlas cumplir cuando es necesario[15]. Es importante destacar que las órdenes de la FTC seguirán protegiendo a todos los consumidores del mundo que interactúen con una empresa, no sólo a los consumidores que hayan presentado reclamaciones. Por último, la FTC mantendrá una lista en línea de las empresas sujetas a órdenes obtenidas en relación con la aplicación de los principios DPF UE-EE.UU.[16].

---

dores, afirma que dará prioridad a las remisiones de los principios DPF UE-EE.UU. procedentes de los APD de la UE. Además, la FTC utiliza las denuncias de su base de datos Consumer Sentinel, a la que pueden acceder muchos otros organismos encargados de hacer cumplir la ley, para identificar tendencias, determinar prioridades de aplicación e identificar posibles objetivos de investigación. Los particulares de la UE pueden utilizar el mismo sistema de denuncia disponible para los consumidores de EE.UU. para presentar una denuncia a la FTC en https://reportfraud.ftc.gov/. Sin embargo, para las denuncias individuales UE-EE.UU. relativas a los principios DPF, puede ser más útil que los particulares de la UE presenten denuncias a la APD de su Estado miembro o a un organismo independiente de resolución de litigios.

14 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Este importe se ajusta periódicamente en función de la inflación.

15 El año pasado, la FTC votó a favor de agilizar el proceso de investigación de los infractores reincidentes. Véase el comunicado de prensa, Fed. Trade Comm'n, FTC Authorizes Investigations into Key Enforcement Priorities (1 de julio de 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes- investigations-key-enforcement- priorities.

16 *Cf*. FTC, Privacy Shield, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. Cooperación con las autoridades de protección de datos de la UE

La FTC reconoce el importante papel que las APD de la UE pueden desempeñar con respecto al cumplimiento de los principios DPF UE-EE.UU. y anima a aumentar las consultas y la cooperación en materia de aplicación. De hecho, un enfoque coordinado de los retos planteados por la evolución actual del mercado digital, y los modelos de negocio intensivos en datos, es cada vez más crítico. La FTC intercambiará información sobre remisiones con las autoridades encargadas de la aplicación de la ley remitentes, incluido el estado de las remisiones, con sujeción a las leyes y restricciones de confidencialidad. En la medida de lo posible, dado el número y el tipo de remisiones recibidas, la información facilitada incluirá una evaluación de los asuntos remitidos, incluida una descripción de las cuestiones significativas planteadas y cualquier medida adoptada para hacer frente a las infracciones de la ley dentro de la jurisdicción de la FTC. La FTC también proporcionará información a la autoridad remitente sobre los tipos de remisiones recibidas con el fin de aumentar la eficacia de los esfuerzos para hacer frente a las conductas ilícitas. Si una autoridad encargada de la aplicación de la ley solicita información sobre el estado de una remisión concreta a efectos de proseguir su propio procedimiento de aplicación de la ley, la FTC responderá, teniendo en cuenta el número de remisiones en consideración y con sujeción a la confidencialidad y otros requisitos legales.

La FTC también colaborará estrechamente con las APD de la UE para prestar asistencia en la aplicación de la ley. En los casos apropiados, esto podría incluir el intercambio de información y la asistencia en la investigación de conformidad con la Ley SAFE WEB de EE.UU., que autoriza la asistencia de la FTC a las fuerzas de seguridad extranjeras cuando la agencia extranjera está aplicando leyes que prohíben prácticas que son sustancialmente similares a las prohibidas por las leyes que la FTC hace cumplir[17]. Como parte de esta asistencia, la FTC puede compartir la información obtenida en relación con una investigación de la FTC, emitir procesos obligatorios en nombre de la APD de la UE que lleva a cabo su propia investigación, y recabar testimonios orales de testigos o demandados en relación con el procedimiento de aplicación de la APD, con sujeción a los requisitos de la Ley SAFE WEB de Estados Unidos. La FTC utiliza regularmente esta autoridad para ayudar a otras autoridades de todo el mundo en casos de protección de la intimidad y de los consumidores.

Además de cualquier consulta con las APD de la UE remitentes sobre asuntos específicos, la FTC participará en reuniones periódicas con representantes designados del Consejo Europeo de Protección de Datos ("EDPB") para debatir en términos generales cómo mejorar la cooperación en materia de aplicación. La FTC también participará, junto con el Departamento de Comercio, la Comisión Europea y representantes del EDPB, en la revisión periódica del DPF UE-EE.UU. para debatir su aplicación. La FTC también fomenta el desarrollo de herramientas que mejoren la cooperación en materia de aplicación de la ley con las APD de la UE, así como con otras autoridades encargadas de velar por el cumplimiento de la privacidad en todo el

17 Para determinar si ejerce su autoridad en virtud de la Ley SAFE WEB de EE.UU., la FTC considera, entre otras cosas: "(A) si la agencia solicitante ha acordado proporcionar o proporcionará asistencia recíproca a la Comisión; (C) si el cumplimiento de la solicitud perjudicaría el interés público de los Estados Unidos; y (C) si la investigación o el procedimiento de aplicación de la agencia solicitante se refiere a actos o prácticas que causan o pueden causar perjuicio a un número significativo de personas." 15 U.S.C. § 46(j)(3). Esta autoridad no se aplica a la aplicación de las leyes de competencia.

mundo. La FTC se complace en afirmar su compromiso de hacer cumplir los aspectos del sector comercial del DPF UE-EE.UU.. Consideramos que nuestra colaboración con los colegas de la UE es fundamental para proteger la intimidad de nuestros ciudadanos y de los suyos.

Atentamente,

Lina M. Khan

Presidente de la Comisión Federal de Comercio

Apéndice A: Cumplimiento del Escudo de Protección de la Intimidad y del Puerto Seguro

	Expediente/Archivo FTC N.°	Caso	Enlace
1	Expediente FTC No. 2023062 Caso No. 3:22-cv-03070 (N.D. Cal.)	US v. Twitter, Inc.	Twitter
2	Expediente FTC No. 192 3209	En el asunto de Residual Pumpkin Entity, LLC, formerly d/b/a CafePress, y PlanetArt, LLC, d/b/a CafePress	CafePress
3	Expediente FTC No. 192 3133 Expediente No. C-4747	En el asunto de Flo Health, Inc.	Flo Health
4	Expediente FTC No. 192 3050 Expediente No. C-4723	En el asunto de Ortho-Clinical Diagnostics, Inc.	Ortho-Clinical
5	Expediente FTC No. 192 3092 Expediente No. C-4709	En el asunto de T&M Protection, LLC	T&M Protection
6	Expediente FTC No. 192 3084 Expediente No. C-4704	En el asunto de TDARX, Inc.	TDARX
7	Expediente FTC No. 192 3093 Expediente No. C-4706	En el asunto de Global Data Vault, LLC	Global Data
8	Expediente FTC No. 192 3078 Expediente No. C-4703	En el asunto de Incentive Services, Inc.	Incentive Services
9	Expediente FTC No. 192 3090 Expediente No. C-4705	En el asunto de Click Labs, Inc.	Click Labs
10	Expediente FTC No. 182 3192 Expediente No. C-4697	En el asunto de Medable, Inc.	Medable
11	Expediente FTC No. 182 3189 Expediente No. 9386	En el asunto de NTT Global Data Centers Americas, Inc., as successor in interest to RagingWire Data Centers, Inc.	RagingWire

	Expediente/Archivo FTC N.°	Caso	Enlace
12	Expediente FTC No. 182 3196 Expediente No. C-4702	En el asunto de Thru, Inc.	Thru
13	Expediente FTC No. 182 3188 Expediente No. C-4698	En el asunto de DCR Workforce, Inc.	DCR Workforce
14	Expediente FTC No. 182 3194 Expediente No. C-4700	En el asunto de LotaData, Inc.	LotaData
15	Expediente FTC No. 182 3195 Expediente No. C-4701	En el asunto de EmpiriStat, Inc.	EmpiriStat
16	Expediente FTC No. 182 3193 Expediente No. C-4699	En el asunto de 214 Technologies, Inc., also d/b/a Trueface.ai	Trueface.ai
17	Expediente FTC No. 182 3107 Expediente No. 9383	En el asunto de Cambridge Analytica, LLC	Cambridge Analytica
18	Expediente FTC No. 182 3152 Expediente No. C-4685	En el asunto de SecureTest, Inc.	SecurTest
19	Expediente FTC No. 182 3144 Expediente No. C-4664	En el asunto de VenPath, Inc.	VenPath
20	Expediente FTC n° 182 3154 Expediente n° C-4666	En el asunto de SmartStart Employment Screening, Inc.	SmartStart
21	Expediente FTC n° 182 3143 Expediente n° C-4663	En el asunto de mResourceLLC, d/b/a Loop Works LLC	mRecurso
22	Expediente FTC n° 182 3150 Expediente n° C-4665	En el asunto de Idmission LLC	IDmisión
23	Expediente FTC n° 182 3100 Expediente n° C-4659	En el asunto de ReadyTech Corporation	ReadyTech
24	Expediente FTC n° 172 3173 Expediente n° C-4630	En el asunto de Decusoft, LLC	Decusoft
25	Expediente FTC n° 172 3171 Expediente n° C-4628	En el asunto Tru Communication, Inc. Tru	
26	Expediente FTC n° 172 3172 Expediente n° C-4629	En el asunto de Md7, LLC	Md7

	Expediente/Archivo FTC N.°	Caso	Enlace
30	Expediente FTC n° 152 3198 Expediente n° C-4543	En el asunto de Jhayrmaine Daniels (d/b/a California Skate-Line)	Jhayrmaine Daniels
31	Expediente FTC n° 152 3190 Expediente n° C-4545	En el asunto de Dale Jarrett Racing Adventure, Inc. Dale Jarrett	
32	Expediente FTC n° 152 3141 Expediente n° C-4540	En el asunto de Golf Connect, LLC	Golf Connect
33	Expediente FTC n° 152 3202 Expediente n° C-4546	En el asunto de Inbox Group, LLC	Grupo Inbox
34	Expediente n° 152 3187 Expediente n° C-4542	En el asunto de IOActive, Inc. IOActive	
35	Expediente FTC n° 152 3140 Expediente n° C-4549	En el asunto de Jubilant Clinsys, Inc. Jubilant	
36	Expediente FTC n° 152 3199 Expediente n° C-4547	En el asunto Just Bagels Manufacturing, Inc. Sólo Bagels	
37	Expediente FTC n° 152 3138 Expediente n° C-4548	En el asunto de NAICS Association, LLC	NAICS
38	Expediente FTC n° 152 3201 Expediente n° C-4544	En el asunto One Industries Corp. Una industria	
39	Expediente FTC n° 152 3137 Expediente n° C-4550	En el asunto Pinger, Inc. Pinger	
40	Expediente FTC n° 152 3193 Expediente n° C-4552	En el asunto de SteriMed Medical Waste Solutions	SteriMed
41	Expediente FTC n° 152 3184 Expediente n° C-4541	En el asunto de Contract Logix, LLC	Contrato Logix
42	Expediente FTC n° 152 3185 Expediente n° C-4551	En el asunto de Forensics Consulting Solutions, LLC	Consultoría forense
43	Expediente FTC n° 152 3051 Expediente n° C-4526	En el asunto de American Int'l Mailing, Inc. AIM	
44	Expediente FTC n° 152 3015 Expediente n° C-4525	En el asunto de TES Franchising, LLC	TES

	Expediente/Archivo FTC N.°	Caso	Enlace
45	Expediente FTC n° 142 3036 Expediente n° C-4459	En el asunto de American Apparel, Inc. American Apparel	
46	Expediente FTC n° 142 3026 Expediente n° C-4469	En el asunto Fantage. com, Inc. Fantage	
47	Expediente FTC n° 142 3017 Expediente n° C-4461	En el asunto de Apperian, Inc. Apperian	
48	Expediente FTC n° 142 3018 Expediente n° C-4462	En el asunto de Atlanta Falcons Football Club, LLC	Halcones de Atlanta
49	Expediente FTC n° 142 3019 Expediente n° C-4463	En el asunto de Baker Tilly Virchow Krause, LLP	Baker Tilly
50	Expediente FTC n° 142 3020 Expediente n° C-4464	En el asunto de BitTorrent, Inc. BitTorrent	
51	Expediente FTC n° 142 3022 Expediente n° C-4465	En el asunto de Charles River Laboratories, Int'l	Río Charles
52	Expediente FTC n° 142 3023 Expediente n° C-4466	En el asunto de DataMotion, Inc. DataMotion	
53	Expediente FTC n° 142 3024 Expediente n° C-4467	En el asunto de DDC Laboratories, Inc., d/b/a DNA Diagnostics Center	DDC
54	Expediente FTC n° 142 3028 Expediente n° C-4470	En el asunto de Level 3 Communications, LLC	Nivel 3
55	Expediente FTC n° 142 3025 Expediente n° C-4468	En el asunto de PDB Sports, Ltd., d/b/a Denver Broncos Football Club, LLP	Broncos
56	Expediente FTC n° 142 3030 Expediente n° C-4471	En el asunto de Reynolds Consumer Products, Inc. Reynolds	
57	Expediente FTC n° 142 3031 Expediente n° C-4472	En el asunto de Receivable Management Services Corporation	Gestión de cobros
58	Expediente FTC n° 142 3032 Expediente n° C-4473	En el asunto de Tennessee Football, Inc. Fútbol Tennessee	

	Expediente/Archivo FTC N.°	Caso	Enlace
59	Expediente FTC n° 102 3058 Expediente n° C-4369	En el asunto de Myspace LLC	Myspace
60	Expediente FTC n° 092 3184 Expediente n° C-4365	En el asunto de Facebook, Inc. Facebook	
61	Expediente FTC n° 092 3081 Acción civil n° 09-CV-		
5276 (C.D. Cal.)	FTC contra Javian Karnani, y Balls of Kryptonite, LLC, d/b/a Bite Size Deals, LLC, y Best Priced Brands, LLC	Bolas de Kriptonita	
62	Expediente FTC n° 102 3136 Expediente n° C-4336	En el asunto de Google, Inc. Google	
63	Expediente FTC n° 092 3137 Expediente n° C-4282	En el asunto de World Innovators, Inc. Innovador es del mundo	
64	Expediente FTC n° 092 3141 Expediente n° C-4271	En el asunto de Progressive Gaitways LLC	Pasarelas progresivas
65	Expediente FTC n° 092 3139 Expediente n° C-4270	En el asunto Onyx Graphics, Inc. Gráficos Onyx	
66	Expediente FTC n° 092 3138 Expediente n° C-4269	En el asunto de ExpatEdge Partners, LLC	ExpatEdge
67	Expediente FTC n° 092 3140 Expediente n° C-4281	En el asunto de Directors Desk LLC	Escritorio de dirección
68	Expediente FTC n° 092 3142 Expediente n° C-4272	En el asunto de Collectify LLC	Recopilar

ANEXO V



The Secretary of Transportation
Washington, DC 20590

6 de julio de 2023

Comisario Didier Reynders Comisión Europea
Rue de la Loi / Wetstraat 200 1049 1049 Bruselas
Bélgica

Estimado Comisario Reynders:

El Departamento de Transporte de los Estados Unidos ("Departamento" o "DOT") agradece la oportunidad de describir su papel en la aplicación de los principios del marco de protección de datos UE-EE.UU. ("DPF UE-EE.UU."). El DPF UE-EE.UU. desempeñará un papel fundamental en la protección de los datos personales facilitados durante las transacciones comerciales en un mundo cada vez más interconectado. Permitirá a las empresas llevar a cabo importantes operaciones en la economía global, garantizando al mismo tiempo que los consumidores de la UE mantengan importantes protecciones de la intimidad.

El Departamento de Transporte expresó públicamente por primera vez su compromiso de hacer cumplir el Marco de Puerto Seguro EE.UU.-UE en una carta enviada a la Comisión Europea hace más de 22 años, compromisos que se repitieron y ampliaron en una carta de 2016 relativa al Marco del Escudo de Privacidad UE-EE.UU.. En esas cartas, el Departamento de Transporte se comprometió a hacer cumplir enérgicamente los principios de privacidad de puerto seguro entre Estados Unidos y la UE, y posteriormente los principios del Escudo de privacidad entre la UE y Estados Unidos. El Departamento de Transporte hace extensivo este compromiso a los principios DPF UE-EE.UU. y la presente carta conmemora dicho compromiso.

En particular, el Departamento de Transporte confirma su compromiso en los siguientes ámbitos clave: 1) dar prioridad a la investigación de las presuntas infracciones de los principios DPF UE-EE.UU.; 2) adoptar las medidas de ejecución adecuadas contra las entidades que hagan afirmaciones falsas o engañosas sobre la participación en los principios DPF UE- EE.UU.; y 3) supervisar y hacer públicas las órdenes de ejecución relativas a las infracciones de los principios DPF UE-EE.UU.. Proporcionamos información sobre cada uno de estos compromisos y, para que el contexto sea necesario, los antecedentes pertinentes sobre el papel del Departamento de Transporte en la protección de la intimidad de los consumidores y la aplicación de los principios DPF UE-EE.UU.

1. Fondo

A. Autoridad de protección de datos del Departamento de Transporte

El Departamento está firmemente comprometido a garantizar la privacidad de la información facilitada por los consumidores a las compañías aéreas y a los agentes de venta de billetes. La autoridad del Departamento de Transporte para actuar en este ámbito se encuentra en el 49 U.S.C. 41712, que prohíbe a una compañía aérea o a un agente de venta de billetes realizar "prácticas desleales o engañosas" en el transporte aéreo o en la venta de transporte aéreo. El artículo 41712 sigue el modelo del artículo 5 de la Ley de la Comisión Federal de Comercio (FTC) (15 U.S.C. 45). Recientemente, el DOT ha publicado una normativa que define las prácticas desleales y engañosas, en consonancia con los precedentes tanto del DOT como de la FTC (14 CFR § 399.79). En concreto, una práctica es "desleal" si causa o puede causar un perjuicio sustancial que no sea razonablemente evitable y si el perjuicio no se ve compensado por los beneficios para los consumidores o la competencia. Una práctica es "engañosa" para los consumidores si es probable que inducir a error a un consumidor, que actúe razonablemente dadas las circunstancias, con respecto a un asunto importante. Un asunto es material si es probable que haya afectado a la conducta o decisión del consumidor con respecto a un producto o servicio. Aparte de estos principios generales, el Departamento de Transporte interpreta específicamente el artículo 41712 en el sentido de que prohíbe a los transportistas y agentes de venta de billetes: (1) infringir los términos de su política de privacidad; (2) infringir cualquier norma emitida por el Departamento que identifique prácticas específicas de privacidad como desleales o engañosas; o (3) infringir la Ley de protección de la privacidad infantil en línea (COPPA) o las normas de la FTC que aplican la COPPA; o (4) incumplir, como participante en el DPF UE-EE.UU., los principios del DPF UE-EE.UU.[1].

Como se ha señalado anteriormente, en virtud de la legislación federal, el Departamento de Transporte tiene autoridad exclusiva para regular las prácticas de privacidad de las compañías aéreas, y comparte jurisdicción con la FTC con respecto a las prácticas de privacidad de los agentes de venta de billetes en la venta de transporte aéreo.

Así pues, una vez que un transportista o vendedor de transporte aéreo se compromete públicamente a respetar los principios DPF UE-EE.UU., el Departamento puede hacer uso de las facultades que le confiere el artículo 41712 para garantizar el cumplimiento de dichos principios. Por lo tanto, una vez que un pasajero proporciona información a un transportista o agente de venta de billetes que se ha comprometido a respetar los principios DPF UE-EE.UU., cualquier incumplimiento por parte del transportista o agente de venta de billetes constituiría una infracción del artículo 41712.

B. Prácticas de aplicación

La Oficina de Protección del Consumidor de Aviación (Office of Aviation Consumer Protection, OACP) del Departamento[2] investiga y persigue los casos contemplados en el 49 U.S.C. 41712. Aplica la prohibición legal del artículo 41712 contra las prácticas desleales y engañosas principalmente mediante la negociación, la preparación de órdenes de cese y desistimiento y la redacción de órdenes de imposición de sanciones civiles. La oficina se entera de posibles infracciones en gran medida por las quejas que recibe de particulares, agencias de viajes, compañías aéreas y organismos

1 https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.

2 Anteriormente denominada Oficina de Ejecución y Procedimientos Aeronáuticos.

gubernamentales estadounidenses y extranjeros. Los consumidores pueden utilizar el sitio web del Departamento de Transporte para presentar denuncias contra compañías aéreas y agencias de viajes[3].

Si no se llega a un acuerdo razonable y apropiado en un caso, la OACP está facultada para iniciar un procedimiento de ejecución que implique una audiencia probatoria ante un juez de derecho administrativo ("ALJ") del Departamento de Transporte. El ALJ está facultado para dictar órdenes de cese y sanciones civiles. Las infracciones del artículo 41712 pueden dar lugar a la emisión de órdenes de cese y desistimiento y la imposición de sanciones civiles de hasta 37.377 dólares por cada infracción del artículo 41712.

El Departamento no está facultado para conceder indemnizaciones o compensaciones pecuniarias a los denunciantes. Sin embargo, sí está facultado para aprobar acuerdos resultantes de investigaciones llevadas a cabo por su OACP que beneficien directamente a los consumidores (por ejemplo, dinero en efectivo, vales) como compensación a las sanciones pecuniarias que de otro modo deberían pagarse al Gobierno de Estados Unidos. Esto ha ocurrido en el pasado, y también puede ocurrir en el contexto del acuerdo UE-EE. DPF cuando las circunstancias lo justifiquen. Las violaciones repetidas de la sección 41712 por una aerolínea plantearían cuestiones sobre la disposición de esta a cumplir la normativa, lo que, en situaciones graves, podría dar lugar a que se considerara que una aerolínea ya no es apta para operar y, por lo tanto, perdiera su autoridad de explotación económica.

Hasta la fecha, el Departamento de Transporte ha recibido relativamente pocas denuncias de supuestas violaciones de la intimidad por parte de agentes de venta de billetes o compañías aéreas. Cuando surgen, se investigan de acuerdo con los principios expuestos anteriormente.

C. Las protecciones jurídicas del DOT benefician a los consumidores de la UE

En virtud del artículo 41712, la prohibición de prácticas desleales o engañosas en el transporte aéreo o la venta de transporte aéreo se aplica a las compañías aéreas estadounidenses y extranjeras, así como a los agentes de venta de billetes. El Departamento de Transporte actúa con frecuencia contra compañías aéreas estadounidenses y extranjeras por prácticas que afectan tanto a los consumidores extranjeros como a los estadounidenses, basándose en que las prácticas de la compañía aérea tuvieron lugar en el transcurso de la prestación de servicios de transporte con origen o destino en los Estados Unidos. El Departamento de Transporte utiliza y seguirá utilizando todos los recursos disponibles para proteger a los consumidores extranjeros y estadounidenses de las prácticas desleales o engañosas en el transporte aéreo por parte de las entidades reguladas.

El Departamento de Transporte también aplica, con respecto a las compañías aéreas, otras leyes específicas cuyas protecciones se extienden a los consumidores no estadounidenses, como la Ley de Protección de la Privacidad de los Niños en Internet ("COPPA"). Entre otras cosas, la COPPA exige que los operadores de sitios web y servicios en línea dirigidos a niños, o sitios de audiencia general que recopilen a sabiendas información personal de niños menores de 13 años, proporcionen un aviso a los padres y obtengan su consentimiento verificable. Los sitios web y servicios con sede en Estados Unidos que estén sujetos a la COPPA y recojan información personal de niños extranjeros están obligados a cumplir la COPPA. Los sitios web y servicios en línea con sede en el extranjero también deben cumplir la COPPA si están dirigidos

3 http://www.transportation.gov/airconsumer/privacy-complaints.

a niños en Estados Unidos, o si recopilan a sabiendas información personal de niños en Estados Unidos. En la medida en que las compañías aéreas estadounidenses o extranjeras que operan en Estados Unidos infrinjan la COPPA, el Departamento de Transporte tendría jurisdicción para adoptar medidas coercitivas.

II. Aplicación de los principios DPF UE-EE.UU.

Si una compañía aérea o un agente de venta de billetes opta por participar en el DPF UE- EE.UU. y el Departamento recibe una denuncia de que dicha compañía aérea o agente de venta de billetes ha infringido presuntamente los principios del DPF UE-EE. UU., el Departamento tomaría las siguientes medidas para hacer cumplir enérgicamente los principios del DPF UE- EE.UU.

A. Prioridad de la investigación de presuntas infracciones

La OACP del Departamento investigará todas las denuncias de infracción de los principios del DPF UE-EE.UU., incluidas las denuncias recibidas de las autoridades de protección de datos de la UE ("DPA"), y adoptará medidas coercitivas cuando haya pruebas de infracción. Además, la OACP cooperará con la FTC y el Departamento de Comercio y dará prioridad a las alegaciones de que las entidades reguladas no están cumpliendo los compromisos de privacidad adquiridos como parte del DPF UE-EE. UU.

Al recibir una denuncia de infracción de los principios DPF UE-EE.UU., la OACP puede tomar una serie de medidas como parte de su investigación. Por ejemplo, puede revisar el agente de billetes o la policía privada de la aerolínea, obtener más información del agente responsable del billete de terceros, hacer un seguimiento con la entidad remitente y evaluar si existe un patrón de violaciones o número significativo de consumidores afectados. Además, determinaría si el problema afecta a asuntos que son competencia del Departamento de Comercio o de la FTC, evaluaría si la educación de los consumidores y de las empresas sería útil y, en su caso, iniciaría un procedimiento de aplicación. Además, determinaría si el asunto es competencia del Departamento de Comercio o de la FTC, evaluaría si sería útil educar a los consumidores y a las empresas y, en su caso, iniciaría un procedimiento de aplicación.

Si el Departamento tiene conocimiento de posibles violaciones de los principios DPF UE- EE.UU. por parte de los agentes de venta de billetes, se coordinará con la FTC al respecto. También informaremos a la FTC y al Departamento de Comercio del resultado de cualquier acción de aplicación de los principios DPF UE-EE.UU.

B. Tratamiento de las solicitudes de participación falsas o engañosas

El Departamento mantiene su compromiso de investigar las violaciones de los principios del DPF UE-EE.UU., incluidas las afirmaciones falsas o engañosas de participación en el DPF UE-EE.UU.. Daremos consideración prioritaria a las remisiones del Departamento de Comercio en relación con las organizaciones que identifique como participantes indebidos en el DPF UE-EE.UU. o que utilicen la marca de certificación sin autorización del DPF-UE-EE.UU.

Además, observamos que si la política de privacidad de una organización promete que cumple los principios DPF UE-EE.UU., el hecho de que no realice o mantenga una autocertificación a través del Departamento de Comercio probablemente no eximirá, por sí mismo, a la organización de la aplicación de dichos compromisos por parte del Departamento de Comercio.

C. Supervisión y publicación de las órdenes de ejecución relativas a las infracciones de los DPF UE- EE.UU.

La OACP del Departamento también mantiene su compromiso de supervisar las órdenes de ejecución según sea necesario para garantizar el cumplimiento de los principios DPF UE- EE.UU.. Concretamente, si la oficina emite una orden por la que se ordena a una compañía aérea o a un agente de venta de billetes que cese y desista de cometer futuras infracciones de los principios DPF UE-EE.UU. y del artículo 41712, supervisará el cumplimiento por parte de la entidad de la disposición de cese y desistimiento contenida en la orden. Además, la oficina se asegurará de que las órdenes resultantes de los casos de los principios DPF UE-EE.UU. estén disponibles en su sitio web.

Esperamos seguir colaborando con nuestros socios federales y las partes interesadas de la UE en el proceso UE-EE.UU.DPF.

Espero que esta información le resulte útil. Si tiene alguna pregunta o necesita más información, no dude en ponerse en contacto conmigo.

Atentamente,

Pete Buttigieg

ANEXO VI

U.S. Department of Justice
Criminal Division

Oficina del Fiscal General Adjunto
Washington, D.C. 20530

23 de junio de 2023

Sra. Ana Gallego Torres
Director General de Justicia y Consumidores Comisión Europea
Rue Montoyer/Montoyerstraat 59
1049 Bruselas
Bélgica

Estimada Sra. Directora General Gallego Torres:

La presente carta ofrece un breve resumen de las principales herramientas de investigación utilizadas para obtener datos comerciales y otra información de registros de empresas en Estados Unidos con fines de aplicación de la ley penal o de interés público (civil y reglamentario), incluidas las limitaciones de acceso establecidas en dichas autoridades[1]. Todos los procesos legales descritos en esta carta no son discriminatorios en el sentido de que se utilizan para obtener información de empresas en Estados Unidos, incluidas las empresas que se autocertificarán a través del Marco de Privacidad de Datos UE-EE.UU., sin tener en cuenta la nacionalidad o el lugar de residencia del interesado. Además, las empresas que reciban un procedimiento judicial en Estados Unidos podrán impugnarlo ante los tribunales, como se explica más adelante[2].

1 Este resumen no describe las herramientas de investigación de seguridad nacional utilizadas por las fuerzas de seguridad en investigaciones sobre terrorismo y otras cuestiones de seguridad nacional, incluidas las Cartas de Seguridad Nacional (NSL) para determinada información contenida en informes crediticios, registros financieros y registros de abonados y transacciones electrónicas, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, y para registros electrónicos, 12 U.S.C. § 3414; 15 U. S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162. vigilancia, órdenes de registro, registros comerciales y otras recopilaciones de información en virtud de la Ley de Vigilancia de Inteligencia Extranjera, 50 U.S.C. § 1801 et seq.

2 Esta carta trata de la aplicación de la ley federal y las autoridades reguladoras. Las infracciones de la legislación estatal son investigadas por las autoridades policiales estatales y juzgadas en tribunales estatales. Las autoridades policiales estatales utilizan las órdenes y citaciones emitidas en virtud de la legislación estatal esencialmente de la misma manera que se describe aquí, pero con la posibilidad de que el proceso legal estatal pueda estar

En lo que respecta a la incautación de datos por parte de las autoridades públicas, cabe destacar la Cuarta Enmienda de la Constitución de los Estados Unidos, que establece que "no se violará el derecho del pueblo a la seguridad en sus personas, hogares, documentos y efectos, contra registros e incautaciones irrazonables, y no se expedirá ninguna Orden Judicial, sino por causa probable, apoyada por Juramento o afirmación, y describiendo en particular el lugar que se ha de registrar y las personas o cosas que se han de incautar". Constitución de EE.UU. enmendada. IV. Como el Tribunal Supremo de los Estados Unidos declaró en Berger v. State of New York, "[e]l propósito básico de esta Enmienda, como se reconoce en innumerables decisiones de este Tribunal, es salvaguardar la intimidad y la seguridad de las personas contra las invasiones arbitrarias de los funcionarios gubernamentales". 388 U.S. 41, 53 (1967) (citando Camara v. Mun. Court of San Francisco, 387 U.S. 523, 528 (1967)). En las investigaciones penales nacionales, la Cuarta Enmienda generalmente exige que los agentes del orden obtengan una orden judicial antes de llevar a cabo un registro. Véase Katz v. United States, 389 U.S. 347, 357 (1967). Las normas para la emisión de una orden judicial, como los requisitos de causa probable y particularidad, se aplican a las órdenes judiciales para registros físicos e incautaciones, así como a las órdenes judiciales para el contenido almacenado de comunicaciones electrónicas emitidas en virtud de la Ley de Comunicaciones Almacenadas, como se expone más adelante. Cuando no se aplica el requisito de la orden judicial, la actividad gubernamental sigue estando sujeta a una prueba de "razonabilidad" en virtud de la Cuarta Enmienda. Por lo tanto, la propia Constitución garantiza que el gobierno de EE.UU. no tenga un poder ilimitado o arbitrario para confiscar información privada[3].

Autoridades encargadas de la aplicación de la ley penal:

Los fiscales federales, que son funcionarios del Departamento de Justicia (DOJ), y los agentes federales de investigación, incluidos los agentes de la Oficina Federal de Investigación (FBI), una agencia de aplicación de la ley dentro del DOJ, pueden obligar a las empresas de Estados Unidos a presentar documentos y otra información de registro con fines de investigación penal a través de varios tipos de procesos legales obligatorios, incluidas las citaciones del gran jurado, las citaciones administrativas y las órdenes de registro, y pueden adquirir otras comunicaciones en virtud de las autoridades federales de escuchas telefónicas penales y registros de pluma.

Citaciones del Gran Jurado o para juicio: Las citaciones penales se utilizan para apoyar investigaciones policiales específicas. Una citación del gran jurado es una solicitud oficial emitida por un gran jurado (normalmente a petición de un fiscal federal) para apoyar una investigación del gran jurado sobre una presunta violación concreta de la ley penal. Los grandes jurados son un objetivo de investigación del tribunal y son convocados por un juez o magistrado. Una citación puede requerir que alguien testi-

sujeto a protecciones adicionales previstas por las constituciones o estatutos estatales que superen las de la Constitución de EE.UU. Las protecciones de la ley estatal deben ser al menos iguales a las de la Constitución de los EE.UU., incluida, entre otras, la Cuarta Enmienda.

3 Con respecto a los principios de la Cuarta Enmienda sobre la salvaguarda de los intereses de privacidad y seguridad que s e han analizado anteriormente, los tribunales estadounidenses aplican regularmente esos principios a los nuevos tipos de herramientas de investigación de las fuerzas del orden que permiten los avances tecnológicos. Por ejemplo, en 2018, el Tribunal Supremo dictaminó que la adquisición por parte del gobierno, en una investigación policial, de información histórica sobre la ubicación del sitio celular de una compañía de telefonía celular durante un período prolongado de tiempo es una "búsqueda" sujeta al requisito de orden judicial de la Cuarta Enmienda. Carpenter contra Estados Unidos, 138 S. Ct. 2206 (2018).

fique en un procedimiento, o que presente o ponga a disposición registros comerciales, información almacenada electrónicamente u otros elementos tangibles. La información debe ser relevante para la investigación y la citación no puede ser irrazonable por ser excesivamente amplia, o por ser opresiva o gravosa. Un destinatario puede presentar una moción para impugnar una citación basándose en esos motivos. Véase Fed. R. Crim. P. 17. En circunstancias limitadas, las citaciones judiciales de documentos pueden utilizarse después de que el caso haya sido acusado por el gran jurado.

Autoridad de citación administrativa: Las autoridades de citación administrativa pueden ejercerse en investigaciones penales o civiles. En el contexto de la aplicación de la ley penal, varias leyes federales autorizan el uso de citaciones administrativas para presentar o poner a disposición registros comerciales, información almacenada electrónicamente u otros elementos tangibles relevantes para las investigaciones sobre fraude en la atención sanitaria, abuso de menores, protección del Servicio Secreto, casos de sustancias controladas e investigaciones del Inspector General que impliquen a organismos gubernamentales. Si el gobierno trata de hacer cumplir una citación administrativa en los tribunales, el destinatario de la citación administrativa, al igual que el destinatario de una citación del gran jurado, puede argumentar que la citación no es razonable porque es demasiado amplia, o porque es opresiva o gravosa.

Órdenes judiciales para el registro de pluma y la trampa y rastreo: En virtud de las disposiciones penales de registro y seguimiento, las fuerzas de seguridad pueden obtener una orden judicial para adquirir información en tiempo real, información no contenida sobre marcación, encaminamiento, direccionamiento y señalización de un número de teléfono o correo electrónico previa certificación de que la información facilitada es pertinente para una investigación penal pendiente. Véase 18 U.S.C. §§ 3121-3127. El uso o instalación de un dispositivo de este tipo al margen de la ley constituye un delito federal.

Ley de Privacidad de las Comunicaciones Electrónicas (ECPA): Existen normas adicionales que regulan el acceso del gobierno a la información de los abonados, los datos de tráfico y el contenido almacenado de las comunicaciones en poder de los proveedores de servicios de Internet (también conocidos como "ISP"), las compañías telefónicas y otros proveedores de servicios de terceros, de conformidad con el Título II de la ECPA, también llamada Ley de Comunicaciones Almacenadas (SCA), 18 U.S.C. §§ 2701-2712. La SCA establece un sistema de derechos legales de privacidad que limitan el acceso de las fuerzas de seguridad a los datos más allá de lo que exige el derecho constitucional a los clientes y abonados de los ISP. La SCA establece niveles crecientes de protección de la intimidad en función del grado de intrusión de la recopilación. Para la información de registro de los abonados, las direcciones de Protocolo de Internet (IP) y las marcas de tiempo asociadas, y la información de facturación, las autoridades penales deben obtener una citación. Para la mayoría del resto de la información almacenada que no sea de contenido, como los encabezamientos de los correos electrónicos sin el asunto, las fuerzas de seguridad deben presentar ante un juez hechos concretos que demuestren que la información solicitada es relevante y material para una investigación penal en curso. Para obtener el contenido almacenado de las comunicaciones electrónicas, por lo general, las autoridades encargadas de la aplicación de la ley penal deben obtener una orden de un juez basada en una causa probable para creer que la cuenta en cuestión contiene pruebas de un delito. La SCA también contempla la responsabilidad civil y las sanciones penales[4].

4 Además, la sección 2705(b) de la SCA autoriza al gobierno a obtener una orden judicial, basada en una necesidad demostrada de protección contra la divulgación, que prohíba a un proveedor de servicios de comunicaciones notificar voluntariamente a sus usuarios la recepción de un proceso legal de la SCA. En octubre de 2017, el Fiscal General Adjunto Rod Rosenstein emitió un memorando dirigido a los abogados y agentes del DOJ en el

Órdenes judiciales de vigilancia de conformidad con la ley federal de escuchas telefónicas: Además, las fuerzas del orden pueden interceptar en tiempo real comunicaciones telefónicas, orales o electrónicas con fines de investigación criminal de conformidad con la ley federal de escuchas telefónicas. Véase 18 U.S.C. §§ 2510-2523. Esta autoridad sólo está disponible en virtud de una orden judicial en la que un juez determine, entre otras cosas, que existe causa probable para creer que la intervención telefónica o electrónica producirá pruebas de un delito federal, o el paradero de un fugitivo que huye de la persecución. La ley prevé responsabilidad civil y sanciones penales en caso de violación de las disposiciones relativas a las escuchas telefónicas.

Orden de registro-Fed. R. Crim. P. Rule 41: Las fuerzas del orden pueden registrar físicamente locales en Estados Unidos cuando un juez lo autorice. Las fuerzas del orden deben demostrar al juez, basándose en una causa probable, que se ha cometido o se va a cometer un delito y que es probable que se encuentren objetos relacionados con el delito en el lugar especificado en la orden. Esta autoridad se utiliza a menudo cuando es necesario que la policía realice un registro físico de un local debido al peligro de que se destruyan pruebas si se notifica a la empresa una citación u otra orden de presentación. Una persona sujeta a un registro o cuyos bienes sean objeto de un registro puede solicitar la supresión de las pruebas obtenidas o derivadas de un registro ilegal si dichas pruebas se presentan contra esa persona durante un juicio penal. Véase Mapp v. Ohio, 367 U.S. 643 (1961). Cuando se exige a un titular de datos que revele datos en virtud de una Si la parte obligada tiene una orden judicial, puede impugnar el requisito de revelación por considerarlo excesivamente oneroso. Véase In re Application of United States, 610 F .2d 1148, 1157 (3d Cir . 1979) (donde se sostiene que "el debido proceso exige una audiencia sobre la cuestión de la onerosidad antes de obligar a una compañía telefónica a proporcionar" asistencia con una orden de registro); In re Application of United States, 616 F.2d 1122 (9th Cir. 1980) (donde se llega a la misma conclusión basándose en la autoridad supervisora del tribunal).

Directrices y políticas del DOJ: Además de estas limitaciones constitucionales, estatutarias y normativas al acceso del gobierno a los datos, el Fiscal General ha publicado directrices que imponen más límites al acceso de las fuerzas de seguridad a los datos, y que también contienen protecciones de la intimidad y de las libertades civiles. Por ejemplo, las Directrices del Fiscal General para las operaciones nacionales del FBI (septiembre de 2008) (en lo sucesivo, Directrices AG FBI), disponibles en http://www.justice.gov/archive/opa/docs/guidelines.pdf, establecen límites al uso de medios de investigación para buscar información relacionada con investigaciones que impliquen delitos federales. Estas directrices exigen que el FBI utilice los métodos de investigación menos intrusivos posibles, teniendo en cuenta el efecto sobre la privacidad y las libertades civiles y el daño potencial a la reputación. Además, señalan que "es axiomático que el FBI debe llevar a cabo sus investigaciones y otras actividades de una manera legal y razonable que respete la libertad y la privacidad y evite intrusiones innecesarias en las vidas de las personas respetuosas de la ley". Directrices AG del FBI en 5. El FBI ha aplicado estas directrices a través de la Guía de Investigaciones y Operaciones Domésticas del FBI (DIOG), disponible en https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20

que se establecen directrices para garantizar que las solicitudes de tales órdenes de protección se adapten a los hechos y preocupaciones específicos de una investigación y se establece un límite general de un año sobre el tiempo que una solicitud puede tratar de retrasar la notificación. En mayo de 2022, la Fiscal General Adjunta Lisa Monaco publicó orientaciones complementarias sobre el tema, que entre otras cosas establecían los requisitos de aprobación interna del DOJ para las solicitudes de prórroga de una orden de protección más allá del período inicial de un año y exigían la terminación de las órdenes de protección al cierre de una investigación.

Guide%20%28DIOG%29, un completo manual que incluye límites detallados sobre el uso de herramientas de investigación y orientaciones para garantizar que las libertades civiles y la privacidad estén protegidas en cada investigación. En el Manual de Justicia, también disponible en línea en https://www.justice.gov/jm/justicemanual, se establecen normas y políticas adicionales que prescriben limitaciones a las actividades de investigación de los fiscales federales.

Autoridades civiles y reguladoras (interés público):

También existen límites significativos al acceso civil o reglamentario (es decir, de "interés público") a los datos en poder de las empresas en Estados Unidos. Los organismos con responsabilidades civiles y reglamentarias pueden expedir citaciones a las empresas para obtener registros comerciales, información almacenada electrónicamente u otros elementos tangibles. Estos organismos están limitados en el ejercicio de s u autoridad de citación administrativa o civil no sólo por sus estatutos orgánicos, sino también por la revisión judicial independiente de las citaciones antes de su posible aplicación judicial. Véase, por ejemplo, Fed. R. Civ. P. 45. Las agencias sólo pueden solicitar el acceso a los datos que sean relevantes para los asuntos dentro de su ámbito de autoridad para regular. Además, el receptor de una citación administrativa puede impugnar la ejecución de dicha citación ante un tribunal presentando pruebas de que la agencia no ha actuado de acuerdo con las normas básicas de razonabilidad, como se ha comentado anteriormente.

Existen otras bases jurídicas para que las empresas impugnen las solicitudes de datos de los organismos administrativos en función de sus sectores específicos y de los tipos de datos que posean. Por ejemplo, las instituciones financieras pueden impugnar las citaciones administrativas que solicitan determinados tipos de información por considerar que infringen la Ley de Secreto Bancario y sus reglamentos de aplicación. 31 U. S.C. § 5318; 31 C.F.R. Capítulo X. Otras empresas pueden ampararse en la Fair Credit Reporting Act, 15 U.S.C. § 1681b, o en una serie de leyes específicas de otros sectores. El uso indebido de la autoridad de citación de una agencia puede dar lugar a la responsabilidad de la agencia, o a la responsabilidad personal de los funcionarios de la agencia. Véase, por ejemplo, Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3423. Así pues, los tribunales de los Estados Unidos actúan como guardianes contra las solicitudes reglamentarias indebidas y proporcionan una supervisión independiente de las acciones de los organismos federales.

Por último, cualquier poder legal que tengan las autoridades administrativas para incautar físicamente registros de una empresa en Estados Unidos en virtud de un registro administrativo debe cumplir los requisitos basados en la Cuarta Enmienda. Véase See v. City of Seattle, 387 U.S. 541 (1967).

Conclusión:

Todas las actividades policiales y reguladoras en Estados Unidos deben ajustarse a la legislación aplicable, incluida la Constitución, los estatutos, las normas y los reglamentos estadounidenses. Dichas actividades también deben cumplir las políticas aplicables, incluidas las Directrices del Fiscal General que rigen las actividades policiales federales. El marco jurídico descrito anteriormente limita la capacidad de las fuerzas del orden y los organismos reguladores de Estados Unidos para obtener información de empresas en Estados Unidos, tanto si la información se refiere a personas estadounidenses como a ciudadanos de países extranjeros, y además permite la revisión judicial de cualquier solicitud gubernamental de datos en virtud de estas autoridades.

Bruce C. Swartz
Deputy Assistand Attoney General and Counselor for International Affair

ANEXO VII

Oficina del Director de Inteligencia Nacional
Oficina del Consejero General
WASHINGTON, DC 20511

9 de diciembre de 2022

Leslie B. Kiernan
Consejero General Departamento de Comercio de EE.UU.
1401 Constitution Ave., NW
Washington, DC 20230

Estimada Sra. Kiernan,

El 7 de octubre de 2022, el Presidente Biden firmó la Orden Ejecutiva 14086, Mejora de las salvaguardias para las actividades de inteligencia de señales de Estados Unidos, que refuerza el riguroso conjunto de salvaguardias de privacidad y libertades civiles que se aplican a las actividades de inteligencia de señales de Estados Unidos. Estas salvaguardias incluyen exigir que las actividades de inteligencia de señales respondan a objetivos legítimos enumerados; prohibir explícitamente tales actividades para la consecución de objetivos prohibidos específicos; establecer procedimientos novedosos para garantizar que las actividades de inteligencia de señales promuevan estos objetivos legítimos y no promuevan objetivos prohibidos; Exigir que las actividades de inteligencia de señales se lleven a cabo sólo después de una determinación, basada en una evaluación razonable de todos los factores pertinentes, de que las actividades son necesarias para promover una prioridad de inteligencia validada y sólo en la medida y de una manera que sea proporcional a la prioridad de inteligencia validada para la que han sido autorizadas; y ordenar a los elementos de la Comunidad de Inteligencia (CI) que actualicen sus políticas y procedimientos para reflejar las salvaguardias de inteligencia de señales exigidas por la orden ejecutiva y lo que es más importante, el Decreto también introduce un mecanismo independiente y vinculante que permite a las personas de los "Estados cualificados", designados en virtud del Decreto, solicitar reparación si creen que han sido objeto de actividades ilegales de inteligencia de señales de Estados Unidos, incluidas las actividades que violan las protecciones establecidas en el Decreto.

La promulgación por el Presidente Biden de la Orden Ejecutiva 14086 supuso la culminación de más de un año de minuciosas negociaciones entre representantes de la Comisión Europea (CE) y de los Estados Unidos, y establece las medidas que los Estados Unidos adoptarán para cumplir los compromisos contraídos en virtud del Marco de protección de datos entre la UE y los Estados Unidos. En consonancia con el espíritu de cooperación que dio lugar al Marco, tengo entendido que ha recibido usted dos series de preguntas de la CE sobre cómo aplicará el CI el Decreto. Me complace responder a estas preguntas con la presente carta.

Sección 702 de la Ley de Vigilancia de Inteligencia Extranjera de 1978 (FISA Sección 702)

El primer grupo de preguntas se refiere a la Sección 702 de la FISA, que permite la recopilación de información de inteligencia extranjera a través de la selección de personas no estadounidenses que se cree razonablemente que se encuentran fuera de los Estados Unidos con la asistencia obligada de los proveedores de servicios de comunicaciones electrónicas. En concreto, las preguntas se refieren a la interacción entre esa disposición y el Decreto 14086, así como a las demás salvaguardias que se aplican a las actividades realizadas en virtud del artículo 702 de la FISA.

Para empezar, podemos confirmar que el CI aplicará las salvaguardias establecidas en el Decreto 14086 a las actividades realizadas en virtud del artículo 702 de la FISA.

Además, se aplican otras numerosas salvaguardias al uso que hace el Gobierno de la Sección 702 de la FISA. Por ejemplo, todas las certificaciones de la Sección 702 de la FISA deben estar firmadas por e l Fiscal General y el Director de Inteligencia Nacional (DNI), y el Gobierno debe presentar todas esas certificaciones para su aprobación por el Tribunal de Vigilancia de Inteligencia Extranjera (FISC), que está compuesto por jueces independientes, vitalicios, que cumplen mandatos no renovables de siete años. Las certificaciones identifican las categorías de información de inteligencia extranjera que deben recopilarse, que deben cumplir la definición legal de información de inteligencia extranjera, a través de la selección de personas no estadounidenses que se cree razonablemente que se encuentran fuera de Estados Unidos. Las certificaciones han incluido información relativa al terrorismo internacional y otros temas, como la adquisición de información relativa a armas de destrucción masiva. Cada certificación anual debe presentarse a la FISC para su aprobación en un paquete de solicitud de certificación que incluye las certificaciones del Fiscal General y del DNI, declaraciones juradas de determinados jefes de agencias de inteligencia y procedimientos de selección de objetivos, procedimientos de minimización y procedimientos de consulta que son vinculantes para el Gobierno. Los procedimientos de selección de objetivos exigen, entre otras cosas, que el CI evalúe razonablemente, basándose en la totalidad de las circunstancias, que es probable que la selección de objetivos conduzca a la recopilación de información de inteligencia extranjera identificada en una certificación de la Sección 702 del PISA.

Además, al recopilar información en virtud de la Sección 702 de la FISA, el CI debe: proporcionar una explicación por escrito de la base de su evaluación, en el momento de la selección de objetivos, de que se espera que el objetivo posea, se espera que reciba o es probable que comunique información de inteligencia extranjera identificada en una certificación de la Sección 702 de la PISA; confirmar que se sigue cumpliendo la norma de selección de objetivos establecida en los procedimientos de selección de objetivos de la Sección 702 de la PISA; y cesar la recopilación si ya no se cumple la norma. Véase U.S. Government Submission to Foreign Intelligence Surveillance Court, 2015 Summcuy of Notable Section 702 Requirements, en 2-3 (15 de julio de 2015).

Exigir al CI que deje constancia por escrito y afirme periódicamente la validez de su evaluación de que los objetivos de la Sección 702 de la FISA cumplen las normas de selección aplicables facilita la supervisión por la FISC de las actividades de selección del CI. Cada evaluación y justificación de la selección de objetivos registrada es revisada cada dos meses por los fiscales de supervisión de inteligencia del Departamento de Justicia (DOJ), que llevan a cabo esta función de supervisión con independencia de las operaciones de inteligencia exterior. La sección del DOJ que realiza esta. En virtud de una norma establecida desde hace tiempo por la FISC, esta función es responsable de informar a la FISC de cualquier violación de los procedimientos aplicables. Esta información, junto con las reuniones periódicas entre la FISC y esta sección del DOJ en relación con la supervisión de la selección de objetivos de la Sección 702

de la FISA, permite a la FISC exigir el cumplimiento de la selección de objetivos de la Sección 702 de la FISA y otros procedimientos y garantizar de otro modo que las actividades del Gobierno sean legales. En particular, la FISC puede hacer esto de varias maneras, incluyendo la emisión de decisiones correctivas vinculantes para poner fin a la autoridad del Gobierno para recopilar contra un objetivo particular, o para modificar o retrasar la recopilación de datos de la Sección 702 de la FISA. La FISC también puede exigir al Gobierno que presente más informes sobre su cumplimiento de los procedimientos de selección de objetivos y otros procedimientos, o exigir cambios en dichos procedimientos.

La recogida "masiva" de información de inteligencia sobre señales

El segundo grupo de preguntas se refiere a la recopilación "masiva" de inteligencia de señales, que se define en el Decreto 14086 como "la recopilación autorizada de grandes cantidades de datos de inteligencia de señales que, debido a consideraciones técnicas u operativas, se adquieren sin utilizar discriminantes (por ejemplo, sin utilizar identificadores específicos o términos de selección)".

Con respecto a estas cuestiones, señalamos en primer lugar que ni la FISA ni las Cartas de Seguridad Nacional autorizan la recogida masiva. Con respecto a la FISA:

- Los Títulos I y III de la FISA, que autorizan respectivamente la vigilancia electrónica y los registros físicos, requieren una orden judicial (con excepciones limitadas, como las circunstancias de emergencia) y exigen siempre una causa probable para creer que el objetivo es una potencia extranjera o un agente de una potencia extranjera. Véase 50 U.S.C. §§ 1805, 1824.
- La USA FREEDOM Act de 2015 modificó el Título IV de FISA, que autoriza el uso de registros de pluma y dispositivos de trampa y rastreo, en virtud de una orden judicial (excepto en circunstancias de emergencia), para exigir al Gobierno que base las solicitudes en un "término de selección específico." Véase 50 U.S.C. § 1842(c)(3).
- El Título V de la FISA, que permite a la Oficina Federal de Investigación (FBI) obtener determinados tipos de registros comerciales, exige una orden judicial basada en una solicitud que especifique que "existen hechos concretos y articulables que dan motivos para creer que la persona a la que pertenecen los registros es una potencia extranjera o un agente de una potencia extranjera". Véase 50 U.S.C. § 1862(b)(2)(B)[1].
- Por último, el artículo 702 de la FISA autoriza la "selección de personas razonablemente que se cree que se encuentran fuera de Estados Unidos para adquirir información de inteligencia extranjera". Véase 50 U.S.C. § 188la(a). Así pues, como ha señalado la Junta de Supervisión de la Privacidad y las Libertades Civiles, la recogida de datos por parte del Gobierno en virtud del artículo 702 de la FISA "consiste enteramente en la selección de personas individuales y la adquisición de comunicaciones asociadas con esas perso-

1 Desde 2001 hasta 2020, el Título V de la FISA permitía al FBI solicitar autorización a la FISC para obtener "cosas tangibles" que fueran relevantes para determinadas investigaciones autorizadas. Véase USA PATRIOT Act, Pub. L. N° 107-56, 115 Stat. 272, § 215 (2001). Este que ha expirado y, por tanto, ya no es ley, proporcionó la autoridad en virtud de la cual el Gobierno recopiló en su día metadatos de telefonía en bloque. Sin embargo, incluso antes de que expirara la disposición, la USA FREEDOM Act la había modificado para exigir al Gobierno que basara una solicitud al FISC en un "término de selección específico". Véase USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, § I 03 (2015).

nas, de las que el Gobierno tiene motivos para esperar que obtendrá determinados tipos de inteligencia extranjera", de modo que el "programa no funciona mediante la recogida de comunicaciones en bloque". Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, en 103 (2 de julio de 2014)[2].

En relación a las cartas de seguridad nacional, la USA FREEDOM Act de 2015 impone un requisito de "plazo de selección específico" para el uso de dichas cartas. Véase 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709(b).

Además, el Decreto 14086 establece que "se dará prioridad a la recogida selectiva" y que, cuando el CI lleve a cabo una recogida masiva, "sólo se autorizará la recogida masiva de inteligencia de señales si se determina... que la información necesaria para avanzar en una prioridad de inteligencia validada no puede obtenerse razonablemente mediante la recogida selectiva". Véase el Decreto 14086, § 2(c)(ii)(A).

Además, cuando el CI determina que la recogida masiva cumple estas normas, el Decreto 14086 establece salvaguardias adicionales. Concretamente, el Decreto exige al CI que, cuando lleve a cabo una recogida masiva, "aplique métodos y medidas técnicas razonables para limitar los datos recogidos a lo estrictamente necesario para hacer avanzar una prioridad de inteligencia validada, minimizando al mismo tiempo la recogida de información no pertinente". Véase id. La Orden también establece que "las actividades de inteligencia de señales", que incluyen la consulta de inteligencia de señales obtenida mediante la recopilación masiva, "sólo se llevarán a cabo tras la determinación, basada en una evaluación razonable de todos los factores pertinentes, de que las actividades son necesarias para avanzar en una prioridad de inteligencia validada". Véase id. § 2(a)(ii)(A). La Orden aplica además este principio al establecer que el CI sólo puede consultar información de inteligencia de señales no minimizada obtenida en masa para la consecución de seis objetivos permitidos, y que dichas consultas deben realizarse con arreglo a políticas y procedimientos que "tengan debidamente en cuenta el impacto [de las consultas] en la intimidad y las libertades civiles de todas las personas, con independencia de su nacionalidad o del lugar en que residan". Véase id. § 2(c)(iii)(D). Por último, la Orden establece controles de tratamiento, seguridad y acceso a los datos recogidos. Véase id. § 2(c)(iii)(A) y§ 2(c)(iii)(B).

Esperamos que estas aclaraciones le sean de utilidad. No dude en ponerse en contacto con nosotros si tiene más preguntas sobre la forma en que el CI de EE.UU. tiene previsto aplicar el Decreto 14086.

Christopher C. Fonzone

Consejero General

2 Los artículos 703 y 704, que autorizan al Consejo Internacional a atacar a personas estadounidenses que se encuentren en el extranjero, exigen una orden judicial (salvo en circunstancias de emergencia) y siempre requieren una causa probable para creer que el objetivo es una potencia extranjera, un agente de una potencia extranjera o un funcionario o empleado de una potencia extranjera. Véase50U.S.C.§§ 1881b, 1881c.



Bruselas, 10.7.2023
C(2023) 4745 final
ANEXOS 8

ANEXOS

a la

DECISIÓN DE APLICACIÓN DE LA COMISIÓN

de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre la UE y los EE.UU.

ANEXO VIII

LISTA DE ABREVIATURAS

En la presente Decisión aparecen las siguientes abreviaturas:

AAA	Asociación Americana de Arbitraje
Reglamento AG	Reglamento del Fiscal General sobre el Tribunal de Revisión de Protección de Datos
AGG-DOM	Directrices del Fiscal General sobre operaciones domésticas del FBI
APA	Ley de Procedimiento Administrativo
CIA	Agencia Central de Inteligencia
CNSS	Comisión de Sistemas de Seguridad Nacional
Tribunal de Justicia	Tribunal de Justicia de la Unión Europea
Decisión	Decisión de Ejecución de la Comisión de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo al nivel adecuado de protección de los datos personales con arreglo al marco de privacidad de datos UE-EE.UU.
DHS	Departamento de Seguridad Interior
DNI	Director de Inteligencia Nacional
DoC	Departamento de Comercio de EE.UU.
DoJ	Departamento de Justicia de EE.UU.
DoT	Departamento de Transportes de EE.UU.
DPA	Autoridad de Protección de Datos
Lista DPF	Lista marco de protección de datos
DPRC	Tribunal de Revisión de la Protección de Datos
ECOA	Ley de igualdad de oportunidades de crédito
ECPA	Ley de privacidad de las comunicaciones electrónicas
EEE	Espacio Económico Europeo
OE 12333	Orden ejecutiva 12333 “Actividades de inteligencia de los Estados Unidos”.

OE 14086, la OE	Orden ejecutiva 14086 "Mejora de las salvaguardias para las actividades de inteligencia de señales de EE.UU.".
EU-U.S. DPF o DPF	Marco de protección de datos UE-EE.UU.
Panel DPF UE-EE.UU.	Panel sobre el marco de privacidad de datos UE- EE.UU.
FBI	Oficina Federal de Investigación
FCRA	Ley de Información Crediticia Equitativa
FISA	Ley de Vigilancia de la Inteligencia Exterior
FISC	Tribunal de Vigilancia de Inteligencia Exterior
FISCR	Tribunal de Revisión de la Vigilancia de Inteligencia Extranjera
FOIA	Ley de libertad de información
FRA	Ley Federal de Registros
FTC	Comisión Federal de Comercio de EE.UU.
HIPAA	Ley de Portabilidad y Responsabilidad de los Seguros Sanitarios
ICDR	Centro Internacional de Resolución de Conflictos
IOB	Junta de Supervisión de Inteligencia
NIST	Instituto Nacional de Normas y Tecnología
NSA	Agencia de Seguridad Nacional
NSL	Carta(s) de Seguridad Nacional
ODNI	Oficina del Director de Inteligencia Nacional
ODNI CLPO, CLPO	Oficial de Protección de las Libertades Civiles del Director de Inteligencia Nacional
OMB	Oficina de Gestión y Presupuesto
OPCL	Oficina de Privacidad y Libertades Civiles del Departamento de Justicia
PCLOB	Consejo de Supervisión de la Privacidad y las Libertades Civiles
PIAB	Consejo Asesor Presidencial sobre Inteligencia
PPD 28	Directiva Política Presidencial 28
Reglamento (UE) 2016/679	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
SAOP	Alto funcionario de la Agencia para la Protección de la Intimidad
Los principios	Principios del marco de privacidad de datos UE- EE.UU.
EE.UU.	Estados Unidos
Unión	Unión Europea

CÓDIGOS **COMENTADOS**

COLEX



LA **EDITORIAL JURÍDICA** DE **REFERENCIA** PARA LOS **PROFESIONALES** DEL **DERECHO** DESDE **1981**

DESCUBRA MÁS OBRAS EN:

www.colex.es

Editorial Colex SL Tel.: 910 600 164 info@colex.es

TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL Y EL NUEVO MARCO DE PRIVACIDAD DE DATOS UE-EE.UU.

El nuevo Marco de Privacidad de Datos UE-EE.UU. introduce nuevas garantías vinculantes al objeto de dar respuesta a cada uno de los motivos de inquietud puestos de manifiesto por el TJUE, en su día, en las Sentencias «Schrems I» y «Schrems II». Entre estas garantías se encuentran la limitación del acceso por parte de los servicios de inteligencia estadounidenses a los datos de la UE y el establecimiento de un Tribunal de Recurso en Materia de Protección de Datos, al que los ciudadanos de la UE tendrán acceso.

Esperemos que con la aprobación de este nuevo Marco de Privacidad de Datos se pueda no sólo «cerrar», definitivamente, la falta de garantías señalada por el TJUE y que provocó la invalidez de los dos marcos de privacidad anteriores (Safe Harbor y Privacy Shield) sino, sobre todo, establecer un nuevo marco seguro y duradero, mediante el que se puedan realizar las transferencias de datos personales necesarias UE-EE.UU.

Este trabajo se centra, tras abordar lo que podríamos denominar «cuestiones generales en materia de transferencias internacionales de datos de carácter personal», en el estudio de los diferentes esfuerzos llevados a cabo a nivel jurídico para establecer un marco regulatorio satisfactorio para las transferencias internacionales de datos de carácter personal UE-EE.UU., haciendo especial hincapié en el nuevo Marco transatlántico de Privacidad de Datos, recientemente aprobado.

ALFONSO ORTEGA GIMÉNEZ



Doctor *Honoris Causa* por la Universidad Autónoma San Sebastián de San Lorenzo (Paraguay) y por el Instituto Interamericano de Investigación y Docencia en Derechos Humanos (México); Doctor en Derecho; Premio extraordinario de Doctorado; Licenciado en Derecho y Master en Comercio Internacional por la Universidad de Alicante. Profesor Titular de Derecho internacional privado de la Universidad Miguel Hernández de Elche (UMH). Director del Observatorio Provincial de la Inmigración de Alicante. Vicedecano de Grado en Derecho de la UMH. Director del Máster Universitario en Abogacía de la UMH. Director de la Cátedra de Relaciones Privadas Internacionales UMH-Ilustre Colegio de Abogados de Orihuela. Ha participado, como autor, coautor, director y/o coordinador en más de 225 libros. Consejero académico del despacho profesional GRUPO ASESOR ROS (https://www.rosgrupoasesor.es)

ISBN: 978-84-1194-073-3

9 788411 940733