COMISIÓN
EUROPEA

Bruselas, 25.7.2024
COM(2024) 357 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Segundo Informe relativo a la aplicación del Reglamento General de Protección de Datos

1 INTRODUCCIÓN

El presente documento constituye el segundo Informe de la Comisión relativo a la aplicación del Reglamento General de Protección de Datos (RGPD), adoptado de conformidad con el artículo 97 del RGPD. El primer informe se adoptó el 24 de junio de 2020 (en lo sucesivo, «informe de 2020») [(1)].

El RGPD es una de las piedras angulares del enfoque de la UE para la transformación digital. Sus principios básicos (un tratamiento leal, seguro y transparente de los datos personales que garantice que las personas sigan teniendo el control sobre ellos) sustentan todas las políticas de la UE que implican el tratamiento de datos personales.

Desde el informe de 2020, la UE ha adoptado una serie de iniciativas destinadas a situar a las personas en el centro de la transición digital. Cada iniciativa persigue un objetivo particular, como crear un entorno en línea más seguro, hacer que la economía digital sea más justa y competitiva, facilitar la investigación pionera, garantizar el desarrollo de una inteligencia artificial (IA) segura y fiable, y crear un auténtico mercado único de datos. En lo que respecta a los datos personales, estas iniciativas se sustentan en el RGPD, el cual también proporciona una base para iniciativas sectoriales que afectan al tratamiento de datos personales, por ejemplo en los ámbitos de los servicios financieros, la salud, el empleo, la movilidad y la aplicación de las leyes.

Existe un amplio consenso entre las partes interesadas, las autoridades de protección de datos y los Estados miembros en cuanto a que, a pesar de algunos retos, el RGPD ha dado resultados importantes para los particulares y las empresas. El enfoque basado en el riesgo y tecnológicamente neutro ofrece una sólida protección de datos a los interesados y establece obligaciones proporcionadas para los responsables y encargados del tratamiento. Al mismo tiempo, deben realizarse nuevos avances en algunos ámbitos. En particular, en los próximos años, la atención debe centrarse en apoyar los esfuerzos de cumplimiento de las partes interesadas, especialmente las pequeñas y medianas empresas (pymes), los pequeños operadores, los investigadores y las organizaciones de investigación, mediante el suministro de orientaciones más claras y prácticas por parte de las autoridades de protección de datos y el logro de una interpretación y una aplicación más coherentes del RGPD en toda la UE.

De conformidad con el artículo 97 del RGPD, la Comisión debe examinar, en particular, la aplicación y el funcionamiento de la transferencia internacional de datos personales a países terceros (es decir, países fuera de la UE/EEE) (capítulo V del RGPD) y los mecanismos de cooperación y coherencia entre las autoridades nacionales de protección de datos (capítulo VII del RGPD). Sin embargo, al igual que en el informe de 2020, el presente informe proporciona una evaluación general de la aplicación del RGPD que va más allá de estos dos elementos: también señala una serie de acciones necesarias para apoyar la aplicación eficaz del RGPD en ámbitos prioritarios clave.

El presente informe tiene en cuenta las siguientes fuentes: i) la posición y las conclusiones del Consejo, adoptadas en diciembre de 2023 ([2]); ii) las aportaciones recabadas de las partes interesadas, en particular a través del Grupo Multilateral de Expertos sobre el

---

([1]) «La protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos», de 24.6.2020 [COM(2020) 264 final].

([2]) https://data.consilium.europa.eu/doc/document/ST-15507-2023-INIT/es/pdf.

RGPD ([3]) y de una convocatoria pública de datos ([4]), y iii) las aportaciones de las autoridades de protección de datos a través de la contribución del Comité Europeo de Protección de Datos ([5]) (el Comité) y de un informe elaborado por la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) sobre la base de entrevistas realizadas con autoridades de protección de datos individuales ([6]) (el «informe de la FRA»). El informe también se basa en el seguimiento continuado por parte de la Comisión de la aplicación del RGPD, especialmente los diálogos bilaterales con los Estados miembros sobre el cumplimiento de la legislación nacional, la contribución activa a la labor del Comité y contactos estrechos con un amplio abanico de partes interesadas sobre la aplicación práctica del Reglamento.

2 APLICACIÓN DEL RGPD Y FUNCIONAMIENTO DE LOS MECANISMOS DE COOPERACIÓN Y COHERENCIA

El sistema de ventanilla única para el control del cumplimiento del RGPD tiene por objeto garantizar una interpretación y una ejecución armonizadas por parte de autoridades independientes de protección de datos. Dicho sistema exige cooperación entre las autoridades de protección de datos en los casos de tratamiento transfronterizo cuando los interesados de varios Estados miembros se ven sustancialmente afectados. Los conflictos entre autoridades los resuelve el Comité con arreglo al mecanismo de coherencia del RGPD.

2.1 Aumento de la eficiencia en la tramitación de los asuntos transfronterizos: propuesta de normas procedimentales

El informe de 2020 señalaba la necesidad de una tramitación más eficiente y armonizada de los asuntos transfronterizos en toda la UE, en particular a la luz de las grandes diferencias existentes entre los procedimientos administrativos nacionales y las distintas interpretaciones de algunos conceptos del mecanismo de cooperación del RGPD. Por consiguiente, en julio de 2023, la Comisión adoptó una propuesta de Reglamento sobre las normas procedimentales ([7]), basada también en una lista de cuestiones presentadas por el Comité a la Comisión en octubre de 2022 ([8]) y en las aportaciones de las partes interesadas ([9]) y los Estados miembros ([10]). La propuesta complementa el RGPD al establecer normas detalladas sobre las reclamaciones transfronterizas, la participación del

([3]) Puede consultarse un resumen de las aportaciones del Grupo Multilateral de Expertos sobre el RGPD en el siguiente enlace: Report from Multistakeholder Expert group on GDPR application - June 2024.pdf. Las aportaciones recibidas en respuesta a la convocatoria pública de datos y a través de reuniones bilaterales con las partes interesadas se hacen eco en gran medida de las opiniones expresadas por los miembros del Grupo Multilateral de Expertos sobre el RGPD.

([4]) https://ec.europa.eu/info/law/better-regulation/have-your-say_es.

([5]) *Contribution of the EDPB to the evaluation of the GDPR under Article 97* [«Contribución del CEPD a la evaluación del RGPD con arreglo al artículo 97», documento en inglés] | Comité Europeo de Protección de Datos (europa.eu).

([6]) *GDPR in practice – Experiences of data protection authorities* [«El RGPD en la práctica: experiencias de las autoridades de protección de datos», documento en inglés] | Agencia de los Derechos Fundamentales de la Unión Europea (europa.eu).

([7]) Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas procedimentales adicionales en lo que se refiere a la garantía del cumplimiento del Reglamento (UE) 2016/679 [COM(2023) 348 final].

([8]) https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-eu-commission-procedural-aspects-could-be_es.

([9]) A través del Grupo Multilateral de Expertos sobre el RGPD y de una convocatoria de datos puesta en marcha en febrero de 2023.

([10]) En particular a través del Grupo de Expertos de los Estados miembros sobre el RGPD: https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=es&do=groupDetail.groupDetail&groupID=3461.

reclamante, los derechos a las garantías procesales de las partes investigadas (responsables y encargados del tratamiento) y la cooperación entre las autoridades de protección de datos. La armonización de estos aspectos procedimentales contribuiría a una finalización más rápida de las investigaciones y a que los particulares dispusieran de una vía de recurso ágil. En la actualidad, esta propuesta está siendo negociada por el Parlamento Europeo y el Consejo.

2.2 Mayor cooperación entre las autoridades de protección de datos y uso del mecanismo de coherencia

El número de asuntos transfronterizos ha aumentado significativamente en los últimos años. Las autoridades de protección de datos han demostrado una mayor disposición a utilizar las herramientas de cooperación previstas en el RGPD. Todas las autoridades de protección de datos hicieron uso del instrumento de asistencia mutua ([11]), así como de las solicitudes «informales» de asistencia mutua con carácter voluntario. Las autoridades de protección de datos están a favor de las solicitudes informales, que no imponen un plazo ni una obligación estricta de responder. Aunque el Comité adoptó unas directrices sobre operaciones conjuntas en 2021 ([12]), las autoridades todavía no han hecho un uso significativo de este instrumento ([13]) y aluden a las diferencias en los procedimientos nacionales y la falta de claridad sobre el procedimiento como las principales razones de su limitado uso.

El RGPD ofrece a las autoridades de protección de datos interesadas la posibilidad de formular una objeción pertinente y motivada en caso de desacuerdo con un proyecto de decisión de la autoridad de protección de datos principal en un asunto transfronterizo. Cuando las autoridades de protección de datos no puedan alcanzar un consenso sobre una objeción pertinente y motivada, el RGPD prevé que sea el Comité quien resuelva los conflictos ([14]). Los temas que se plantearon con mayor frecuencia en las objeciones pertinentes y motivadas fueron: i) la base jurídica del tratamiento; ii) las obligaciones de información y transparencia; iii) la notificación de violaciones de la seguridad de los datos; iv) los derechos de los interesados; v) las excepciones aplicadas a las transferencias internacionales; vi) el uso de medidas correctoras, y vii) el importe de una multa administrativa.

El sistema de aplicación del RGPD se basa en la premisa de una cooperación leal y efectiva entre las autoridades de protección de datos. Si bien el procedimiento de resolución de conflictos desempeña un papel importante en esta arquitectura de ejecución, debe utilizarse con el ánimo con el que se diseñó, es decir, teniendo debidamente en cuenta el reparto de competencias entre las autoridades de protección de datos, la necesidad de respetar los derechos a las garantías procesales y el interés por lograr una resolución oportuna del caso para los interesados. Cada procedimiento de resolución de conflictos precisa de considerables recursos de la autoridad principal, las autoridades interesadas y la secretaría del Comité, y retrasa la presentación de una solución a los interesados.

([11]) Artículo 61 del RGPD.
([12]) internal_edpb_document_1_2021_on_art_62_joint_operations_en.pdf (europa.eu)
([13]) Artículo 62 del RGPD.
([14]) Artículo 65 del RGPD.

Mayor uso de los instrumentos de cooperación por parte de las autoridades de protección de datos

- Se han registrado casi 2 400 casos en el sistema de intercambio de información del Comité ([15]).
- Las autoridades principales de protección de datos han emitido alrededor de 1 500 proyectos de decisión ([16]), de los cuales 990 dieron lugar a decisiones definitivas en las que se declara una infracción del RGPD ([17]).
- Las autoridades de protección de datos activaron casi 1 000 solicitudes «formales» de asistencia mutua ([18]) y alrededor de 12 300 solicitudes «informales» ([19]).
- Se han iniciado cinco operaciones conjuntas en las que han participado autoridades de protección de datos de siete Estados miembros.
- Las autoridades de protección de datos de dieciocho Estados miembros formularon objeciones pertinentes y motivadas ([20]).

Las autoridades de protección de datos utilizan cada vez más el mecanismo de coherencia del RGPD, el cual consta de tres componentes: i) dictámenes del Comité; ii) resolución de conflictos por el Comité, y iii) el procedimiento de urgencia ([21]).

Cada vez más, el Comité aborda cuestiones importantes de aplicación general en sus dictámenes ([22]). El Comité debe garantizar una consulta oportuna y significativa antes de la adopción de dichos dictámenes. Los asuntos sometidos a resolución de conflictos han abordado cuestiones como la base jurídica para el tratamiento de datos destinado a la publicidad comportamental en las redes sociales y el tratamiento de datos de menores en línea. La mayoría de las decisiones vinculantes posteriores han sido impugnadas ante el Tribunal General.

La transparencia en el proceso de toma de decisiones del Comité es fundamental para garantizar el respeto del derecho a una buena administración en virtud de la Carta de los Derechos Fundamentales de la UE. El procedimiento de urgencia del RGPD permite a las autoridades de protección de datos establecer excepciones al mecanismo de cooperación y coherencia para adoptar medidas urgentes cuando sea necesario para proteger los derechos y libertades de los interesados. Como excepción al procedimiento normal de cooperación en virtud del RGPD, existen instrumentos, como el procedimiento de urgencia, que están concebidos para utilizarse únicamente en circunstancias excepcionales y cuando el

([15]) A 3 de noviembre de 2023 (contribución del Comité).
([16]) De conformidad con el artículo 60, apartado 3, del RGPD.
([17]) A 3 de noviembre de 2023.
([18]) La autoridad irlandesa fue la que más solicitudes formales presentó (246), mientras que las autoridades alemanas fueron las que más solicitudes recibieron (516).
([19]) La autoridad irlandesa fue la que más solicitudes informales presentó (4 245), seguida por las autoridades alemanas (2 036).
([20]) De las 289 objeciones pertinentes y motivadas comunicadas por las autoridades, 101 (35 %) fueron planteadas por las autoridades alemanas. El índice de éxito a la hora de alcanzar un consenso sobre las objeciones pertinentes y motivadas oscila entre el 15 % (de las objeciones formuladas por las autoridades alemanas) y el 100 % (de las objeciones formuladas por la autoridad polaca).
([21]) Artículos 64, 65 y 66 del RGPD, respectivamente.
([22]) Dictámenes en virtud del artículo 64, apartado 2, del RGPD.

procedimiento normal de cooperación no pueda proteger los derechos y libertades de los interesados.

El mecanismo de coherencia

- El Comité ha adoptado 190 dictámenes de coherencia.
- Se han adoptado nueve decisiones vinculantes en materia de resolución de conflictos ([23]). Todas ellas exigían a la autoridad de protección de datos principal que modificara su proyecto de decisión y varias han dado lugar a multas significativas.
- Cinco autoridades de protección de datos adoptaron medidas provisionales en el marco del procedimiento de urgencia (Alemania, España, Finlandia, Italia y Noruega).
- Dos autoridades de protección de datos solicitaron una decisión vinculante urgente al Comité ([24]) y este ordenó medidas definitivas urgentes en un caso.

2.3 Medidas ejecutorias más estrictas

En los últimos años, las autoridades de protección de datos han experimentado un importante repunte en las actividades de control del cumplimiento, especialmente la imposición de multas sustanciales en casos históricos contra grandes multinacionales tecnológicas. Por ejemplo, se impusieron multas por i) infringir la licitud y la seguridad del tratamiento; ii) infringir el tratamiento de categorías especiales de datos personales, y iii) vulnerar los derechos de los particulares ([25]). Esto ha llevado a las empresas privadas a «tomarse en serio la protección de datos» ([26]) y ha contribuido a integrar una cultura del cumplimiento en las organizaciones. Las autoridades de protección de datos adoptan decisiones en las que declaran infracciones del RGPD en casos basados en reclamaciones y por propia iniciativa. Muchas autoridades de protección de datos han hecho un uso eficaz de los procedimientos de «arreglo amistoso» para resolver rápidamente los casos basados en reclamaciones de manera satisfactoria para el reclamante, si bien dichos procedimientos no están disponibles en todos los Estados miembros. La propuesta de normas procedimentales reconoce la posibilidad de que las reclamaciones se resuelvan mediante un arreglo amistoso ([27]).

Las autoridades de protección de datos han hecho un amplio uso de sus poderes correctivos, aunque el número de medidas correctoras impuestas varía considerablemente entre ellas. Aparte de las multas, las medidas correctoras más utilizadas fueron las advertencias, los apercibimientos y las órdenes de cumplimiento del RGPD. Los responsables y encargados del tratamiento impugnan con frecuencia las decisiones por las que se constatan infracciones del RGPD ante los órganos jurisdiccionales nacionales, generalmente aludiendo razones procesales ([28]).

Medidas ejecutorias más estrictas

([23]) De conformidad con el artículo 65, apartado 1, letra a), del RGPD.
([24]) De conformidad con el artículo 66, apartado 2, del RGPD.
([25]) Véase el apartado 5.3.4 de la contribución del Comité.
([26]) Informe de la FRA, p. 36.
([27]) Propuesta de normas procedimentales, artículo 5.
([28]) En Rumanía, la totalidad de las veintiséis decisiones en las que se declaraba la existencia de una infracción fueron recurridas ante los tribunales, mientras que en los Países Bajos el porcentaje de impugnación fue del 23 %. La tasa de éxito de las impugnaciones más elevada fue la de Bélgica (39 %).

- Las autoridades de protección de datos han incoado más de 20 000 investigaciones por iniciativa propia ([29]).
- En conjunto, reciben más de 100 000 reclamaciones al año ([30]).
- El plazo medio de tramitación de las reclamaciones por parte de las autoridades de protección de datos (desde la recepción hasta el cierre del asunto) oscila entre uno y doce meses, y es de tres meses o menos en cinco Estados miembros [Dinamarca (un mes), España (un mes y medio), Estonia (tres meses), Grecia (tres meses) e Irlanda (tres meses)].
- Más de 20 000 reclamaciones se han resuelto por medio de arreglos amistosos, y Austria, Hungría, Luxemburgo e Irlanda son los países donde se utilizan con más frecuencia.
- En 2022, el país con el mayor número de decisiones por las que se impusieron medidas correctoras fue Alemania (3 261), seguido de España (774), Lituania (308) y Estonia (332). El menor número de medidas correctoras se impuso en Liechtenstein (8), Chequia (8), Islandia (10), Países Bajos (17) y Luxemburgo (22).
- Las autoridades de protección de datos han impuesto más de 6 680 multas por un importe aproximado de 4 200 millones EUR ([31]). El mayor importe total de las multas fue impuesto por la autoridad de Irlanda (2 800 millones EUR), seguido de Luxemburgo (746 millones EUR), Italia (197 millones EUR) y Francia (131 millones EUR). Por su parte, los importes más bajos corresponden a Liechtenstein (9 600 EUR), Estonia (201 000 EUR) y Lituania (435 000 EUR).

Si bien la mayoría de las autoridades de protección de datos consideran que sus instrumentos de investigación son adecuados, algunas requieren instrumentos adicionales a nivel nacional, como sanciones adecuadas en caso de que los responsables del tratamiento no cooperen o no faciliten la información necesaria ([32]). Las autoridades de protección de datos consideran que los recursos insuficientes y las lagunas en los conocimientos técnicos y jurídicos son el principal factor que afecta a su capacidad de ejecución ([33]).

2.4 El Comité

El Comité está compuesto por el responsable de una autoridad de protección de datos de cada Estado miembro y por el Supervisor Europeo de Protección de Datos. La Comisión puede participar, pero sin derecho a voto. El Comité, con el apoyo de su secretaría, se encarga de garantizar una aplicación coherente del RGPD ([34]). La mayoría de las autoridades de protección de datos consideran que el Comité ha desempeñado un papel positivo a la hora de reforzar la cooperación entre ellas ([35]). Muchas autoridades de

([29]) Las autoridades de protección de datos de Alemania iniciaron el mayor número de investigaciones por iniciativa propia (7 647), seguidas de Hungría (3 332), Austria (1 681) y Francia (1 571).

([30]) En 2022, nueve autoridades de protección de datos recibieron más de 2 000 reclamaciones. El mayor número de reclamaciones se registró en Alemania (32 300), Italia (30 880), España (15 128), Países Bajos (13 133) y Francia (12 193), mientras que el número más bajo lo registraron Liechtenstein (40), Islandia (140) y Croacia (271).

([31]) Todas las autoridades impusieron multas administrativas, excepto Dinamarca, que no prevé dicha posibilidad. El mayor número de multas se impuso en Alemania (2 106) y España (1 596), y el menor, en Liechtenstein (3), Islandia (15) y Finlandia (20).

([32]) Informe de la FRA, p. 38.

([33]) Informe de la FRA, pp. 20 y 23. Véanse también la posición y las conclusiones del Consejo, apartado 17.

([34]) Artículo 70, apartado 1, del RGPD.

([35]) Informe de la FRA, p. 64.

protección de datos destinan recursos significativos a las actividades del Comité, aunque las más pequeñas argumentan que su tamaño les impide participar plenamente ([36]). Algunas autoridades consideran que debe mejorarse la eficiencia de los procesos del Comité, en particular mediante la reducción del número de reuniones y la prestación de menos atención a cuestiones menores ([37]). Dependiendo del resultado de las negociaciones sobre la propuesta de normas procedimentales relativas al RGPD, que tiene por objeto reducir el número de casos que se presentan al Comité para la resolución de conflictos, es posible que haya que reflexionar sobre si el Comité necesita recursos adicionales.

En noviembre de 2023, el Comité había adoptado 35 directrices. Aunque las partes interesadas y las autoridades de protección de datos las han considerado útiles, también opinan que las directrices deben presentarse con mayor rapidez y que la calidad debe mejorarse ([38]). Las partes interesadas señalan que las directrices a menudo son excesivamente teóricas, demasiado largas y no reflejan el enfoque basado en el riesgo del RGPD ([39]). Las autoridades de protección de datos y el Comité deben proporcionar directrices concisas y prácticas que den respuesta a problemas concretos y reflejen un equilibrio entre la protección de datos y otros derechos fundamentales. También deben ser fáciles de entender para las personas sin formación jurídica, como las pymes y las organizaciones de voluntariado ([40]). Una manera de lograrlo es aumentar la transparencia en la elaboración de las directrices y realizar consultas en una fase temprana para permitir una mejor comprensión de la dinámica del mercado, las prácticas empresariales y la manera de aplicar las directrices en la práctica ([41]). Se acoge con satisfacción el hecho de que, como parte de su Estrategia 2024-2027, el Comité haya destacado su objetivo de proporcionar orientaciones prácticas que resulten accesibles para el público pertinente ([42]).

Las partes interesadas subrayan la necesidad de directrices adicionales, en particular relativas a la anonimización y la seudonimización ([43]), el interés legítimo y la investigación científica ([44]). En el informe de 2020, la Comisión pidió al Comité que adoptara directrices en materia de investigación científica, pero todavía no lo ha hecho. Habida cuenta de la importancia de la investigación científica en la sociedad, en particular para el seguimiento de las enfermedades y el desarrollo de tratamientos y para fomentar la innovación, es esencial que las autoridades de protección de datos tomen medidas para aclarar estas cuestiones sin más demora ([45]). Las autoridades públicas también se beneficiarían de orientaciones para abordar los retos particulares a los que se enfrentan ([46]).

([36]) Informe de la FRA, p. 67. En 2023, las autoridades alemanas de protección de datos fueron las que más recursos dedicaron a las actividades del Comité (26 equivalentes a jornada completa), seguidas de Irlanda (16) y Francia (12) (de acuerdo con la contribución del Comité).
([37]) Informe de la FRA, p. 67.
([38]) Informe de la FRA, p. 67; resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([39]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([40]) Véanse también la posición y las conclusiones del Consejo, apartado 45.
([41]) Véanse también la posición y las conclusiones del Consejo, apartado 34.
([42]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.
([43]) Véanse también la posición y las conclusiones del Consejo, apartado 31, letra d).
([44]) Requieren claridad, en particular, sobre el significado del término «investigación científica», el papel del consentimiento para el tratamiento de datos personales con fines de investigación, la base jurídica pertinente y las funciones y responsabilidades de los agentes participantes.
([45]) Véanse también la posición y las conclusiones del Consejo, apartado 31, letra b).
([46]) Posición y conclusiones del Consejo, apartados 27 a 28.

2.5 Autoridades de protección de datos

2.5.1 Independencia y recursos

La independencia de las autoridades de protección de datos está consagrada en la Carta de los Derechos Fundamentales de la UE y en el Tratado de Funcionamiento de la UE. El RGPD establece requisitos para garantizar la «total independencia» de las autoridades de protección de datos ([47]). El informe de la FRA constató que la mayoría de las autoridades de protección de datos operan con independencia del Gobierno, el Parlamento o cualquier otro organismo público ([48]).

Las autoridades de protección de datos requieren recursos humanos, técnicos y financieros adecuados para poder desempeñar de manera eficaz e independiente las tareas que se les encomiendan en el marco del RGPD. En el informe de 2020, la Comisión señaló que la dotación de recursos de las autoridades de protección de datos seguía sin ser satisfactoria y había planteado sistemáticamente esta cuestión a los Estados miembros. Desde entonces, la situación ha mejorado.

Aumento de los recursos para las autoridades de protección de datos ([49])

- Entre 2020 y 2024, en las autoridades de protección de datos, excepto en dos, se produjo un aumento del personal, y dicho aumento superó el 25 % en 14 Estados miembros.
- La autoridad de protección de datos de Irlanda registró el mayor aumento del personal (79 %), seguida de Estonia y Suecia (ambos 57 %) y Bulgaria (56 %).
- Se produjo una ligera disminución del personal de la autoridad en Chequia (– 1 %), mientras que no hubo aumento en Liechtenstein y se produjeron aumentos menores en Chipre (4 %) y Hungría (8 %).
- Entre 2020 y 2024, en todas las autoridades de protección de datos, excepto en una, se produjo un aumento del presupuesto, y dicho aumento superó el 50 % en 13 Estados miembros.
- La autoridad de protección de datos de Chipre registró el mayor aumento del presupuesto (130 %), seguida de Austria (107 %), Bulgaria (100 %) y Estonia (97 %).
- El presupuesto de la autoridad griega de protección de datos disminuyó un 15 %, mientras que se produjeron pequeños aumentos presupuestarios en las autoridades de Liechtenstein (1 %), Eslovaquia (6 %) y Chequia (8 %).

Aunque estas estadísticas muestran una tendencia general al alza en la dotación de recursos a las autoridades de protección de datos, las propias autoridades consideran que siguen careciendo de recursos humanos suficientes ([50]). Subrayan la necesidad de conocimientos técnicos muy especializados, en particular sobre tecnologías nuevas y emergentes ([51]), cuya ausencia afecta a la cantidad y la calidad de su trabajo, así como las dificultades para

([47]) Artículo 52 del RGPD.
([48]) Informe de la FRA, p. 31.
([49]) Véase el apartado 4.4.1 de la contribución del Comité, también en lo que respecta a las cifras absolutas.
([50]) Solo cinco autoridades de protección de datos consideran que disponen de recursos humanos adecuados (contribución del Comité, página 33).
([51]) Informe de la FRA, p. 20. Algunas autoridades de protección de datos externalizan determinadas tareas a contratistas externos, como la tramitación de reclamaciones, el análisis jurídico y el análisis forense.

competir por los recursos humanos con el sector privado. Las autoridades de protección de datos mencionan la insuficiencia de conocimientos jurídicos y la falta de competencias lingüísticas como factores que afectan a su desempeño. La baja remuneración, la incapacidad de seleccionar al personal de manera autónoma y la pesada carga de trabajo se destacan como factores clave que afectan a la capacidad de las autoridades para contratar y retener al personal ([52]). Las autoridades de protección de datos también subrayan su necesidad de recursos financieros para modernizar y digitalizar sus procesos y adquirir equipos técnicos ([53]). Todas las autoridades de protección de datos desempeñan funciones que van más allá de las que les encomienda el RGPD ([54]), por ejemplo, como autoridades de control en el marco de la Directiva sobre protección de datos en el ámbito penal y la Directiva sobre la intimidad en las comunicaciones electrónicas, mientras que muchas expresan su preocupación por hacer frente a responsabilidades adicionales en virtud de la nueva legislación del ámbito digital ([55]).

2.5.2 Dificultades para tramitar un gran número de reclamaciones

Varias autoridades de protección de datos indican que se utilizan demasiados recursos en la tramitación de las reclamaciones, cuyo número es muy elevado y que en su mayoría son triviales e infundadas, a su juicio, ya que existe la obligación, sujeta a control judicial, de tramitar todas las reclamaciones, de acuerdo con el RGPD ([56]). Esto significa que las autoridades de protección de datos no pueden asignar recursos suficientes a otras actividades, como las investigaciones por iniciativa propia, las campañas de sensibilización pública y la colaboración con los responsables del tratamiento ([57]). Como autoridades públicas, las autoridades de protección de datos tienen la facultad de asignar sus recursos como consideren oportuno para cumplir cada una de sus funciones (enumeradas en el artículo 57, apartado 1, del RGPD) en aras del interés público. Muchas autoridades de protección de datos han adoptado estrategias para aumentar la eficiencia de la tramitación de reclamaciones, como la automatización ([58]), el uso de procedimientos de arreglo amistoso ([59]) y la «agrupación» de reclamaciones relacionadas con cuestiones similares ([60]).

2.5.3 Interpretación del RGPD por parte de las autoridades nacionales de protección de datos

Un objetivo central del RGPD era eliminar el enfoque fragmentado de la protección de datos que existía en virtud de la anterior Directiva sobre protección de datos (Directiva 95/46/CE) ([61]). Sin embargo, las autoridades de protección de datos siguen adoptando interpretaciones divergentes sobre conceptos clave en esta materia ([62]). Las partes interesadas consideran que este es el principal obstáculo para la aplicación coherente del RGPD en la UE. La persistencia de interpretaciones divergentes crea inseguridad jurídica y aumenta los costes para las empresas (por ejemplo, al exigir documentación diferente

([52]) Informe de la FRA, p. 24.
([53]) Informe de la FRA, p. 22.
([54]) Véase el apartado 4.4.5 de la contribución del Comité.
([55]) Contribución del Comité, p. 32.
([56]) Informe de la FRA, p. 48.
([57]) Informe de la FRA, p. 45. Las autoridades de protección de datos consideran especialmente importantes las investigaciones de oficio, ya que los reclamantes pueden no ser conscientes de multitud de infracciones del RGPD.
([58]) Informe de la FRA, p. 8.
([59]) Informe de la FRA, p. 39.
([60]) Informe de la FRA, p. 41.
([61]) Considerando 9 del RGPD.
([62]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

para varios Estados miembros), lo cual perturba la libre circulación de datos personales en la UE, plantea dificultades para las empresas transfronterizas y obstaculiza la investigación y la innovación sobre desafíos sociales urgentes.

Entre las cuestiones específicas planteadas por las partes interesadas figuran las siguientes: i) las autoridades de protección de datos de tres Estados miembros tienen opiniones divergentes sobre la base jurídica adecuada para el tratamiento de datos personales al realizar un ensayo clínico; ii) a menudo existen opiniones divergentes sobre si una entidad constituye un responsable o un encargado del tratamiento, y iii) en algunos casos, las autoridades de protección de datos no siguen las directrices del Comité o publican directrices a escala nacional que entran en conflicto con las del Comité ([63]). Estas cuestiones se agravan cuando varias autoridades de protección de datos de un solo Estado miembro adoptan interpretaciones contradictorias.

Algunas partes interesadas también consideran que determinadas autoridades de protección de datos y el Comité adoptan interpretaciones que se alejan del enfoque basado en el riesgo del RGPD, lo que plantea dificultades para el desarrollo de la economía digital ([64]) y la libertad y pluralidad de los medios de comunicación. Como ámbitos que suscitan preocupación, mencionan los siguientes: i) la interpretación de la anonimización; ii) la base jurídica del interés legítimo y el consentimiento ([65]), y iii) las excepciones a la prohibición de la toma de decisiones individuales automatizadas ([66]). Cabe recordar que las autoridades de protección de datos y el Comité se encargan de garantizar tanto la protección de las personas físicas en relación con el tratamiento de sus datos personales como la libre circulación de datos personales dentro de la UE. Tal y como se consagra en el RGPD ([67]), el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

2.5.4 Colaboración con los responsables y encargados del tratamiento

Las partes interesadas subrayan la ventaja de tener la oportunidad de entablar un diálogo constructivo con las autoridades de protección de datos para garantizar que cumplen el RGPD desde el principio, en particular en relación con las tecnologías emergentes. Las partes interesadas señalan que algunas autoridades de protección de datos colaboran activamente con los responsables del tratamiento, mientras que otras tardan en responder, ofrecen respuestas vagas o no responden ([68]).

3 APLICACIÓN DEL RGPD POR PARTE DE LOS ESTADOS MIEMBROS

3.1 Fragmentación de la aplicación nacional

Si bien el RGPD es directamente aplicable como Reglamento, obliga a los Estados miembros a legislar en determinados ámbitos y les ofrece la posibilidad de especificar en mayor detalle su aplicación en un número limitado de ámbitos ([69]). A la hora de legislar a escala nacional, los Estados miembros deben hacerlo de acuerdo con las condiciones y los límites establecidos por el RGPD. Al igual que en 2020, las partes interesadas informan de dificultades derivadas de la fragmentación de las normas nacionales en las que los Estados

([63]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([64]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([65]) Artículo 6, apartado 1, letra f), y artículo 6, apartado 1, letra a) del RGPD.
([66]) Artículo 22, apartado 2, del RGPD.
([67]) Considerando 4.
([68]) Resumen de las observaciones del grupo multilateral de expertos sobre el RGPD.
([69]) Por ejemplo, la edad mínima para que un niño otorgue su consentimiento en relación con los servicios de la sociedad de la información (artículo 8, apartado 1, del RGPD).

miembros tienen la posibilidad de especificar más el RGPD, en particular en lo que respecta a las siguientes cuestiones:

- la edad mínima para que un niño otorgue su consentimiento en relación con los servicios de la sociedad de la información que se le oferten ([70]);
- la introducción por parte de los Estados miembros de condiciones adicionales relativas al tratamiento de datos genéticos, biométricos o relativos a la salud ([71]);
- el tratamiento de datos personales relativos a condenas e infracciones penales ([72]), lo que crea dificultades en determinados sectores regulados.

Al mismo tiempo, muchas partes interesadas argumentan que los problemas de fragmentación se derivan principalmente de interpretaciones divergentes del RGPD por parte de las autoridades de protección de datos, más que del uso de cláusulas de especificación facultativas por parte de los Estados miembros.

Los Estados miembros consideran que un grado limitado de fragmentación puede ser aceptable y que las cláusulas de especificación previstas en el RGPD siguen siendo beneficiosas, en particular para el tratamiento por parte de las autoridades públicas ([73]). El RGPD exige a los Estados miembros que consulten a su autoridad nacional de protección de datos a la hora de elaborar legislación relativa al tratamiento de datos personales ([74]). Sin embargo, el informe de la FRA constató que algunos Gobiernos fijaban plazos muy ajustados para dichas autoridades y, en algunos casos, no las consultaban ([75]).

3.2 Seguimiento por parte de la Comisión

La Comisión supervisa la aplicación del RGPD de forma continua y ha incoado procedimientos de infracción contra los Estados miembros sobre cuestiones como la independencia de las autoridades de protección de datos (especialmente la ausencia de influencia externa y la disponibilidad de acciones judiciales en caso de desestimación) ([76]) y el derecho a la tutela judicial efectiva de los interesados cuando la autoridad de protección de datos no dé curso a una reclamación ([77]). Como parte de su seguimiento, la Comisión también pide que las autoridades de protección de datos faciliten, con carácter estrictamente confidencial, información periódica ([78]) sobre los casos transfronterizos a gran escala en curso, en particular los relativos a grandes multinacionales tecnológicas,

La Comisión se comunica periódicamente con los Estados miembros sobre la aplicación del RGPD. Como se expuso en el informe de 2020, la Comisión ha seguido utilizando el grupo de expertos de los Estados miembros sobre el RGPD ([79]) para facilitar los debates y el intercambio de experiencias sobre la aplicación efectiva del RGPD. El grupo de expertos ha mantenido debates específicos sobre las siguientes cuestiones: i) el control de los tribunales en el ejercicio de su función judicial (artículo 55 del RGPD; artículo 8 de la

([70]) Artículo 8, apartado 1, del RGPD.
([71]) Una posibilidad prevista en el artículo 9, apartado 4, del RGPD.
([72]) Artículo 10 del RGPD.
([73]) Posición y conclusiones del Consejo, apartado 30.
([74]) Artículo 36 del RGPD.
([75]) Informe de la FRA, p. 11.
([76]) Bélgica (2021/4045) y Bélgica (2022/2160).
([77]) Finlandia (2022/4010) y Suecia (2022/2022).
([78]) En la que se incluyan la referencia del asunto, el tipo de investigación (por iniciativa propia o a raíz de una reclamación), un resumen del alcance de la investigación, las autoridades de protección de datos afectadas, los principales trámites procesales adoptados y sus fechas, las medidas de investigación o cualquier otra medida adoptada y sus fechas.
([79]) https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=es&do=groupDetail.groupDetail&groupID=3461.

Carta); ii) la conciliación del derecho a la protección de los datos personales con el derecho a la libertad de expresión (artículo 85 del RGPD), y iii) el derecho a la tutela judicial efectiva contra una autoridad de control (artículo 78 del RGPD). Tras estos debates, la Comisión recopiló resúmenes de los enfoques adoptados en la aplicación de dichas disposiciones en los Estados miembros ([80]). La Comisión también utilizó este grupo para intercambiar puntos de vista con los Estados miembros a la hora de preparar la propuesta de normas procedimentales.

La conformidad de la legislación y de las prácticas nacionales con las normas de protección de datos establecidas en el corpus de Derecho de la UE sobre el espacio Schengen también se evalúa como parte de las evaluaciones de Schengen, realizadas conjuntamente por los Estados miembros y la Comisión. Se llevan a cabo al menos cinco evaluaciones de protección de datos *in situ* al año, que actualmente se centran en sistemas informáticos de gran magnitud y el Sistema de Información de Schengen, el Sistema de Información de Visados y en la función control de las autoridades nacionales de protección de datos sobre dichos sistemas.

La Comisión está contribuyendo activamente al gran número de asuntos incoados ante el Tribunal de Justicia (con alrededor de treinta procedimientos prejudiciales al año en los últimos años), el cual desempeña un papel fundamental en la interpretación coherente de conceptos clave del RGPD. Un corpus de jurisprudencia del Tribunal cada vez más extenso ha aportado diversas aclaraciones, tales como la definición de conceptos como datos personales ([81]), categorías especiales de datos personales ([82]), responsable del tratamiento ([83]), consentimiento ([84]), interés legítimo ([85]), derecho de acceso ([86]), derecho de supresión ([87]), derecho a indemnización ([88]), toma de decisiones individuales automatizada ([89]), multas administrativas ([90]), delegados de protección de datos ([91]), publicación de datos personales en registros ([92]) y la aplicación del RGPD a las actividades de los parlamentos ([93]).

4 DERECHOS DE LOS INTERESADOS

Sensibilización de la ciudadanía sobre el RGPD y las autoridades de protección de datos (Eurobarómetro 549 de 2024 sobre justicia, derechos y valores)

- El 72 % de los encuestados de toda la UE afirman haber oído hablar del RGPD, incluido un 40 % que sabe lo que es.

([80]) https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=es&meetingId=31754&fromExpertGroups=3461.
([81]) Asunto C-319/22, ECLI:EU:C:2023:837.
([82]) Asuntos C-184/20, ECLI:EU:C:2022:601; C-252/21, ECLI:EU:C:2023:537.
([83]) Asuntos C-683/21, ECLI:EU:C:2023:949; C-604/22, ECLI:EU:C:2024:214; C-231/22, ECLI:EU:C:2024:7.
([84]) Asunto C-61/19, ECLI:EU:C:2020:901.
([85]) Asuntos C-597/19, ECLI:EU:C:2021:492; C-252/21, ECLI:EU:C:2023:537.
([86]) Asuntos C-307/22, ECLI:EU:C:2023:811; C-154/21, ECLI:EU:C:2023:3.
([87]) Asunto C-460/20, ECLI:EU:C:2022:962.
([88]) Asunto C-300/21, ECLI:EU:C:2023:370; asunto C-687/21, ECLI:EU:C:2024:72; asunto C-667/21, ECLI:EU:C:2023:1022.
([89]) Asuntos acumulados C-26/22 y C-64/22, ECLI:EU:C:2023:958.
([90]) Asuntos C-807/21, ECLI:EU:C:2023:950; Asunto C-683/21, ECLI:EU:C:2023:949.
([91]) Asunto C-453/21, ECLI:EU:C:2023:79.
([92]) Asuntos C-439/19, ECLI:EU:C:2021:504; C-184/20, ECLI:EU:C:2022:601.
([93]) Asuntos C-33/22, ECLI:EU:C:2024:46; C-272/19, ECLI:EU:C:2020:535.

- En 19 Estados miembros, más del 70 % de los encuestados indicaron haber oído hablar del RGPD, con Suecia a la cabeza (92 %), seguida de Países Bajos (88 %), Malta y Dinamarca (84 %), mientras que los países con porcentajes más bajos fueron Bulgaria (59 %), Lituania (63 %) y Francia (64 %).
- El 68 % de los encuestados de la UE indican que han oído hablar de una autoridad nacional responsable de proteger sus derechos en materia de protección de datos, y el 24 % de todos los encuestados afirma saber también de qué autoridad se trata.
- En todos los Estados miembros, al menos la mitad de los encuestados ha oído hablar de dicha autoridad nacional, con los niveles más altos en Países Bajos (82 %), Chequia, Eslovenia y Polonia (todos ellos el 75 %), y Portugal (74 %). Los países donde los encuestados están menos familiarizados con esta autoridad fueron Austria (56 %) y España (58 %).

Los particulares están cada vez más familiarizados con el RGPD y ejercen activamente sus derechos en virtud de este con mayor frecuencia ([94]). Las autoridades de protección de datos dedican recursos sustanciales a promover el conocimiento sobre los derechos y las obligaciones en materia de protección de datos entre el público en general, por ejemplo, a través de las redes sociales y campañas de televisión, líneas de ayuda, boletines informativos y presentaciones en las instituciones educativas ([95]). Muchas de estas iniciativas se han beneficiado de financiación de la UE ([96]). La Agencia de los Derechos Fundamentales señala que, si bien el público general está más familiarizado con la protección de datos, todavía no la comprende en profundidad, como demuestra el gran número de reclamaciones triviales o infundadas ([97]). Se han desarrollado varias herramientas digitales de uso sencillo para facilitar a los interesados el ejercicio de sus derechos ([98]). Los actos legislativos, en particular el Reglamento de Gobernanza de Datos ([99]), deben conducir a la creación de vías adicionales para que los interesados ejerzan sus derechos en el futuro. Las empresas señalan que el derecho de supresión se utiliza cada vez más, algo que rara vez ocurre con el derecho de rectificación y el de oposición.

4.1 El derecho de acceso

Los responsables del tratamiento informan de que el derecho de acceso (artículo 15 del RGPD) es el que más ejercitan los interesados. Si bien el Comité adoptó directrices sobre este derecho en 2022, los responsables del tratamiento siguen informando de dificultades, por ejemplo, al interpretar el concepto de «solicitudes infundadas o excesivas» ([100]), al responder a un elevado número de solicitudes y al tramitar solicitudes que se realizan con fines no relacionados con la protección de datos, como para recabar pruebas para procedimientos judiciales ([101]). Las organizaciones de la sociedad civil señalan que las respuestas a las solicitudes de acceso suelen retrasarse o estar incompletas, mientras que los datos recibidos no siempre se encuentran en un formato legible ([102]). Las autoridades

([94]) Posición y conclusiones del Consejo, apartado 13.
([95]) Contribución del Comité, apartado 6.
([96]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_es.
([97]) Informe de la FRA, pp. 9 y 48.
([98]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([99]) Artículo 10 del Reglamento (UE) 2022/868 (Reglamento de Gobernanza de Datos) (DO L 152 de 3.6.2022, p. 1).
([100]) Artículo 12, apartado 5, del RGPD.
([101]) Sin embargo, el Tribunal de Justicia ha aclarado que el interesado no está obligado a indicar los motivos por los que solicita el acceso a los datos personales: asunto C-307/22, ECLI:EU:C:2023:811, apartado 38.
([102]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

públicas mencionan dificultades en la interacción entre el derecho de acceso y las normas sobre el acceso del público a los documentos ([103]). Por lo tanto, es positivo que el Comité haya puesto en marcha, en febrero de 2024, una acción conjunta sobre el marco de ejecución coordinada relativo al derecho de acceso ([104]).

4.2 El derecho a la portabilidad

En el informe de 2020, la Comisión se comprometió a estudiar los medios prácticos para facilitar una mayor utilización del derecho a la portabilidad (artículo 20 del RGPD) por parte de los particulares, en consonancia con la estrategia de datos. Desde entonces, la Comisión ha adoptado una serie de iniciativas que complementan este derecho. Estas iniciativas facilitan un cambio sencillo entre servicios, por lo que se crean mayores posibilidades de elección para las personas, se apoya la competencia y la innovación, y se permite a las personas aprovechar las ventajas del uso de sus datos. El Reglamento de Datos otorga a los usuarios de dispositivos inteligentes un derecho mejorado a la portabilidad de los datos que se generan a través de dichos dispositivos y exige que el diseño del producto o del servidor final del fabricante o del titular de datos permita que dicha portabilidad sea posible técnicamente. El Reglamento de Mercados Digitales exige que los proveedores de servicios básicos de plataforma identificados como «guardianes de acceso» proporcionen una portabilidad efectiva de los datos de los usuarios, especialmente el acceso continuo y en tiempo real a dichos datos. Otras iniciativas de la Comisión que se encuentran actualmente en fase de negociación o sobre las que se ha alcanzado un acuerdo político prevén la mejora de los derechos de portabilidad en ámbitos específicos, como la Directiva relativa al trabajo en plataformas digitales ([105]), el Espacio Europeo de Datos Sanitarios ([106]) y el marco para el acceso a los datos financieros ([107]).

4.3 El derecho a presentar una reclamación

Como demuestra el gran número de reclamaciones, existe un amplio conocimiento del derecho a presentar una reclamación ante una autoridad de protección de datos. Las organizaciones de la sociedad civil ponen de relieve unas diferencias injustificadas en las prácticas nacionales a la hora de tramitar reclamaciones, cuestión que se aborda en la propuesta de normas procedimentales de la Comisión. Pocos Estados miembros han hecho uso de la opción prevista en el RGPD de conceder a un organismo sin ánimo de lucro el derecho a adoptar medidas con independencia del mandato del interesado (artículo 80, apartado 2). Sin embargo, la Directiva relativa a las acciones de representación ([108]), adoptada en 2020, dará lugar a una mayor armonización a este respecto al facilitar las acciones colectivas de particulares por incumplimiento del RGPD. Las medidas nacionales de transposición de la Directiva entraron en vigor en junio de 2023.

([103]) Posición y conclusiones del Consejo, apartados 27 a 28.
([104]) https://www.edpb.europa.eu/news/news/2024/cef-2024-launch-coordinated-enforcement-right-access_es.
([105]) Trabajadores de plataformas digitales: el Consejo confirma el acuerdo sobre nuevas normas para mejorar sus condiciones laborales - Consilium (europa.eu).
([106]) Propuesta de Reglamento sobre el Espacio Europeo de Datos Sanitarios [COM(2022) 197].
([107]) Propuesta de Reglamento relativo a un marco para el acceso a los datos financieros y por el que se modifican los Reglamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010, (UE) n.º 1095/2010 y (UE) 2022/2554 [COM(2023) 360 final].
([108]) Directiva (UE) 2020/1828, de 25 de noviembre de 2020, relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE (DO L 409 de 4.12.2020, p. 1).

4.4 La protección de los datos personales de los niños

Los niños precisan de una protección específica en lo que respecta a sus datos personales ([109]). El RGPD forma parte de un marco jurídico global que garantiza la protección de los niños tanto en línea como fuera de línea ([110]). Dada la creciente presencia de niños en línea, en los últimos años se han adoptado una serie de medidas a escala nacional y de la UE para velar por su protección. Las autoridades de protección de datos han impuesto multas significativas a las empresas de medios sociales por vulnerar el RGPD al tratar los datos de los niños. También cooperan con otras autoridades para instar a una mayor protección de los niños en el ámbito de la publicidad. En el informe de 2020, la Comisión invitó al Comité a adoptar directrices sobre el tratamiento de los datos de los niños, una labor que se encuentra en proceso de desarrollo ([111]). El Reglamento de Servicios Digitales incluye disposiciones específicas para garantizar un alto nivel de privacidad, seguridad y protección de los niños que utilizan plataformas en línea.

Algunas partes interesadas informan de dificultades en el ejercicio de los derechos de los interesados cuando estos son niños. En particular, argumentan de que los niños no comprenden plenamente sus derechos, carecen de competencias de alfabetización digital y pueden ser objeto de influencias indebidas ([112]). La Comisión ha financiado varias iniciativas nacionales relativas a la protección de los datos de los niños y a la promoción de la sensibilización sobre la protección de datos entre los niños ([113]). En el marco de la estrategia para una internet mejor para los niños (BIK+), la Comisión está proporcionando a los niños recursos de sensibilización y formación sobre sus derechos digitales, especialmente la protección de datos (por ejemplo, el consentimiento digital) ([114]). Se presta cada vez más atención a la necesidad de herramientas de comprobación de la edad eficaces y respetuosas con la privacidad. A principios de 2024, la Comisión creó un Grupo de Trabajo sobre Comprobación de la Edad con los Estados miembros, el Comité y el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual con el objetivo de debatir y apoyar el desarrollo de un enfoque a escala de la UE a este respecto. Este trabajo proseguirá ahora en el marco de la Junta de la Ley de Servicios Digitales, en el Grupo de Trabajo de Protección de Menores. En el contexto del Reglamento sobre la Identidad Digital Europea ([115]), que entró en vigor en mayo de 2024, la Comisión está trabajando para garantizar que la cartera europea de identidad digital se ofrezca a todos los ciudadanos y residentes de la UE en 2026, también para la verificación de la edad. Mientras tanto, antes de que el ecosistema de la cartera sea plenamente operativo, se desarrollará una solución a corto plazo para la verificación de la edad, que estará disponible en toda la UE.

5 OPORTUNIDADES Y RETOS PARA LAS ORGANIZACIONES, EN PARTICULAR LAS PYMES

El RGPD ha creado unas condiciones de competencia equitativas para las empresas que operan en el mercado interior, y su enfoque tecnológicamente neutro y favorable a la innovación les permite reducir la burocracia y beneficiarse de una mayor confianza de los

([109]) Considerando 38 del RGPD.
([110]) Recomendación sobre el desarrollo y el refuerzo de los sistemas integrados de protección de la infancia que redunden en el interés superior del niño: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/combating-violence-against-children-and-ensuring-child-protection_es.
([111]) Véanse también la posición y las conclusiones del Consejo, apartado 31, letra a).
([112]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([113]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=es&etrans=es.
([114]) https://digital-strategy.ec.europa.eu/es/policies/strategy-better-internet-kids.
([115]) Reglamento (UE) 2024/1183 por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (DO L, 2024/1183, 30.4.2024).

consumidores ([116]). Muchas empresas han desarrollado una cultura interna de protección de datos y consideran que la privacidad y la protección de datos son parámetros clave en términos de competencia. Las empresas valoran el enfoque basado en el riesgo del RGPD como principio rector que les permite abordar sus obligaciones con flexibilidad y escalabilidad ([117]).

5.1 Conjunto de instrumentos para las empresas

El RGPD proporciona un conjunto de instrumentos que permiten a las organizaciones gestionar y demostrar de manera flexible su cumplimiento, especialmente códigos de conducta, mecanismos de certificación y cláusulas contractuales tipo. Como se anunció en el informe de 2020, la Comisión adoptó en 2021 cláusulas contractuales tipo sobre la relación entre responsables y encargados del tratamiento ([118]). Estas cláusulas contractuales tipo proporcionan una herramienta de cumplimiento voluntaria prediseñada y fácil de aplicar que resulta especialmente útil para las pymes u organizaciones que pueden no disponer de los recursos necesarios para negociar contratos individuales con sus socios comerciales. Las empresas informan de comentarios dispares sobre el uso de las cláusulas contractuales tipo, en el sentido de que algunas empresas (principalmente pymes) las utilizan total o parcialmente, mientras que otras (en su mayoría empresas más grandes) tienden a no utilizarlas porque prefieren usar sus propias cláusulas.

Las empresas subrayan que los códigos de conducta tienen un gran potencial como instrumento de cumplimiento debido a su especificidad por sectores y a su rentabilidad ([119]). Sin embargo, la elaboración de códigos de conducta ha sido limitada ([120]). Según la información disponible hasta la fecha, solo se han aprobado dos códigos a escala de la UE (ambos en el sector de la nube), mientras que se han aprobado seis códigos a escala nacional ([121]). Las partes interesadas señalan que los principales factores que limitan la adopción de códigos de conducta son unos requisitos gravosos (especialmente la necesidad de crear un organismo de control acreditado), la falta de participación de las autoridades de protección de datos y el largo proceso de aprobación ([122]).

Hacen falta una mayor transparencia en el proceso y unos plazos de aprobación claros. Las autoridades de protección de datos y, en el caso de los códigos a escala de la UE, el Comité deberían fomentar más activamente la elaboración de los códigos de conducta colaborando con las asociaciones que los desarrollan. Esto ayudará a resolver las diferencias de interpretación y a acelerar el proceso de aprobación. Las partes interesadas lamentan las largas demoras en la adopción de códigos de conducta debido al hecho de que se lleven a

([116]) Como se reconoce en el informe de la plataforma «Preparados para el futuro», un grupo de expertos de alto nivel creado para ayudar a la Comisión a simplificar la legislación de la UE y reducir los costes innecesarios asociados a ella: https://commission.europa.eu/law/law-making-process/evaluating-and-improving-existing-laws/refit-making-eu-law-simpler-less-costly-and-future-proof/fit-future-platform-f4f_es. Véase también el resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD y la posición y las conclusiones del Consejo, apartado 12.

([117]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

([118]) 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 [C(2021) 3701] (DO L 199 de 7.6.2021, p. 18).

([119]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

([120]) Posición y conclusiones del Consejo, apartado 25.

([121]) https://www.edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en?f%5B0%5D=coc_scope%3Anational.

([122]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

cabo debates en paralelo en el marco de las labores de desarrollo de directrices. Las empresas también informan de que no se utiliza la certificación de manera generalizada porque el proceso de desarrollo es lento y complejo. Al igual que en el caso de los códigos de conducta, las autoridades de protección de datos deben establecer plazos más claros para la revisión y aprobación de las certificaciones.

En su Estrategia 2024-2027, el Comité se ha comprometido a seguir apoyando medidas de cumplimiento como la certificación y los códigos de conducta, en particular colaborando con grupos clave de partes interesadas para explicar cómo pueden utilizarse los instrumentos ([123]).

5.2 Desafíos específicos para las pymes y los pequeños operadores

En el informe de 2020, la Comisión pidió que se intensificaran los esfuerzos para apoyar el cumplimiento del RGPD por parte de las pymes. En los últimos años, las autoridades de protección de datos y el Comité han seguido desarrollando herramientas de cumplimiento para las pymes, respaldadas en parte por la financiación de la Comisión ([124]). En abril de 2023, el Comité puso en marcha una guía de protección de datos para pequeñas empresas ([125]), que ofrece información práctica a las pymes en un formato accesible y de fácil comprensión.

Las pymes de muchos Estados miembros subrayan los beneficios de un apoyo personalizado por parte de sus autoridades locales de protección de datos. Sin embargo, la diversidad de enfoques de concienciación y orientación por parte de las autoridades de protección de datos significa que las pymes de algunos Estados miembros perciben el cumplimiento como una cuestión compleja y temen posibles medidas o sanciones ([126]). Las autoridades de protección de datos deben redoblar sus esfuerzos para hacer frente a estos desafíos, en particular mediante la colaboración proactiva con las pymes para disipar las preocupaciones infundadas en lo que respecta al cumplimiento. Las autoridades de protección de datos deben centrarse en proporcionar apoyo personalizado y herramientas prácticas, como plantillas (por ejemplo, para realizar evaluaciones del impacto derivado de la protección de datos), líneas telefónicas de ayuda, ejemplos ilustrativos, listas de comprobación y orientaciones sobre operaciones de tratamiento específicas (por ejemplo, facturación o boletines informativos) y medidas técnicas y organizativas. Dado que la mayoría de las pymes no disponen de personal en plantilla que sea experto en protección de datos, cualquier orientación dirigida a estas empresas debe ser fácilmente comprensible para quienes carecen de formación jurídica ([127]).

En consonancia con el enfoque basado en el riesgo del RGPD, las pymes que llevan a cabo actividades de tratamiento de bajo riesgo no soportan una carga de cumplimiento sustancial. Aunque la excepción al mantenimiento de registros de las actividades de tratamiento ([128]) se aplica en circunstancias limitadas ([129]), las pymes que llevan a cabo un tratamiento de bajo riesgo pueden cumplir los requisitos manteniendo registros

([123]) https://www.edpb.europa.eu/system/files/2024-04/edpb_strategy_2024-2027_en.pdf.
([124]) https://commission.europa.eu/law/law-topic/data-protection/eu-funding-supporting-implementation-general-data-protection-regulation-gdpr_en?prefLang=es&etrans=es.
([125]) https://edpb.europa.eu/sme-data-protection-guide/home_es.
([126]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([127]) Véanse la posición y las conclusiones del Consejo, apartado 24; resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([128]) Artículo 30, apartado 5, del RGPD.
([129]) Cuando la organización emplee a menos de 250 personas, salvo que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, del RGPD o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGPD.

simplificados basados en plantillas facilitadas por las autoridades de protección de datos. Además, estos registros deben considerarse una herramienta útil para que las pymes hagan balance de sus actividades de tratamiento.

5.3 Delegados de protección de datos

Los delegados de protección de datos desempeñan un papel importante a la hora de garantizar el cumplimiento del RGPD en las organizaciones en las que trabajan. En general, los delegados de protección de datos que operan en la UE tienen los conocimientos y las capacidades necesarios para desempeñar sus funciones en virtud del RGPD y se respeta su independencia ([130]). Sin embargo, siguen existiendo varios desafíos, entre ellos: i) dificultades a la hora de nombrar delegados de protección de datos que dispongan de los conocimientos especializados necesarios; ii) falta de normas a escala de la UE en materia de educación y formación; iii) falta de integración adecuada de los delegados de protección de datos en los procesos organizativos; iv) falta de recursos; v) tareas adicionales además de la protección de datos, y vi) antigüedad insuficiente ([131]). El Comité señaló que es necesario que las autoridades de protección de datos intensifiquen las actividades de sensibilización, así como sus medidas de información y ejecución, para garantizar que los delegados de protección de datos puedan desempeñar su función en virtud del RGPD ([132]).

6 EL RGPD COMO PIEDRA ANGULAR DE LA POLÍTICA DE LA UE EN EL ÁMBITO DIGITAL

6.1 Política digital basada en el RGPD

En el informe de 2020, la Comisión se comprometió a apoyar la aplicación coherente del marco de protección de datos en relación con las nuevas tecnologías con el fin de apoyar la innovación y los avances tecnológicos. Desde entonces, la UE ha adoptado una serie de iniciativas, algunas de las cuales complementan el RGPD o especifican cómo debe aplicarse en ámbitos específicos, con el fin de perseguir objetivos concretos, como se expone a continuación.

- El Reglamento de Servicios Digitales ([133]), cuyo objetivo es proporcionar un entorno en línea seguro para las personas y las empresas, prohíbe a las plataformas en línea mostrar anuncios basados en la elaboración de perfiles utilizando «categorías especiales de datos personales», tal como se definen en el RGPD.
- Para que los mercados digitales sean más equitativos y disputables, el Reglamento de Mercados Digitales ([134]) prohíbe a los operadores designados como «guardianes de acceso» «combinar» y «cruzar» datos personales procedentes de sus servicios básicos de plataforma con datos personales procedentes de otros servicios, a menos que el usuario haya dado su consentimiento conforme a lo previsto en el RGPD.
- La Ley de Inteligencia Artificial ([135]) especifica las normas de protección de datos de la UE en ámbitos específicos en los que se utiliza la inteligencia artificial, por ejemplo,

([130]) Posición y conclusiones del Consejo, apartado 26; *EDPB 2023 Coordinated Enforcement Action Designation and Position of Data Protection Officers* [«Acción de Ejecución Coordinada del CEPD de 2023; Designación y funciones de los delegados de la protección de datos», documento en inglés]: https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf.
([131]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([132]) Véanse las recomendaciones de la Acción de Ejecución Coordinada del CEPD.
([133]) Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) (DO L 277 de 27.10.2022, p. 1).
([134]) Reglamento (UE) 2022/1925 (Reglamento de Mercados Digitales) (DO L 265 de 12.10.2022, p. 1).
([135]) Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024).

en sistemas de identificación biométrica remota, en el tratamiento de categorías especiales de datos para detectar sesgos y en el tratamiento ulterior de datos personales en espacios controlados de pruebas.

- La Directiva relativa al trabajo en plataformas ([136]) complementa el RGPD en el ámbito del empleo mediante el establecimiento de normas sobre los sistemas automatizados de supervisión y toma de decisiones utilizados por las plataformas digitales de trabajo, y en particular determinadas limitaciones al tratamiento de datos personales, la transparencia y la supervisión y revisión humanas, y la portabilidad.
- El Reglamento sobre la publicidad política ([137]) prohíbe el uso de categorías especiales de datos personales en la publicidad política y exige una mayor transparencia sobre las técnicas de segmentación y amplificación utilizadas.
- El Reglamento sobre la Identidad Digital Europea permite la creación de una cartera europea de identidad digital universal, fiable y segura. Dicha cartera permitirá a las personas demostrar atributos personales como la edad, los permisos de conducción, los títulos y las cuentas bancarias con pleno control sobre sus datos personales y sin compartir información innecesaria.

La propuesta de Reglamento sobre la privacidad en las comunicaciones electrónicas ([138]) que sustituirá a la actual Directiva sobre la privacidad y las comunicaciones electrónicas ([139]) y complementará el marco legislativo en materia de privacidad y protección de datos se encuentra en fase de negociación desde hace varios años. Es necesario reflexionar sobre los próximos pasos de esta iniciativa, incluida su relación con el RGPD.

La Ley sobre la Europa Interoperable ([140]) tiene por objeto hacer que los servicios públicos digitales sean interoperables en toda la UE y apoya la cooperación entre las autoridades de protección de datos, en particular a través de los espacios controlados de pruebas de interoperabilidad.

Varias iniciativas de la UE proporcionan una base jurídica para el tratamiento de datos personales por parte de entidades privadas para la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales. Toda legislación de este tipo debe estar cuidadosamente orientada a minimizar la injerencia en el derecho a la protección de los datos personales y debe ser proporcionada al objetivo perseguido ([141]). La Carta, el RGPD y la jurisprudencia del Tribunal de Justicia proporcionan un marco para medir estas iniciativas. El paquete de medidas contra el blanqueo de capitales propuesto ([142]) contiene salvaguardias sustanciales para la protección de los datos personales, sin comprometer el objetivo de mitigar los riesgos de blanqueo de capitales y financiación del terrorismo y de detectar eficazmente las tentativas delictivas de utilizar indebidamente el sistema financiero de la UE.

([136]) Trabajadores de plataformas digitales: el Consejo confirma el acuerdo sobre nuevas normas para mejorar sus condiciones laborales - Consilium (europa.eu).

([137]) Reglamento (UE) 2024/900 sobre la transparencia y la segmentación de la publicidad política (DO L, 2024/900, 20.3.2024).

([138]) Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas [COM(2017) 10 final].

([139]) Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

([140]) Reglamento (UE) 2024/903 (Ley sobre la Europa Interoperable) (DO L, 2024/903, 22.3.2024).

([141]) Véanse la posición y las conclusiones del Consejo, apartado 31, letra f).

([142]) https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en?prefLang=es&etrans=es.

En este contexto, el Consejo ha subrayado que cualquier nueva legislación de la UE que contenga disposiciones sobre el tratamiento de datos personales debe ser coherente con el RGPD y la jurisprudencia del Tribunal de Justicia.

6.2 Un marco jurídico para mejorar el intercambio de datos

La estrategia de datos tiene por objeto crear un mercado único de datos en el que los datos fluyan libremente dentro de la UE y entre sectores en beneficio de las empresas, los investigadores y las administraciones públicas. Un objetivo clave de la estrategia de datos es la creación de espacios comunes europeos de datos que faciliten su puesta en común, su acceso y su intercambio. En lo que respecta a los datos personales, el RGPD proporciona el marco para todas las iniciativas destinadas a mejorar la libre circulación de datos en la UE, que es a su vez un objetivo del RGPD. En cuanto a los datos personales, no se abordan las protecciones del RGPD.

El Reglamento de Gobernanza de Datos ([143]) y el Reglamento Datos ([144]) son pilares de la estrategia de datos. El Reglamento de Gobernanza de Datos establece normas concretas en el contexto de la reutilización de los datos del sector público que contengan datos personales y establece un marco legislativo para los servicios de intermediación de datos, incluidos los servicios de gestión de información personal (PIMS) o las nubes de datos personales ofrecidos con el fin de facultar a los interesados en el ejercicio de sus derechos en virtud del RGPD. También establece las condiciones de uso de los datos con fines altruistas. Por su parte, el Reglamento de Datos refuerza el control de los interesados sobre los datos que generan mediante el uso de productos inteligentes que poseen, alquilan o arriendan al imponer requisitos técnicos para el acceso a los datos y su portabilidad.

El Espacio Europeo de Datos Sanitarios (EEDS) ([145]) refleja las necesidades específicas identificadas en el sector de los datos sanitarios, al tiempo que se basa en el RGPD. Permite a las personas acceder fácilmente a sus datos sanitarios en formato electrónico y compartirlos con los profesionales sanitarios, también en otros Estados miembros, con la consiguiente mejora de la prestación de asistencia sanitaria y el aumento del control de los pacientes sobre sus datos. También establece un marco jurídico común para la reutilización de datos sanitarios con fines como la investigación, la innovación y la salud pública sujeta a la expedición de un permiso por parte de un organismo de acceso a los datos sanitarios. Para garantizar la protección de los datos personales, el EEDS proporcionará un marco fiable para el acceso seguro a los datos sanitarios y su tratamiento. La Comisión sigue apoyando los avances en el desarrollo de espacios comunes europeos de datos en catorce sectores mediante la aplicación del nuevo marco legislativo y la financiación de iniciativas sectoriales específicas.

6.3 Gobernanza de las nuevas normas digitales

El desarrollo de la normativa digital plantea la necesidad de una estrecha cooperación en todos los ámbitos normativos ([146]). Esta cooperación resulta, si cabe, más necesaria debido a que las cuestiones de protección de datos están cada vez más relacionadas con asuntos como, por ejemplo, el Derecho de la competencia, el Derecho de los consumidores, la normativa de los mercados digitales, la regulación de las comunicaciones electrónicas y la ciberseguridad. Este es el caso, por ejemplo, al evaluar la compatibilidad de los modelos

([143]) Reglamento (UE) 2022/868 (Reglamento de Gobernanza de Datos) (DO L 152 de 3.6.2022, p. 1).
([144]) Reglamento (UE) 2023/2854 (Reglamento de Datos) (DO L, 2023/2854, 22.12.2023).
([145]) https://www.europarl.europa.eu/doceo/document/TA-9-2024-0331_ES.html.

([146]) Véanse la posición y las conclusiones del Consejo, apartados 40 a 41, y el resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

«consentimiento o remuneración» (también llamados popularmente «pay or okay») con el Derecho de la Unión.

En algunos casos, las autoridades de protección de datos se encargan de hacer cumplir disposiciones específicas de la nueva legislación de la UE en el ámbito digital ([147]). Las nuevas normas digitales también crean estructuras específicas que reúnen a los reguladores competentes para garantizar una aplicación coherente, como el Grupo de Alto Nivel sobre el Reglamento de Mercados Digitales, el Comité Europeo de Innovación en materia de Datos (creado en virtud del Reglamento de Gobernanza de Datos) y la Junta Europea de Servicios Digitales (creada en virtud del Reglamento de Servicios Digitales). La Directiva SRI 2 ([148]) establece normas más detalladas sobre la cooperación entre las autoridades reguladoras y las autoridades de protección de datos en la gestión de incidentes de seguridad que constituyan violaciones de la seguridad de los datos personales.

Al margen de estas estructuras formales, las autoridades de protección de datos están tomando medidas para garantizar que sus acciones sean complementarias y coherentes con otros ámbitos reglamentarios. En julio de 2020, las autoridades de protección de los consumidores y de los datos crearon un «grupo de voluntarios» para determinar buenas prácticas y compartir experiencias de aplicación normativa. Las autoridades de protección de datos siguen participando en talleres conjuntos con la Red de Cooperación para la Protección de los Consumidores. En 2023, el Comité creó un grupo de trabajo sobre la interacción entre la protección de datos, la competencia y la protección de los consumidores.

Si bien estos avances son positivos, es necesario contar con medios de cooperación más estructurados y eficientes, en particular para abordar situaciones que afectan a un gran número de particulares en la UE y en las que participan varios reguladores ([149]). Estas estructuras deben garantizar que las autoridades sigan siendo responsables en todo momento de todas las cuestiones relativas al cumplimiento de las normas en sus ámbitos de competencia. Los Estados miembros también deben trabajar para garantizar que se lleve a cabo una cooperación adecuada a nivel nacional ([150]).

7 TRANSFERENCIAS INTERNACIONALES Y COOPERACIÓN MUNDIAL

7.1 El conjunto de instrumentos de transferencia del RGPD

Los flujos de datos se han convertido en una parte integrante de la transformación digital de la sociedad y de la globalización de la economía. Más que nunca, el respeto de la privacidad es indispensable para asegurar unos flujos comerciales estables, seguros y competitivos, así como para facilitar muchas formas de cooperación internacional. El conjunto de instrumentos de transferencia del RGPD que establece su capítulo V ofrece una variedad de instrumentos para abordar diferentes hipótesis de transferencia, al tiempo que garantiza que los datos sigan beneficiándose de un elevado nivel de protección cuando abandonan la UE.

Desde el informe de 2020, se han aclarado aún más los requisitos para las transferencias de datos establecidos en la legislación de la UE en materia de protección de datos, y el

([147]) Véase, por ejemplo, el artículo 37, apartado 3, del Reglamento de Datos.
([148]) Directiva (UE) 2022/2555 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80).
([149]) Véanse la posición y las conclusiones del Consejo, apartados 18 y 40 a 41, y el resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([150]) Alemania ha creado un «clúster digital» que incluye a reguladores de diversos ámbitos con el objetivo de ampliar su cooperación en todos los aspectos de la digitalización y compartir conocimientos y buenas prácticas: https://www.dataguidance.com/news/germany-bsi-announces-formation-digital-cluster-bonn.

conjunto de instrumentos de transferencia ha seguido evolucionando. Una aclaración importante hace referencia al concepto de «transferencia internacional», que, de acuerdo con la definición del Comité ([151]), abarca toda comunicación de datos personales por parte de un responsable o encargado del tratamiento sujeto al RGPD a otro responsable o encargado del tratamiento en un tercer país, independientemente de que el tratamiento por parte de este último esté o no sujeto al RGPD ([152]). Estas orientaciones del Comité fueron especialmente importantes para proporcionar seguridad jurídica a los responsables y encargados del tratamiento europeos sobre las situaciones en las que se necesita una herramienta de transferencia con arreglo al capítulo V del RGPD.

El Tribunal de Justicia también ha aportado más aclaraciones en su sentencia Schrems II ([153]) sobre la protección que deben proporcionar diferentes instrumentos de transferencia para garantizar que no se menoscabe el nivel de protección garantizado por el RGPD ([154]). En particular, estos instrumentos deben garantizar que las personas cuyos datos se transfieren fuera de la UE gocen de un nivel de protección sustancialmente equivalente al garantizado dentro de la UE ([155]). Es responsabilidad del exportador de datos de la UE evaluar si este es el caso, teniendo en cuenta las circunstancias específicas de sus transferencias ([156]).

Para evaluar el nivel de protección, los exportadores de datos deben tener en cuenta tanto las garantías de protección de datos establecidas en el instrumento de transferencia celebrado con un importador de datos no perteneciente a la UE (por ejemplo, un contrato) como los elementos pertinentes del sistema jurídico del país en el que esté situado el importador de datos, en particular en lo que respecta al posible acceso a los datos por parte de las autoridades públicas de ese país ([157]). Este último debe evaluarse a la luz de los criterios de evaluación de la adecuación establecidos en el artículo 45 del RGPD. El Tribunal también profundizó en estos criterios, en particular en lo que se refiere a las normas sobre el acceso a los datos personales por parte de las autoridades públicas con fines de aplicación de la ley y de seguridad nacional.

Esta interpretación también se ha reflejado en las orientaciones del Comité, que actualizó sus «referencias sobre adecuación» ([158]) (que proporcionaron orientaciones sobre los elementos que la Comisión debe tener en cuenta al llevar a cabo una evaluación de la adecuación). El Comité también adoptó nuevas orientaciones que ofrecen aclaraciones adicionales sobre las siguientes cuestiones: i) los elementos que deben tener en cuenta los exportadores de datos individuales a la hora de evaluar el nivel de protección; ii) una visión general de las posibles fuentes que pueden utilizarse, y iii) ejemplos de posibles medidas complementarias (por ejemplo, garantías contractuales y técnicas) ([159]). Las orientaciones destacan específicamente que cada evaluación realizada por los exportadores de datos es única y que, por lo tanto, deben tener en cuenta las características específicas de cada transferencia, que pueden diferir en función de la finalidad de la transferencia de datos, los tipos de entidades implicadas, el sector en el que se realiza la transferencia, las categorías de datos personales transferidos, etc. ([160]).

([151]) Directrices n.º 05/2021 del CEPD.
([152]) Sección 2 de las Directrices n.º 05/2021 del CEPD.
([153]) Asunto C-311/18, ECLI:EU:C:2020:559 (Schrems II).
([154]) Schrems II, apartado 93.
([155]) Schrems II, apartados 96 y 105.
([156]) Schrems II, apartado 131.
([157]) Schrems II, apartado 105.
([158]) Recomendaciones n.º 02/2020 del CEPD y referencias de adecuación (WP 254 rev. 01).
([159]) Recomendaciones n.º 01/2020 del CEPD, complementadas por las Recomendaciones n.º 02/2020.
([160]) Véanse, por ejemplo, los apartados 8 a 13 y 32 a 33 de las Recomendaciones n.º 01/2020.

Teniendo en cuenta estas diferentes aclaraciones sobre los requisitos para las transferencias internacionales de datos, en los últimos años se han dado pasos significativos para seguir desarrollando y poniendo en práctica el conjunto de instrumentos de transferencia del RGPD.

7.1.1 Decisiones de adecuación

Como también se refleja en las observaciones recibidas de las partes interesadas, las decisiones de adecuación siguen desempeñando un papel clave en el conjunto de instrumentos de transferencia del RGPD ([161]), ya que ofrecen una solución sencilla y exhaustiva para las transferencias de datos sin necesidad de que el exportador proporcione más garantías u obtenga ninguna autorización. Al permitir la libre circulación de datos personales, estas decisiones han abierto canales comerciales para los operadores de la UE, en particular al complementar y amplificar los beneficios de los acuerdos comerciales, y han facilitado la cooperación con socios extranjeros en una amplia gama de ámbitos, desde la cooperación en materia de regulación hasta la investigación.

Desde el informe de 2020, ha seguido creciendo el número de países que han puesto en marcha leyes modernas en materia de protección de datos en las que prevén, entre otras cosas, principios clave en materia de protección de datos, derechos individuales y una aplicación efectiva por parte de reguladores independientes. Esta tendencia ([162]) también ha permitido a la Comisión intensificar su labor en materia de adecuación. Esto incluye la adopción de una decisión de adecuación para el Reino Unido ([163]), que es fundamental para garantizar el correcto funcionamiento de los diversos acuerdos celebrados con el Reino Unido tras el Brexit. Para garantizar que la decisión de adecuación tenga garantías de futuro, incluye una «cláusula de extinción» que vencerá en 2025, tras lo cual podrá renovarse si el nivel de protección sigue siendo adecuado. La Comisión también adoptó una decisión de adecuación para la República de Corea ([164]), que complementa el Acuerdo de Libre Comercio UE-Corea sobre los flujos de datos personales y facilita la cooperación en materia de regulación. Está prevista una primera revisión de la decisión de adecuación para finales de 2024.

Además, tras la anulación de la decisión de adecuación del Escudo de la privacidad UE-EE. UU., la Comisión entabló conversaciones con el Gobierno estadounidense para desarrollar un nuevo acuerdo de conformidad con los requisitos aclarados por el Tribunal ([165]). El presidente de los Estados Unidos adoptó un nuevo Decreto sobre el refuerzo de las salvaguardias para las actividades de inteligencia de señales de los Estados Unidos, por el que se introdujeron nuevas salvaguardias vinculantes y ejecutables para garantizar que solo se pueda acceder a los datos con fines de seguridad nacional en la medida en que resulte necesario y proporcionado, y que la ciudadanía europea disponga de vías de recurso efectivas. Sobre esta base, la Comisión adoptó su decisión de adecuación sobre el Marco de Privacidad de Datos UE-EE. UU. ([166]), que permite que los datos personales circulen libremente desde la UE a las empresas estadounidenses que se adhieran al Marco de Privacidad de Datos. Dado que las salvaguardias establecidas por el Gobierno de los Estados Unidos en el ámbito de la seguridad nacional se aplican a todas las

([161]) Véanse, por ejemplo, la contribución del Comité, páginas 7 y 8; la posición y conclusiones del Consejo apartado 36, y el resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

([162]) Comunicación de la Comisión titulada «Intercambio y protección de los datos personales en un mundo globalizado» de 10.1.2017 [COM(2017) 7 final].

([163]) Decisión de Ejecución (UE) 2021/1772 de la Comisión (DO L 360 de 11.10.2021, p. 1).

([164]) Decisión de Ejecución (UE) 2022/254 de la Comisión (DO L 44 de 24.2.2022, p. 1).

([165]) https://commission.europa.eu/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-2020-08-10_es.

([166]) Decisión de Ejecución (UE) 2023/1795 de la Comisión (DO L 231 de 20.9.2023, p. 118).

transferencias de datos a empresas de los Estados Unidos, independientemente del mecanismo de transferencia del RGPD utilizado, se ha facilitado significativamente el uso de otras herramientas, como las cláusulas contractuales tipo y las normas corporativas vinculantes. Durante el verano de 2024 se llevará a cabo una primera revisión del funcionamiento del Marco de Privacidad de Datos con el objeto de verificar si todos los elementos pertinentes se han implantado plenamente y funcionan eficazmente en la práctica.

Actualmente se están llevando a cabo negociaciones sobre adecuación con Brasil y Kenia, así como, por primera vez, con varias organizaciones internacionales (las conversaciones sobre adecuación se encuentran, por ejemplo, en una fase avanzada con la Organización Europea de Patentes) ([167]). En consonancia también con las peticiones de diversas partes interesadas ([168]), la Comisión ha participado activamente en conversaciones exploratorias con países de diferentes regiones del mundo.

La Comisión también supervisa continuamente la evolución en los países que ya se benefician de las constataciones de adecuación y revisa periódicamente las decisiones existentes, de conformidad con sus correspondientes obligaciones en virtud del RGPD ([169]). En abril de 2023, la Comisión adoptó su informe sobre la primera revisión periódica de la decisión de adecuación relativa a Japón ([170]), en el que se llegaba a la conclusión de que Japón sigue garantizando un nivel de protección adecuado ([171]). La revisión demostró que los marcos de protección de datos de la UE y Japón han seguido convergiendo desde la adopción de las decisiones de adecuación mutua.

Además, de conformidad con el artículo 97 del RGPD, la primera revisión de las once decisiones de adecuación ([172]) adoptadas en virtud del anterior marco de protección de datos de la UE (la Directiva sobre protección de datos) se inició como parte de la evaluación de 2020 de la aplicación y el funcionamiento del RGPD. La conclusión de este aspecto de la revisión se aplazó, en particular para tener en cuenta la sentencia del Tribunal de Justicia en el asunto Schrems II y su posterior interpretación por parte del Comité. Las mencionadas aclaraciones del Tribunal sobre los elementos clave de la norma de adecuación dieron lugar a intercambios detallados con los países y territorios afectados sobre aspectos pertinentes de su marco jurídico, así como sobre mecanismos de supervisión y ejecución.

El 15 de enero de 2024, la Comisión publicó su informe sobre estas once decisiones, junto con informes detallados por país en los que se describe la evolución en cada uno de los países y territorios desde la adopción de las decisiones de adecuación, así como las normas aplicables al acceso a los datos por parte de las autoridades públicas, en particular con fines

([167]) La Organización Europea de Patentes es una organización intergubernamental creada sobre la base del Convenio sobre la Patente Europea y su misión principal es la concesión de patentes europeas. En este contexto, coopera estrechamente con empresas y autoridades públicas de los Estados miembros de la UE, así como con diferentes instituciones y organismos de la UE.

([168]) Contribución del Comité, pp. 7 y 8.

([169]) Artículo 45, apartados 4 y 5, del RGPD. Véase también Schrems I, apartado 76.

([170]) Decisión de Ejecución (UE) 2019/419 de la Comisión (DO L 76 de 19.3.2019, p. 1). Véase también https://ec.europa.eu/commission/presscorner/detail/es/IP_19_421. Esta decisión constituyó la primera decisión de adecuación adoptada en virtud del RGPD y el primer acuerdo de adecuación recíproca.

([171]) Informe de la Comisión sobre la primera revisión del funcionamiento de la decisión de adecuación relativa a Japón, de 3.4.2023 [COM(2023) 275 final y SWD(2023) 75 final].

([172]) Andorra, Argentina, Canadá (para los operadores comerciales), Guernesey, las Islas Feroe, la Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay.

de aplicación de la ley y de seguridad nacional ([173]). El informe concluye que los once países y territorios siguen ofreciendo un nivel adecuado de protección de los datos personales transferidos desde la UE, lo cual refleja que todos los países y territorios correspondientes han modernizado y reforzado de diferentes maneras su marco jurídico en materia de privacidad. Además, con el fin de abordar las diferencias existentes en lo relativo al nivel de protección, se han negociado y acordado garantías adicionales para los datos personales transferidos desde Europa con algunos de ellos, en aquellos casos en los que ha sido necesario para garantizar la continuidad de la decisión de adecuación.

Estas revisiones también muestran que las decisiones de adecuación, en lugar de constituir un fin en sí mismas, han sentado las bases para una cooperación más estrecha y una mayor convergencia normativa entre la UE y estos socios afines. Por ejemplo, el informe sobre la primera revisión del funcionamiento de la decisión de adecuación relativa a Japón reconoce que el refuerzo adicional del marco de protección de datos de Japón puede allanar el camino para ampliar la decisión de adecuación más allá de los intercambios comerciales, a fin de cubrir transferencias actualmente no incluidas en su ámbito de aplicación, como por ejemplo en la esfera de la cooperación reglamentaria y la investigación. Las conversaciones para estudiar esta posible ampliación están en curso. En general, las decisiones de adecuación se han convertido en un componente estratégico de la relación general de la UE con estos socios extranjeros y se reconocen como un factor clave para profundizar la cooperación en un amplio abanico de ámbitos.

Además de proporcionar una base sólida para una mayor cooperación bilateral, la creciente red de países y territorios para los que la UE ha adoptado una decisión de adecuación ofrece nuevas oportunidades para maximizar los beneficios de unos flujos de datos seguros y libres y para cooperar más estrechamente entre socios afines en la aplicación de las normas de protección de datos. Por consiguiente, en marzo de 2024, la Comisión organizó la primera reunión de alto nivel sobre flujos de datos seguros, en la que se reunieron ministros competentes en la materia y directores de las autoridades de protección de datos de quince países y territorios para los que la UE ha adoptado una decisión de adecuación, así como el presidente del Comité Europeo de Protección de Datos ([174]). En la reunión se definieron varios puntos de actuación concretos sobre los que se está llevando a cabo un trabajo de seguimiento en el seno de este grupo.

En líneas más generales, gracias a su «efecto de red», las decisiones de adecuación adoptadas por la Comisión Europea son cada vez más importantes también fuera de la UE, ya que no solo permiten la libre circulación de datos con las treinta economías del EEE, sino también con muchas más jurisdicciones de todo el mundo que reconocen a los países para los que existe una decisión de adecuación de la UE como «destinos seguros» con arreglo a sus propias normas de protección de datos ([175]).

7.1.2 Instrumentos que ofrecen garantías adecuadas

Desde el informe de 2020, se han desarrollado instrumentos adicionales que prevén garantías adecuadas y se han publicado orientaciones prácticas para facilitar su uso.

Como se anunció en el informe de 2020, la Comisión ha adoptado cláusulas contractuales tipo modernizadas ([176]), las cuales se desarrollaron basándose en gran medida en las

([173]) Informe de la Comisión sobre la primera revisión del funcionamiento de las decisiones de adecuación adoptadas en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE, de 15.1.2024 [COM(2024) 7 final] [y SWD(2024) 3 final].

([174]) https://ec.europa.eu/commission/presscorner/detail/es/mex_24_1307#11.

([175]) Por ejemplo, Argentina, Colombia, Israel, Marruecos, Suiza y Uruguay.

([176]) Decisión de Ejecución (UE) 2021/914 de la Comisión (DO L 199 de 7.6.2021, p. 31).

observaciones de diversas partes interesadas ([177]). Las nuevas cláusulas contractuales tipo han sustituido a los tres conjuntos de cláusulas adoptados en virtud de la Directiva sobre protección de datos. Las principales novedades son las siguientes: i) garantías actualizadas en consonancia con el RGPD; ii) un enfoque modular que ofrezca un único punto de entrada en el que se englobe una amplia gama de hipótesis de transferencia; iii) una mayor flexibilidad para el uso de cláusulas contractuales tipo por diversas partes, y iv) un conjunto de instrumentos prácticos para dar cumplimiento a la sentencia Schrems II.

Las partes interesadas han acogido favorablemente las cláusulas contractuales tipo modernizadas, y las observaciones recibidas confirman que siguen siendo, con diferencia, el instrumento más utilizado para las transferencias por parte de los exportadores de datos de la UE ([178]). Para ayudar a los exportadores de datos en sus esfuerzos de cumplimiento, la Comisión ha elaborado una serie de preguntas y respuestas que proporcionan orientaciones adicionales sobre el uso de las cláusulas ([179]), las cuales se actualizarán en caso de que surjan nuevas dudas, también a la luz de las observaciones adicionales recibidas en el marco de esta evaluación.

Muchos exportadores de datos afirman tener dificultades para llevar a cabo las «evaluaciones de impacto de las transferencias» que exige la sentencia Schrems II, refiriéndose, en particular, a su complejidad, así como a los costes y el tiempo necesarios para llevarlas a cabo ([180]). Si bien acogen con satisfacción las orientaciones del Comité y las cláusulas contractuales tipo, también solicitan orientaciones adicionales (por ejemplo, sobre las responsabilidades de las partes implicadas y el nivel de detalle requerido en las evaluaciones de impacto de las transferencias) y herramientas adicionales para ayudar en la realización de dichas evaluaciones (por ejemplo, plantillas, evaluaciones generales por país, catálogos de riesgos). Aunque las partes interesadas proporcionaron estas observaciones sobre todo en lo que respecta a las cláusulas contractuales tipo, también se piden las mismas evaluaciones para otros instrumentos de transferencia (como las normas corporativas vinculantes). Por lo tanto, es importante que el Comité estudie formas y herramientas para seguir ayudando a los exportadores de datos en sus esfuerzos de cumplimiento en este contexto, sobre la base de la experiencia adquirida al aplicar los requisitos previstos en la sentencia Schrems II en los últimos años, también como parte de las actividades de ejecución de las autoridades nacionales de protección de datos.

Para complementar las cláusulas contractuales tipo existentes, la Comisión está desarrollando conjuntos adicionales de cláusulas para proporcionar a los exportadores de datos de la UE un paquete completo y coherente. Esto incluirá las cláusulas contractuales tipo en virtud del Reglamento (UE) 2018/1725 para las transferencias de datos por parte de las instituciones y organismos de la UE a operadores comerciales de terceros países ([181]) y las cláusulas contractuales tipo para las transferencias de datos a importadores de datos de terceros países cuyas operaciones de tratamiento estén directamente sujetas al RGPD. Estas últimas responden a la petición de las partes interesadas de cubrir específicamente los escenarios en los que el importador de datos entra en el ámbito de aplicación territorial del RGPD (por ejemplo, porque el tratamiento en cuestión se dirige al mercado de la UE

([177]) Esto incluía, por ejemplo, el Dictamen conjunto 2/2021 del CEPD-SEPD como parte del procedimiento de adopción de las cláusulas contractuales tipo.

([178]) Posición y conclusiones del Consejo, apartado 37; contribución del Comité, página 9; resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

([179]) https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_es.

([180]) Véase, por ejemplo, el resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.

([181]) De conformidad con el artículo 48, apartado 2, letra b), del Reglamento (UE) 2018/1725.

de conformidad con el artículo 3, apartado 2, del RGPD) ([182]). Como aclara el Comité, en este caso también es necesaria un instrumento de transferencia en virtud del capítulo V del RGPD debido al aumento de los riesgos para los datos personales tratados fuera de la UE, por ejemplo, debido a legislaciones nacionales posiblemente contradictorias o a un acceso desproporcionado por parte del Gobierno en el tercer país ([183]). Las nuevas cláusulas contractuales tipo que está desarrollando la Comisión abordarán específicamente este escenario y tendrán plenamente en cuenta los requisitos que ya se aplican directamente a dichos responsables y encargados del tratamiento en virtud del RGPD ([184]).

Como también reconocen los diferentes tipos de partes interesadas ([185]), las cláusulas tipo desempeñan un papel cada vez más importante a la hora de facilitar los flujos de datos en todo el mundo. Varias jurisdicciones han aprobado las cláusulas contractuales tipo de la UE como mecanismo de transferencia de su propia legislación en materia de protección de datos, con adaptaciones formales que se limitan a su ordenamiento jurídico nacional ([186]). Otros países han adoptado sus propias cláusulas tipo, las cuales comparten importantes características comunes con las de la UE ([187]). Un ejemplo especialmente pertinente es la creación de cláusulas tipo por parte de otras organizaciones o redes internacionales o regionales, como el Comité Consultivo del Consejo de Europa del Convenio 108, la Red Iberoamericana de Protección de Datos y la Asociación de Naciones de Asia Sudoriental (ASEAN) ([188]). Esto brinda nuevas oportunidades para facilitar los flujos de datos entre las distintas regiones del mundo sobre la base de cláusulas tipo. Un ejemplo concreto es la Guía UE-ASEAN sobre las cláusulas contractuales tipo de la UE y las cláusulas tipo de la ASEAN, que, a partir de las aportaciones de las empresas, contribuye a los esfuerzos de cumplimiento en el marco de ambos conjuntos de cláusulas ([189]).

Además de las cláusulas contractuales tipo, las normas corporativas vinculantes siguen utilizándose ampliamente para los flujos de datos entre miembros de grupos empresariales o entre empresas que realizan una actividad económica conjunta. Dado que se aplica el RGPD, el Comité adoptó ochenta dictámenes favorables sobre decisiones nacionales por las que se aprueban normas corporativas vinculantes ([190]). El Comité también publicó orientaciones sobre los elementos que deben incluirse en las normas corporativas vinculantes para los responsables del tratamiento (y la información que debe facilitarse como parte de su aplicación), las cuales se han actualizado para reflejar los requisitos del RGPD y la sentencia Schrems II ([191]). También se están elaborando orientaciones

([182]) Posición y conclusiones del Consejo, apartado 37; contribución del Comité, página 9; resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([183]) Directrices n.º 05/2021 del CEPD, p. 3.
([184]) Como también se establece en las Directrices n.º 05/2021 del CEPD, sección 4.
([185]) Contribución del Comité, página 9, y resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([186]) Por ejemplo, el Reino Unido (https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf) y Suiza (https://www.edoeb.admin.ch/edoeb/en/home/datenschutz/arbeit_wirtschaft/datenuebermittlung_ausland.html).
([187]) Por ejemplo, Nueva Zelanda (https://privacy.org.nz/responsibilities/your-obligations/disclosing-personal-information-outside-new-zealand/) y Argentina (https://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm).
([188]) Véanse https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4; https://www.redipd.org/sites/default/files/2023-02/anexo-modelos-clausulas-contractuales-en.pdf y https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf.
([189]) https://commission.europa.eu/document/download/df5cd5a0-7387-4a2a-8058-8d2ccfec3062_es?filename=%28Final%29%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf.
([190]) Contribución del Comité, p. 9.
([191]) Recomendaciones n.º 01/2022 del CEPD.

actualizadas sobre las normas corporativas vinculantes para los encargados del tratamiento ([192]). Dado que las normas corporativas vinculantes tienen por objeto establecer políticas o programas vinculantes en materia de protección de datos en las empresas, muchas partes interesadas las consideran un instrumento de cumplimiento especialmente útil y un instrumento de transferencia fiable ([193]). Al mismo tiempo, las partes interesadas siguen informando de que la duración y la complejidad del proceso de aprobación por parte de las autoridades nacionales de protección de datos obstaculizan una adopción más amplia de las normas corporativas vinculantes. Por lo tanto, es importante que las autoridades sigan trabajando para optimizar y acortar el proceso de aprobación.

Desde el informe de 2020, también se han tomado medidas para facilitar el uso de la certificación y de los códigos de conducta como herramientas para las transferencias, por ejemplo, mediante la adopción de directrices específicas sobre ambas herramientas por parte del Comité ([194]). No obstante, las partes interesadas informan sobre dificultades relacionadas con la complejidad y duración prolongada, similares a las mencionadas anteriormente con respecto a la certificación y los códigos de conducta como herramientas de responsabilidad proactiva.

Por último, el RGPD también prevé instrumentos específicos (acuerdos internacionales y acuerdos administrativos aprobados por las autoridades de protección de datos) que deben utilizar las autoridades públicas para transferir datos personales a sus homólogas en terceros países o a las organizaciones internacionales. El Comité adoptó directrices sobre las garantías que deben incluirse en dichos instrumentos ([195]), las cuales pueden contribuir a la negociación de dichos acuerdos y arreglos.

7.1.3 Garantizar la complementariedad con otras políticas

Dado que los flujos de datos se han vuelto esenciales para tantas actividades, es fundamental garantizar que las políticas de protección de datos y otras políticas se complementen entre sí. La inclusión de garantías de protección de datos en los instrumentos internacionales no solo es a menudo una condición previa para los flujos de datos, sino también un importante catalizador para una cooperación estable y fiable.

Por ejemplo, los acuerdos internacionales que establecen las garantías necesarias en materia de protección de datos, en particular al garantizar la continuidad de la protección por parte de una autoridad requirente, son esenciales para garantizar la cortesía y facilitar el acceso transfronterizo de las autoridades policiales a las pruebas electrónicas que obran en poder de las empresas y, de este modo, velar por una lucha más eficaz contra la delincuencia. Este enfoque se refleja en el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia ([196]), que mejora las normas existentes para obtener acceso transfronterizo a pruebas electrónicas en las investigaciones penales al tiempo que se ofrecen unas garantías adecuadas en materia de protección de datos. Varios Estados miembros de la UE han firmado ya el Protocolo. Del mismo modo, están avanzando las negociaciones bilaterales entre la UE y EE. UU. sobre un acuerdo relativo al acceso transfronterizo a las pruebas electrónicas para la cooperación en materia penal ([197]).

El intercambio de datos del registro de nombres de los pasajeros (PNR) es otro ámbito de la política de seguridad de la UE que se ha beneficiado del desarrollo de garantías sólidas

([192]) Contribución del Comité, p. 9.
([193]) Resumen de las observaciones del Grupo Multilateral de Expertos sobre el RGPD.
([194]) Directrices n.º 07/2022 y Directrices n.º 04/2021 del CEPD.
([195]) Directrices n.º 2/2020 del CEPD.
([196]) Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas (STCE n.º 224).
([197]) https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en?prefLang=es&etrans=es.

en materia de protección de datos. En 2023, la UE y Canadá concluyeron sus negociaciones sobre un nuevo Acuerdo relativo al PNR en consonancia con los requisitos establecidos por el Tribunal de Justicia en su Dictamen 1/15 ([198]). Se han introducido garantías similares en el capítulo relativo al PNR del Acuerdo de Comercio y Cooperación entre la UE y el Reino Unido. La inclusión de una mayor protección de la privacidad en estos acuerdos, que puede servir de modelo para futuros acuerdos con otros socios, aporta seguridad jurídica a las compañías aéreas y, al mismo tiempo, garantiza la estabilidad de importantes intercambios de información para luchar contra el terrorismo y otros delitos transnacionales graves.

En las negociaciones relativas a la declaración sobre la Iniciativa Conjunta sobre el Comercio Electrónico, la Comisión también se muestra a favor de que se establezcan disposiciones estrictas para proteger la privacidad e impulsar el comercio digital en la Organización Mundial del Comercio. Tras la entrada en vigor del RGPD, también se han incluido sistemáticamente disposiciones similares sobre la lucha contra los obstáculos injustificados al comercio digital, al tiempo que se protege el espacio político necesario de las Partes en el ámbito de la protección de datos, en los acuerdos de libre comercio celebrados por la UE, en particular en el Acuerdo de Comercio y Cooperación entre la UE y el Reino Unido y en los acuerdos con Chile, Japón y Nueva Zelanda. También se están barajando disposiciones relativas a la privacidad y los flujos de datos en las negociaciones sobre comercio digital con Singapur y Corea del Sur.

7.2 Cooperación internacional en materia de protección de datos

7.2.1 La dimensión bilateral

La Comisión ha seguido dialogando con países y organizaciones internacionales sobre el desarrollo, la reforma y la aplicación de las normas de privacidad, en particular mediante la presentación de observaciones a consultas públicas sobre proyectos de legislación o medidas reglamentarias en el ámbito de la privacidad ([199]), la testificación ante los órganos parlamentarios competentes ([200]) y la participación en reuniones específicas con representantes gubernamentales, delegaciones parlamentarias y reguladores de muchas regiones del mundo ([201]). Varias de estas actividades se han llevado a cabo a través del proyecto «Enhanced Data Protection and Data Flows» («Mejora de la protección de datos y los flujos de datos»), financiado por la UE, que brinda apoyo a los países que tienen la intención de desarrollar marcos modernos de protección de datos o de reforzar la capacidad de sus autoridades reguladoras, a través de la formación, el intercambio de conocimientos, el desarrollo de capacidades y el intercambio de buenas prácticas. La Comisión también contribuyó a otras iniciativas, como la Alianza Digital UE-CELAC.

La protección de datos también seguirá desempeñando un papel clave en la labor que la Comisión desempeña en relación con la ampliación. La legislación de la UE en materia de protección de datos es un componente importante del esfuerzo global que hacen los países candidatos por adaptar sus marcos jurídicos a los de la UE (especialmente porque el tratamiento y el intercambio de datos personales constituyen el núcleo de multitud de políticas). Además, la independencia y el correcto funcionamiento de una autoridad de protección de datos es un elemento clave de los sistemas de contrapoderes institucionales

([198]) Propuesta de Decisión del Consejo sobre la firma, en nombre de la Unión Europea, del Acuerdo entre Canadá y la Unión Europea sobre la transferencia y el tratamiento de datos del registro de nombres de los pasajeros (PNR) [COM(2024) 94 final].

([199]) Se trataba de consultas organizadas, por ejemplo, por Australia, China, Ruanda, Argentina, Brasil, Etiopía, Indonesia, Perú, Malasia y Tailandia.

([200]) Por ejemplo, ante los órganos parlamentarios de Chile, Ecuador y Paraguay.

([201]) Esto también incluyó la organización de seminarios y visitas de estudio, por ejemplo, con Kenia, Indonesia y Singapur.

y del Estado de Derecho, y será cada vez más importante a medida que la UE integre gradualmente a los países candidatos en el mercado único (según lo previsto en iniciativas como el Plan de Crecimiento para los Balcanes Occidentales).

Un aspecto cada vez más importante del diálogo de la UE con terceros países se centra en los intercambios entre los reguladores. Como se anunció en el informe de 2020, la Comisión ha creado una «Academia de Protección de Datos» para fomentar los intercambios entre las autoridades de protección de datos de la UE y de terceros países y, de este modo, contribuir al desarrollo de capacidades y mejorar la cooperación «sobre el terreno». La Academia ofrece formación adaptada a petición de las autoridades de terceros países y reúne los conocimientos especializados de los representantes de las fuerzas de seguridad, el mundo académico, el sector privado y las instituciones europeas. El valor añadido de la formación reside en la adaptación de los distintos componentes a los intereses y necesidades de la autoridad requirente. Además, estas formaciones permiten a las autoridades de protección de datos de la UE y de terceros países establecer contactos, compartir conocimientos, intercambiar experiencias y buenas prácticas, y determinar posibles ámbitos de cooperación. Hasta la fecha, la Academia ha impartido formación a las autoridades de protección de datos de Brasil, Indonesia, Kenia, Nigeria y Ruanda, y actualmente está preparando formaciones para otros países.

Más allá de la importancia de mantener un diálogo entre los reguladores, existe una necesidad creciente, como también se reconoce en las observaciones recibidas del Consejo y del Comité ([202]), de desarrollar instrumentos jurídicos adecuados que permitan formas más estrechas de cooperación y asistencia mutua, en particular al permitir el intercambio necesario de información en el contexto de las investigaciones. De hecho, dado que las intrusiones en la vida privada producen cada vez más efectos transfronterizos, a menudo solo pueden investigarse y abordarse eficazmente mediante la cooperación entre reguladores de la UE y de fuera de ella. Por consiguiente, la Comisión solicitará autorización para entablar negociaciones destinadas a celebrar acuerdos de cooperación en materia de ejecución con los terceros países pertinentes (como también se prevé en el artículo 50 del RGPD). A este respecto, la Comisión toma nota de la petición del Comité de que se consideren como posibles homólogos a los países donde la mayoría de los operadores estén sujetos de forma directa al RGPD, en particular los países del G7 o aquellos que cuentan con decisiones de adecuación ([203]).

El establecimiento de estos acuerdos de cooperación y asistencia mutua en materia de ejecución también contribuiría a garantizar el cumplimiento por parte de los operadores extranjeros que estén sujetos al RGPD porque, por ejemplo, porque ofrecen bienes o servicios específicamente al mercado de la UE, así como a la aplicación efectiva del RGPD sobre ellos. El Consejo toma nota de la importancia de hacer cumplir el RGPD en tales casos, y expresa su preocupación por la igualdad de condiciones con las entidades de la UE, así como por la protección efectiva de los derechos de las personas ([204]). La Comisión está de acuerdo con el llamamiento del Consejo a que se estudien diferentes formas de facilitar el cumplimiento en estos casos. Si bien es cierto que unas modalidades más formales de cooperación con los reguladores de terceros países podrían desempeñar un papel importante, también se debería perseguir con mayor firmeza el uso de otras vías ya existentes. Esto incluye hacer pleno uso del conjunto de poderes previstos en el artículo 58 del RGPD e implicar a representantes de empresas extranjeras en la UE (nombrados de conformidad con el artículo 27 del RGPD).

([202]) Contribución del Comité, p. 8; posición y conclusiones del Consejo, apartado 38.
([203]) Contribución del Comité, p. 8.
([204]) Posición y conclusiones del Consejo, apartado 39.

7.2.2 La dimensión multilateral

La Comisión también sigue participando activamente en una serie de foros internacionales para promover valores compartidos y fomentar la convergencia a escala regional y mundial.

Esto incluye, por ejemplo, contribuir activamente a la labor del Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter persona (Convenio 108), el único instrumento multilateral jurídicamente vinculante en el ámbito de la protección de datos personales. Hasta la fecha, 31 Estados han ratificado el Protocolo que modifica y moderniza el Convenio 108 ([205]), entre ellos muchos Estados miembros de la UE, así como algunos no miembros del Consejo de Europa (Argentina, Mauricio y Uruguay). Entre los Estados miembros de la UE, solo la firma de un Estado miembro sigue pendiente ([206]), mientras que hasta la fecha ocho Estados miembros ([207]) han firmado el Convenio modernizado, pero no lo han ratificado. La Comisión insta al Estado miembro restante a firmar el Convenio modernizado y a los demás a que procedan rápidamente a la ratificación a fin de permitir su entrada en vigor en un futuro próximo. Además, sigue fomentando de forma proactiva la adhesión de terceros países.

A nivel del G20 y el G7, los debates sobre la privacidad y los flujos de datos se han centrado en poner en práctica el concepto de «libre circulación de datos con confianza», propuesto inicialmente por Japón, que reconoce que la protección y la seguridad de estos pueden contribuir a la confianza en la economía digital y facilitar los flujos de datos ([208]). La OCDE desempeña un papel especialmente importante en este contexto, ya que proporciona un foro para una comunidad de expertos en materia de libre circulación de datos con confianza, la cual reúne a una amplia gama de partes interesadas (Gobiernos, reguladores, industria, sociedad civil, mundo académico) para contribuir a proyectos específicos y cuestiones relacionadas con este ámbito. Además, un resultado significativo de la iniciativa de la libre circulación de datos con confianza, a la que la Comisión contribuyó significativamente, es la adopción por parte de la OCDE de una Declaración sobre el acceso de los gobiernos a los datos personales en poder de las entidades del sector privado, el primer instrumento internacional en este ámbito. La Declaración contiene una serie de requisitos compartidos para salvaguardar la privacidad en el acceso a los datos personales con fines de seguridad nacional y de aplicación de la ley. En un contexto global en el que cada vez más se reconoce que la confianza en las transferencias de datos se ve afectada negativamente por el acceso desproporcionado del Gobierno, la presente Declaración constituye una importante contribución para facilitar los flujos de datos fiables. La Comisión seguirá animando a los países a adherirse a la Declaración, que también está abierta a los países que no son miembros de la OCDE.

La Comisión también está colaborando con diferentes organizaciones y redes regionales que conforman garantías comunes en materia de protección de datos. Entre ellas se incluyen, por ejemplo, la ASEAN, la Unión Africana, el Foro de Autoridades de Privacidad de Asia-Pacífico, la Red Iberoamericana de Protección de Datos y la Red Africana de Autoridades de Protección de Datos (NADPA-RAPDP). El desarrollo de la mencionada

([205]) Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 223).
([206]) Dinamarca.
([207]) Bélgica, Chequia, Grecia, Irlanda, Letonia, Luxemburgo, Países Bajos y Suecia.
([208]) Véase, por ejemplo, https://www.g7germany.de/resource/blob/974430/2062292/fbdb2c7e996205aee402386aae057c5e/2022-07-14-leaders-communique-data.pdf?download=1.

Guía UE-ASEAN sobre cláusulas tipo es un ejemplo concreto de dicha cooperación fructífera.

Por último, la Comisión mantiene un diálogo con diferentes organizaciones internacionales, en particular para explorar formas de facilitar aún más sus flujos de datos con la UE. Dado que muchas organizaciones han modernizado sus marcos de protección de datos en los últimos años, o están en proceso de hacerlo, también están surgiendo nuevas oportunidades de intercambio de experiencias y buenas prácticas. A este respecto, los talleres anuales con organizaciones internacionales y un grupo de trabajo específico sobre transferencias internacionales de datos organizados por el Supervisor Europeo de Protección de Datos han demostrado ser foros especialmente útiles para intercambiar y explorar instrumentos concretos de cooperación, especialmente el intercambio de datos personales ([209]).

8 CONCLUSIÓN

En los seis años que han transcurrido desde que el RGPD pasó a ser aplicable, este ha empoderado a las personas al permitirles tener un verdadero control sobre sus datos. También ha contribuido a crear unas condiciones de competencia equitativas para las empresas y ha proporcionada una piedra angular para las numerosas iniciativas que impulsan la transición digital en la UE.

Para alcanzar la plena consecución de los dos objetivos del RGPD (a saber, una protección sólida de los particulares, al tiempo que se garantiza la libre circulación de datos personales dentro de la UE, y la seguridad de los flujos de datos fuera de la UE), es necesario centrarse en:

- una aplicación rigurosa del RGPD, empezando por la rápida adopción de la propuesta de normas procedimentales de la Comisión para ofrecer vías de recurso rápidas y seguridad jurídica en los casos que afectan a los particulares en toda la Unión;
- el apoyo proactivo por parte de las autoridades de protección de datos a las partes interesadas en sus esfuerzos de cumplimiento, especialmente a las pymes y los pequeños operadores;
- una interpretación y aplicación coherentes del RGPD en toda la UE;
- una cooperación eficaz entre los reguladores, tanto a escala nacional como de la UE, para garantizar una aplicación sistemática y coherente del creciente corpus de normas digitales de la UE;
- seguir avanzando en la estrategia internacional de la Comisión en materia de protección de datos.

Para apoyar la aplicación efectiva del RGPD e influir en nuevas reflexiones sobre la protección de datos, son necesarias varias acciones identificadas en este punto. La Comisión apoyará y supervisará su aplicación también con vistas al próximo informe, previsto para 2028.

Desarrollo de estructuras de cooperación eficaces

Se invita al Parlamento Europeo y al Consejo a que adopten rápidamente la propuesta sobre las normas procedimentales del RGPD.

([209]) https://www.edps.europa.eu/data-protection/our-work/edps-worldwide/data-protection-and-international-organisations_en.

Se invita al Comité y a las autoridades de protección de datos a que lleven a cabo las siguientes acciones:

- establecer una cooperación regular con otros reguladores sectoriales sobre cuestiones que repercutan en la protección de datos, en particular aquellas establecidas en virtud de la nueva legislación de la UE en el ámbito digital, y participar activamente en estructuras a escala de la UE diseñadas para facilitar la cooperación entre reguladores;
- hagan un uso más amplio de los instrumentos de cooperación previstos en el RGPD, de modo que la resolución de litigios solo se utilice como último recurso;
- aplicar fórmulas de trabajo más eficientes y específicas a las directrices, los dictámenes y las decisiones, y dar prioridad a cuestiones clave con el fin de reducir la carga que pesa sobre las autoridades de protección de datos y responder con mayor rapidez a la evolución del mercado.

Los Estados miembros deben:

- garantizar la independencia plena y efectiva de las autoridades nacionales de protección de datos;
- asignar recursos suficientes a las autoridades de protección de datos para que puedan desempeñar sus funciones, en particular mediante la provisión de los recursos técnicos y los conocimientos especializados necesarios para hacer frente a las tecnologías emergentes y cumplir nuevas responsabilidades en virtud de la legislación digital;
- dotar a las autoridades de protección de datos de los instrumentos de investigación necesarios para que puedan utilizar eficazmente los poderes de ejecución previstos en el RGPD;
- apoyar el diálogo entre las autoridades de protección de datos y otros reguladores nacionales, en particular aquellos que se creen en virtud de nuevos instrumentos jurídicos en materia digital.

La Comisión:

- apoyará activamente la rápida adopción de la propuesta de las normas procedimentales del RGPD por parte de los colegisladores;
- seguirá supervisando de cerca la independencia efectiva y plena de las autoridades nacionales de protección de datos;
- creará sinergias y coherencia entre el RGPD y toda la legislación que afecte al tratamiento de datos personales sobre la base de la experiencia y, en caso necesario, adoptará las medidas adecuadas para proporcionar seguridad jurídica;
- reflexionará como abordar mejor la necesidad de una cooperación estructurada y eficiente entre los reguladores para garantizar una aplicación eficaz, coherente y congruente de las normas de la UE en materia digital, respetando al mismo tiempo la competencia de las autoridades de protección de datos en lo que respecta a todas las cuestiones relativas al tratamiento de datos personales.

Aplicar y complementar el marco jurídico

Los Estados miembros deben:

- garantizar que se consulte oportunamente a las autoridades de protección de datos antes de la adopción de la legislación sobre el tratamiento de datos personales.

La Comisión:

- seguirá haciendo uso de todos los instrumentos a su disposición, en particular los procedimientos de infracción, para garantizar que los Estados miembros cumplan el RGPD;
- seguirá apoyando los intercambios de puntos de vista y prácticas nacionales entre los Estados miembros, en particular a través del Grupo de Expertos de los Estados miembros sobre el RGPD;
- llevará a cabo acciones para garantizar la protección, la capacitación y el respeto de los niños en línea;
- reflexionará sobre las posibles perspectivas de futuro en relación con la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, especialmente su relación con el RGPD.

Apoyar a las partes interesadas

Se invita al Comité y a las autoridades de protección de datos a que lleven a cabo las siguientes acciones:

- entablar un diálogo constructivo con los responsables y encargados del tratamiento acerca del cumplimiento del RGPD;
- seguir intensificando los esfuerzos para apoyar el cumplimiento por parte de las pymes, proporcionando orientaciones y herramientas diseñadas a medida, disipando cualquier preocupación infundada en materia de cumplimiento que tengan las pymes que no tratan datos personales como actividad principal, y acompañándolas en sus esfuerzos de cumplimiento;
- apoyar la aplicación de medidas de cumplimiento eficaces por parte de las empresas, como la certificación y los códigos de conducta (también como herramientas para las transferencias), mediante la colaboración con las partes interesadas durante el proceso de aprobación, el establecimiento de plazos claros para las aprobaciones y, tal como se prometió en la Estrategia 2024-2027 del Comité, la explicación a los principales grupos de partes interesadas de cómo pueden utilizarse estas herramientas;
- garantizar que las directrices nacionales y la aplicación del RGPD a escala nacional sean coherentes con las directrices del Comité y la jurisprudencia del Tribunal de Justicia;
- resolver interpretaciones divergentes del RGPD entre las autoridades de protección de datos, y especialmente entre las autoridades de un mismo Estado miembro;
- proporcionar directrices concisas, prácticas y accesibles para el público pertinente, tal como se prometió en la Estrategia 2024-2027 del Comité;
- garantizar consultas más tempranas y significativas acerca de las directrices y dictámenes con el fin de comprender mejor la dinámica del mercado y las prácticas empresariales, estudiar debidamente las observaciones recibidas y tener en cuenta la aplicación concreta de las interpretaciones adoptadas;
- completar con carácter prioritario los trabajos en curso sobre las directrices relativas a los datos de los niños, la investigación científica, la anonimización, la seudonimización y el interés legítimo;
- intensificar las actividades de sensibilización, la información y las medidas coercitivas para garantizar que los delegados de protección de datos puedan desempeñar las funciones que les confiere el RGPD.

La Comisión:

- seguirá prestando apoyo financiero a las actividades de las autoridades de protección de datos que faciliten la aplicación de las obligaciones del RGPD por parte de las pymes;
- utilizará todos los medios disponibles para proporcionar aclaraciones oportunas sobre cuestiones de importancia para las partes interesadas, especialmente las pymes, en particular solicitando dictámenes del Comité.

Continuar el desarrollo del conjunto de instrumentos para las transferencias de datos y la cooperación internacional

Se invita al Comité y a las autoridades de protección de datos a llevar a cabo las siguientes acciones:

- completar las labores de optimización y acortamiento del proceso de aprobación de las normas corporativas vinculantes, así como la actualización de las orientaciones sobre los elementos que deben incluirse en las normas corporativas vinculantes para el encargado del tratamiento;
- explorar formas y herramientas para seguir ayudando a los exportadores de datos en sus esfuerzos de cumplimiento en relación con los requisitos de la sentencia Schrems II;
- explorar otras formas de garantizar el cumplimiento efectivo de las normas por parte de los operadores establecidos en terceros países que entren en el ámbito territorial de aplicación del RGPD.

Los Estados miembros deben:

- garantizar la firma y la ratificación del Convenio 108 modernizado del Consejo de Europa lo antes posible, con vistas a permitir su entrada en vigor.

La Comisión:

- seguirá avanzando en los diálogos sobre adecuación que están en curso, explorará el desarrollo de las constataciones existentes en materia de adecuación y entablará nuevas conversaciones sobre adecuación con socios interesados;
- fomentará una mayor cooperación entre la red de países que se benefician de decisiones de adecuación;
- finalizará los trabajos sobre cláusulas contractuales tipo adicionales, en particular en lo que respecta a las transferencias de datos a importadores de datos cuyo tratamiento esté directamente sujeto al RGPD y a las transferencias efectuadas en virtud del Reglamento (UE) 2018/1725 por parte de las instituciones y organismos de la Unión;
- cooperará con socios internacionales para facilitar los flujos de datos sujetos a cláusulas contractuales tipo;
- apoyará los procesos de reforma en curso en terceros países sobre normas de protección de datos nuevas o modernizadas mediante el intercambio de experiencias y buenas prácticas;
- colaborará con organizaciones internacionales y regionales como la OCDE y el G7 para promover la circulación de datos fiables basada en normas estrictas de protección de datos, incluido en el contexto de la iniciativa de «libre circulación de datos con confianza»;
- facilitará y apoyará los intercambios entre los reguladores europeos e internacionales, en particular a través de su Academia de Protección de Datos;

- contribuirá a facilitar la cooperación internacional en materia de cumplimiento de la normativa entre las autoridades de control, especialmente mediante la negociación de acuerdos de cooperación y asistencia mutua.