COMISIÓN
EUROPEA

Bruselas, 24.6.2020
COM(2020) 264 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

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

{SWD(2020) 115 final}

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

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

1 LA PROTECCIÓN DE DATOS COMO PILAR DEL EMPODERAMIENTO DE LOS CIUDADANOS Y DEL ENFOQUE DE LA UE PARA LA TRANSICIÓN DIGITAL

El presente informe es el primero sobre la evaluación y revisión del Reglamento General de Protección de Datos[1] (en lo sucesivo, el «RGPD»), en particular sobre la aplicación y el funcionamiento de las normas sobre la transferencia de datos personales a terceros países y organizaciones internacionales y de las normas sobre cooperación y coherencia, con arreglo al artículo 97 del RGPD.

El RGPD, en aplicación desde el 25 de mayo de 2018, ocupa un lugar central en el marco de la UE[2] para la garantía del derecho fundamental a la protección de datos, consagrado en la Carta de los Derechos Fundamentales de la Unión Europea (artículo 8) y en los Tratados (artículo 16 del Tratado de Funcionamiento de la Unión Europea, en adelante, el «TFUE») El RGPD ha reforzado las salvaguardias de protección de datos, aporta a los particulares derechos adicionales y más sólidos, una mayor transparencia, y garantiza que todos aquellos que tratan datos personales en el ámbito de su aplicación deban rendir más cuentas y tengan una mayor responsabilidad. Dota a las autoridades independientes de protección de datos de competencias mayores y armonizadas e implanta un nuevo sistema de gobernanza. Asimismo, crea unas condiciones de competencia equitativas para todas las empresas que operan en el mercado de la UE, con independencia del lugar en el que estén establecidas, y garantiza la libre circulación de datos dentro de la UE, reforzando así el mercado interior.

El RGPD es un componente importante del enfoque tecnológico centrado en las personas y una guía para el uso de la tecnología en las dos transiciones, la verde y digital, que caracterizan la elaboración de políticas de la UE. Esto se ha puesto de relieve, más recientemente, en el Libro Blanco sobre la Inteligencia Artificial[3] y en la

---

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

[2] A raíz de su incorporación al Acuerdo sobre el Espacio Económico Europeo (EEE), el Reglamento se aplica también a Noruega, Islandia y Liechtenstein.

[3] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

Comunicación sobre una estrategia europea de datos[4] (en lo sucesivo, «la estrategia de datos») de febrero de 2020.

En una economía basada cada vez más en el tratamiento de datos, incluidos los datos personales, el RGPD es una herramienta esencial para garantizar que los particulares tengan un mayor control sobre sus datos personales y que estos datos se traten con fines legítimos, de una manera lícita, justa y transparente. Al mismo tiempo, el RGPD contribuye a fomentar la innovación digna de confianza, en particular a través de su enfoque y principios basados en el riesgo, como la protección de la privacidad desde el diseño y por defecto. La Comisión ha propuesto complementar el marco normativo sobre privacidad y protección de datos[5] mediante el Reglamento sobre la Privacidad y las Comunicaciones Electrónicas[6], destinado a sustituir a la actual Directiva sobre la privacidad y las comunicaciones electrónicas[7]. Esta propuesta está siendo examinada por los colegisladores y es muy importante garantizar su rápida adopción.

Como parte de las prioridades clave de la Comisión para una «Una Europa Adaptada a la Era Digital[8]» y el «Pacto Verde Europeo[9]», pueden desarrollarse nuevas iniciativas para empoderar a los ciudadanos a fin de que desempeñen un papel más activo en la transición digital y en el aprovechamiento del uso de herramientas digitales para lograr una sociedad climáticamente neutra y un desarrollo más sostenible. El RGPD establece un marco para estas iniciativas y garantiza que estas estén diseñadas para empoderar eficazmente a los particulares.

La estrategia en materia de datos[10] aboga por la creación de un «espacio común europeo de datos», un verdadero mercado único de datos, así como de diez espacios de datos sectoriales europeos comunes pertinentes para las dos transiciones, la verde y la digital[11]. Para todas estas prioridades, es fundamental disponer de un marco claro y viable para el intercambio seguro de datos y un aumento de la disponibilidad de datos. La estrategia en materia de datos anunció también la intención de la Comisión de estudiar en la futura legislación cómo hacer posible el uso de los datos contenidos en bases de

---

[4] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

[5] Este marco normativo abarca también la Directiva sobre protección de datos en el ámbito penal (Directiva 2016/680) y Reglamento sobre protección de datos para las instituciones y los organismos de la UE (Reglamento 2018/1725).

[6] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) [COM(2017) 010 final - 2017/03 (COD)].

[7] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

[8] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_es

[9] Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «El Pacto Verde europeo» [COM (2019) 640 final].

[10] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Una estrategia europea de datos» [COM(2020) 66 final].

[11] Estos diez espacios de datos sectoriales europeos comunes se refieren a: la salud, la industria manufacturera, la energía, la movilidad, la agricultura, los datos financieros, la administración pública, un espacio común europeo de datos sobre capacidades, un espacio de datos sobre el Pacto Verde Europeo y una Nube Europea de la Ciencia Abierta.

datos públicas para fines de investigación científica de forma compatible con el RGPD. Los espacios de datos deben contar con el apoyo de la federación en la nube europea, que prestará servicios de tratamiento de datos e infraestructuras en la nube conformes con el RGPD. El RGPD garantiza un elevado nivel de protección de los datos personales y un papel central de las personas en todos estos espacios de datos, al tiempo que proporciona la flexibilidad necesaria para dar cabida a diferentes enfoques.

La necesidad de garantizar la confianza y la demanda de protección de los datos personales no se limitan en modo alguno a la UE. Las personas de todo el mundo valoran cada vez más la privacidad y la seguridad de sus datos. Como muestra un reciente sondeo global[12], consideran que es un factor importante que influye en sus decisiones de compra y en su comportamiento en línea. Un número cada vez mayor de empresas han respondido a esta demanda de privacidad, en particular mediante la ampliación voluntaria de algunos de los derechos y salvaguardias previstos en el RGPD a sus clientes de fuera de la UE. Muchas empresas también promueven el respeto de los datos personales como factor competitivo diferenciador y reclamo en el mercado mundial, al ofrecer productos y servicios innovadores con soluciones novedosas en materia de privacidad o de seguridad de los datos. Por otra parte, el aumento de la capacidad de los actores de los sectores público y privado para recopilar y procesar datos a gran escala plantea cuestiones importantes y complejas que confieren a la privacidad un lugar cada vez más central en el debate público en distintas partes del mundo.

La adopción del RGPD ha inducido a otros países de muchas regiones del mundo a considerar la posibilidad de hacer lo propio. Se trata de una tendencia verdaderamente global que abarca desde Chile a Corea del Sur, desde Brasil a Japón, desde Kenia hasta la India, y desde California hasta Indonesia. El liderazgo de la UE en materia de protección de datos pone de manifiesto su capacidad de establecer normas de referencia a escala mundial para la regulación de la economía digital y ha sido bien acogido por importantes voces de la comunidad internacional, como el Secretario General de las Naciones Unidas, António Guterres, quien ha señalado que el RGPD ha «*establecido un ejemplo [...] inspirador de medidas similares en otros lugares*» y «*[ha] insta[do] a la UE y a sus Estados miembros a que sigan liderando la configuración de la era digital y estén a la vanguardia de la innovación y la regulación tecnológicas*»[13].

La actual crisis pandémica de la COVID-19 constituye un claro ejemplo de esta globalización del debate sobre la privacidad, tanto durante la crisis como en el período de recuperación mundial posterior. En la UE, varios Estados miembros han adoptado medidas de emergencia en un esfuerzo por proteger la salud pública. El RGPD es claro en el sentido de que cualquier restricción debe respetar el contenido esencial de

---

[12] Véase, por ejemplo, el Cisco's Consumer Privacy Study 2019 (https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf). Según este estudio, en el que participaron 2 600 consumidores de todo el mundo, un número significativo de consumidores ya ha tomado medidas para proteger su privacidad, por ejemplo, cambiando de empresas o proveedores debido a sus políticas de datos o a sus prácticas de intercambio de información.

[13] Discurso del Secretario General de las Naciones Unidas al Senado Italiano de 18 de diciembre de 2019 (disponible en: https://www.un.org/press/en/2019/sgsm19916.doc.htm).

los derechos y libertades fundamentales y ser una medida necesaria y proporcionada en una sociedad democrática para salvaguardar un interés público como, por ejemplo, la salud pública. Dado que se están eliminando progresivamente las medidas de contención, los responsables de la toma de decisiones deben dar respuesta a las expectativas de los ciudadanos de que se les ofrezcan soluciones digitales fiables y respetuosas de los derechos a la intimidad y a la protección de los datos personales.

En muchos países, las medidas de protección de la privacidad incorporadas, como la inscripción voluntaria por los usuarios, la minimización y la seguridad de los datos o la exclusión de la geolocalización, se consideran esenciales para garantizar la fiabilidad y la aceptación social de las soluciones basadas en datos destinadas a controlar y contener la propagación del virus, calibrar las contramedidas de política pública, ayudar a los pacientes o aplicar estrategias de salida. En la UE, el marco normativo en materia de protección de datos y privacidad[14] ha demostrado ser una herramienta lo suficientemente flexible para permitir el desarrollo de soluciones prácticas (por ejemplo, las aplicaciones de rastreo), garantizando al mismo tiempo un elevado nivel de protección de los datos personales. En este contexto, el 16 de abril de 2020, la Comisión publicó unas orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia en lo referente a la protección de datos[15].

La protección de los datos personales también es fundamental para prevenir la manipulación de las opciones de los ciudadanos, en particular a través de la microsegmentación de los votantes basada en el tratamiento ilícito de datos personales, evitando las interferencias en los procesos democráticos y preservando el debate abierto, la equidad y la transparencia esenciales en una democracia. Por este motivo, en septiembre de 2018 la Comisión publicó las Orientaciones relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral[16].

Para esta evaluación y revisión, la Comisión ha tenido en cuenta las contribuciones del Consejo[17], del Parlamento Europeo[18], del Comité Europeo de Protección de Datos

---

[14] Este marco incluye, además del RGPD, la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva 2002/58/CE), que establece normas, entre otras cosas, sobre el acceso y el almacenamiento de información en el equipo terminal del usuario.

[15] Comunicación de la Comisión «Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos» 2020/C 124 I/01 - C(2020) 2523 - (DO C 124I de 17.4.2020, p. 1). El 16 de abril de 2020, los Estados miembros de la UE, con el apoyo de la Comisión, desarrollaron un conjunto de instrumentos de la UE para el uso de aplicaciones móviles de rastreo de contactos y alerta en respuesta a la pandemia de coronavirus. Esto forma parte de un enfoque coordinado común para apoyar la supresión gradual de las medidas de confinamiento. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[16] Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral: Contribución de la Comisión Europea a la reunión de dirigentes en Salzburgo los días 19 y 20 de septiembre de 2018 [COM (2018) 638 final].

[17] Posición y conclusiones del Consejo sobre la aplicación del Reglamento General de Protección de Datos:
https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-2/es/pdf

[18] Carta de la Comisión LIBE del Parlamento Europeo de 21 de febrero de 2020 al Comisario Reynders, Ref.: IPOL-COM-LIBE D (2020)6525.

(en lo sucesivo, «el Comité»)[19] y las diferentes autoridades de protección de datos[20], del grupo multilateral de expertos[21] y de otras partes interesadas, incluidas las observaciones realizadas respecto de la hoja de ruta[22].

La opinión general es que, dos años después de que comenzara a aplicarse, el RGPD ha cumplido satisfactoriamente sus objetivos de reforzar la protección del derecho de los particulares a la protección de los datos personales y de garantizar la libre circulación de los datos personales en la UE[23]. Sin embargo, también se han detectado una serie de ámbitos en los que caben mejoras futuras. Como la mayoría de las partes interesadas y las autoridades de protección de datos, la Comisión opina que sería prematuro en estos momentos extraer conclusiones definitivas sobre la aplicación del RGPD. Es probable que la mayoría de los problemas detectados por los Estados miembros y las partes interesadas puedan mejorarse cuando se cuente con una mayor experiencia en la aplicación del RGPD en los próximos años. No obstante, el presente informe pone de relieve los retos a los que se ha enfrentado hasta ahora el RGPD y establece posibles maneras de abordarlos.

A pesar de su énfasis en las dos cuestiones destacadas en el artículo 97, apartado 2, del RGPD, a saber, las transferencias internacionales y los mecanismos de cooperación y coherencia, esta evaluación y revisión adopta un enfoque más amplio para abordar también cuestiones planteadas por diversos actores durante los dos últimos años.

2 PRINCIPALES CONCLUSIONES

Aplicación del RGPD y funcionamiento de los mecanismos de cooperación y coherencia

El RGPD estableció un sistema de gobernanza innovador, basado en autoridades independientes de protección de datos de los Estados miembros y en su cooperación en asuntos transfronterizos y en el Comité Europeo de Protección de Datos («el Comité»). La opinión general es que las autoridades de protección de datos han hecho un uso equilibrado de sus poderes correctivos reforzados, incluidas las advertencias, los apercibimientos, las multas y las limitaciones temporales o definitivas del tratamiento[24]. La Comisión observa que las autoridades han aplicado multas administrativas de entre unos pocos miles y varios millones de euros, dependiendo de la gravedad de las infracciones. Otras sanciones, como las prohibiciones del

[19] Contribución del Comité a la evaluación del RGPD con arreglo al artículo 97, adoptada el 18 de febrero de 2020: https://edpb.europa.eu/our-work-tools/our-documents/other/contribution-edpb-evaluation-gdpr-under-article-97_en

[20] https://edpb.europa.eu/individual-replies-data-protection-supervisory-authorities_es

[21] El Grupo Multilateral de Expertos sobre el Reglamento creado por la Comisión está integrado por representantes de la sociedad civil y del sector empresarial, miembros del mundo académico y profesionales: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537

[22] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12322-Report-on-the-application-of-the-General-Data-Protection-Regulation/feedback?p_id=7669437

[23] Véanse, por ejemplo, la posición y las conclusiones del Consejo, así como la contribución del Comité.

[24] Véase el punto 2.1 del Documento de trabajo de los servicios de la Comisión.

tratamiento, pueden tener un efecto disuasorio igual o incluso superior al de las multas. El objetivo último del RGPD es cambiar la cultura y el comportamiento de todos los actores participantes en beneficio de las personas. En el documento de trabajo de los servicios de la Comisión adjunto se ofrece información más detallada sobre el uso de los poderes correctivos por parte de las autoridades de protección de datos.

Aunque todavía es pronto para evaluar plenamente el funcionamiento de los nuevos mecanismos de cooperación y coherencia, las autoridades de protección de datos han desarrollado su cooperación a través del mecanismo de ventanilla única[25] y de un amplio uso de la asistencia mutua[26]. El mecanismo de ventanilla única, que es un activo clave del mercado interior, se utiliza para resolver muchos casos transfronterizos[27]. Actualmente, están aún pendientes decisiones importantes con dimensión transfronteriza que estarán sujetas al sistema de ventanilla única. Estas decisiones, que afectan a menudo a grandes empresas tecnológicas multinacionales, tendrán un impacto sustancial en los derechos de las personas en muchos Estados miembros.

No obstante, el desarrollo de una cultura europea de protección de datos verdaderamente común entre las autoridades de protección de datos sigue siendo un proceso en curso. Las autoridades de protección de datos no han hecho aún pleno uso de los instrumentos que ofrece el RGPD, como las operaciones conjuntas que podrían llevar a investigaciones conjuntas. En ocasiones, la búsqueda de un enfoque común se tradujo en la adopción del mínimo común denominador y, como consecuencia de ello, se desaprovecharon las oportunidades de fomentar una mayor armonización[28].

Es necesario seguir avanzando para que la tramitación de los casos transfronterizos sea más eficaz y esté más armonizada en toda la UE, también desde el punto de vista del procedimiento, por ejemplo en cuestiones como los procedimientos de tramitación de reclamaciones, los criterios de admisibilidad de las reclamaciones, la duración de los procedimientos debido a los diferentes calendarios o a la ausencia de plazos en el Derecho procesal administrativo nacional, el momento procedimental en que se concede el derecho a ser oído o la información y la participación de los reclamantes durante el procedimiento. Se acoge con satisfacción el proceso de reflexión iniciado por el Comité en relación con esta cuestión, y la Comisión participa en estos debates[29].

Las actividades y las orientaciones del Comité son de una importancia fundamental para que sigan desarrollándose de forma coherente los intercambios entre el Comité y las partes interesadas[30]. A finales de 2019, el Comité había adoptado 67 documentos,

[25] Si una empresa está llevando a cabo un tratamiento de datos transfronterizo, la autoridad competente en materia de protección de datos es la del Estado miembro en que se encuentra el establecimiento principal de la compañía.
[26] Véase el punto 2.2 del Documento de trabajo de los servicios de la Comisión.
[27] Entre el 25 de mayo de 2018 y el 31 de diciembre de 2019, se presentaron 141 proyectos de decisión a través del procedimiento de ventanilla única, de los cuales 79 dieron lugar a decisiones definitivas.
[28] Por ejemplo, las listas nacionales sobre los tipos de operaciones de tratamiento que requieren una evaluación de impacto relativa a la protección de datos en virtud del artículo 35 del RGPD podrían haberse armonizado mejor.
[29] Véase el punto 2.2 del Documento de trabajo de los servicios de la Comisión.
[30] En particular representantes de empresas y de la sociedad civil. Véase el punto 2.3 del Documento de trabajo de los servicios de la Comisión.

incluidas 10 nuevas directrices[31] y 43 dictámenes[32]. En general, las partes interesadas acogen con satisfacción las directrices del Comité y piden que se añadan otras sobre conceptos clave del RGPD, pero también señalan incoherencias entre las orientaciones nacionales y las directrices del Comité. Subrayan la necesidad de un mayor asesoramiento práctico, en particular ejemplos más concretos, y la necesidad de que las autoridades de protección de datos estén dotadas de los recursos humanos, técnicos y financieros necesarios para llevar a cabo eficazmente sus tareas.

La Comisión ha subrayado sistemáticamente la obligación de los Estados miembros de asignar suficientes recursos humanos, financieros y técnicos a las autoridades nacionales de protección de datos[33]. La mayor parte de las autoridades se beneficiaron de un aumento de personal y de presupuesto entre 2016 y 2019[34]; las autoridades irlandesas, neerlandesas, islandesas, luxemburguesas y finlandesas son las que se beneficiaron de los mayores aumentos relativos de personal. Dado que las multinacionales tecnológicas de mayor tamaño están establecidas en Irlanda y Luxemburgo, las autoridades de protección de datos de estos países actúan como autoridades principales en muchos casos transfronterizos importantes y pueden necesitar más recursos de los que cabría esperar atendiendo a su población. Sin embargo, la situación sigue siendo desigual en función de los Estados miembros y todavía no es satisfactoria en términos generales. Las autoridades de protección de datos desempeñan un papel esencial a la hora de garantizar que el RGPD se aplique a nivel nacional y que los mecanismos de cooperación y coherencia en el seno del Comité funcionen de manera eficaz, incluido, en particular, el mecanismo de ventanilla única para los casos transfronterizos. Por consiguiente, se insta a los Estados miembros a proporcionarles recursos suficientes, tal como exige el RGPD[35].

Normas armonizadas, pero aún con cierto grado de fragmentación y enfoques divergentes

La Comisión está supervisando la aplicación del RGPD en la legislación nacional. En el momento de elaboración del presente informe, a excepción de Eslovenia, todos los Estados miembros han adoptado nueva legislación o han adaptado su legislación nacional en materia de protección de datos. Se ha pedido a Eslovenia[36] que aporte aclaraciones a la Comisión sobre la finalización de este proceso[37].

---

[31] Que se añaden a las 10 directrices adoptadas por el Grupo de Trabajo del Artículo 29 en el período previo a la entrada en vigor del Reglamento y refrendadas por el Comité. El Comité adoptó también 4 directrices adicionales entre enero y el final de mayo de 2020, y actualizó una directriz ya existente.

[32] 42 de estos dictámenes se adoptaron con arreglo al artículo 64 del RGPD y uno se adoptó con arreglo al artículo 70, apartado 1, letra s), del RGPD y se refería a la decisión de adecuación con respecto a Japón.

[33] Comunicación de la Comisión al Parlamento Europeo y al Consejo - Balance de las normas de protección de datos como catalizador de la confianza en la UE y fuera de sus fronteras, [COM(2019) 374 final de 24.7.2019].

[34] En total, se ha registrado un aumento del 42 % en el personal y del 49 % en el presupuesto en el caso de las autoridades nacionales de protección de datos, consideradas en su conjunto en el EEE entre 2016 y 2019.

[35] Véase el punto 2.4 del Documento de trabajo de los servicios de la Comisión.

[36] En el caso más reciente, mediante carta del Comisario Reynders de marzo de 2020.

[37] Cabe señalar que la autoridad nacional de protección de datos de Eslovenia está establecida con arreglo a la legislación nacional vigente en materia de protección de datos y supervisa de la aplicación del RGPD en dicho Estado miembro.

El RGPD establece un enfoque coherente para las normas de protección de datos en toda la UE. Sin embargo, obliga a los Estados miembros a legislar en algunos ámbitos[38] y les ofrece la posibilidad de especificar más el RGPD en otros[39]. Como consecuencia de ello, sigue existiendo un cierto grado de fragmentación que se debe sobre todo al uso generalizado de cláusulas de especificación facultativas. Por ejemplo, las diferencias entre Estados miembros en cuanto a la edad de consentimiento de los niños en relación con los servicios de la sociedad de la información crea incertidumbre para los niños y sus padres en cuanto a la aplicación de sus derechos de protección de datos en el mercado único. Esta fragmentación plantea también una serie de retos para la realización de actividades empresariales transfronterizas, la innovación —en particular por lo que respecta a los nuevos avances tecnológicos— y las soluciones en materia de ciberseguridad. Para el funcionamiento eficaz del mercado interior y para evitar cargas innecesarias a las empresas, también es esencial que la legislación nacional no vaya más allá de los márgenes establecidos por el RGPD ni introduzca requisitos adicionales cuando no exista margen para ello.

Un reto específico para la legislación nacional es la conciliación del derecho a la protección de los datos personales con la libertad de expresión y de información y la búsqueda del equilibrio adecuado de estos derechos. Algunas legislaciones nacionales establecen el principio de primacía de la libertad de expresión, mientras que otras establecen la primacía de la protección de los datos personales y únicamente eximen de la aplicación de las normas de protección de datos en situaciones específicas, como aquellas relacionadas con los personajes públicos. Por último, otros Estados miembros prevén una cierta ponderación —ya sea por parte del legislador y/o en una evaluación caso por caso— en lo que se refiere a las excepciones a determinadas disposiciones del RGPD.

La Comisión continuará su evaluación de la legislación nacional. La conciliación ha de operarse por ley, respetar el contenido esencial de dichos derechos y libertades fundamentales y ser una medida necesaria y proporcionada[40]. Las normas de protección de datos (así como su interpretación y aplicación) no deben afectar al ejercicio de la libertad de expresión y de información, por ejemplo mediante la creación de un efecto paralizante o la presión sobre los periodistas para que revelen sus fuentes. La búsqueda de un equilibrio entre estos dos derechos mediante la legislación nacional ha de tener en cuenta la jurisprudencia del Tribunal de Justicia y del Tribunal Europeo de Derechos Humanos[41].

La legislación de los Estados miembros sigue planteamientos diferentes a la hora de aplicar excepciones a la prohibición general de tratamiento de categorías especiales de datos personales en lo que se refiere al nivel de especificación y salvaguardias, incluidas las relativas a la salud y a la investigación. Para hacer frente a este problema, la Comisión está comenzando por examinar —como primer paso— los

[38] Véase el punto 3.1 del Documento de trabajo de los servicios de la Comisión.
[39] Véase el punto 3.2 del Documento de trabajo de los servicios de la Comisión.
[40] Artículo 52, apartado 1, de la Carta.
[41] Véase el punto 3.1 del documento de trabajo de los servicios de la Comisión: Conciliación del derecho a la protección de los datos personales con la libertad de expresión y de información.

diferentes enfoques de los Estados miembros[42]; a continuación, apoyará la creación de un código (o códigos) de conducta que contribuya(n) a un enfoque más coherente en este ámbito y faciliten el tratamiento transfronterizo de datos personales[43]. Además, las futuras directrices del Comité sobre el uso de datos personales en el ámbito de la investigación científica contribuirán a un enfoque armonizado. La Comisión aportará su contribución al Comité, en particular en lo relativo a la investigación en materia de salud, incluido en forma de preguntas concretas y análisis de hipótesis específicas que haya recibido de la comunidad investigadora.

[42] La Comisión ha iniciado un estudio sobre la «Evaluación de las normas de los Estados miembros sobre datos sanitarios a la luz del RGPD», Chafea/2018/Health/03, contrato específico n.º 2019 70 01.
[43] Véanse las medidas anunciadas en la Estrategia Europea de Datos, página 30.

Empoderar a las personas para que controlen sus datos

Según una encuesta sobre los derechos fundamentales[44], el 69 % de la población de la UE de más de 16 años ha oído hablar del RGPD, y el 71 % de las personas en la UE saben cuál es su autoridad nacional de protección de datos.

Los particulares son cada vez más conscientes de sus derechos: los derechos de acceso, rectificación, supresión y portabilidad de sus datos personales, el derecho a oponerse al tratamiento y una mayor transparencia. El RGPD ha fortalecido los derechos procesales, incluyendo el derecho a presentar una reclamación ante una autoridad de protección de datos —incluso a través de acciones de representación— y el derecho a la tutela judicial. Los particulares hacen valer estos derechos cada vez más, pero es necesario facilitar su ejercicio y su plena aplicación. Las reflexiones que está dirigiendo el Comité aclararán y facilitarán aún más el ejercicio de los derechos individuales, mientras que se espera que la propuesta de Directiva sobre acciones de representación[45], una vez adoptada, permita a los particulares presentar demandas colectivas en todos los Estados miembros y reduzca los costes de las demandas transfronterizas.

El derecho a la portabilidad de los datos tiene un claro potencial —aún por aprovechar en su plenitud— para situar a las personas en el centro de la economía de los datos, permitiéndoles cambiar entre distintos proveedores de servicios, combinar diferentes servicios, utilizar otros servicios innovadores y elegir los servicios más favorables en términos de protección de datos. Esto fomentará la competencia de manera indirecta y apoyará la innovación. Liberar este potencial es una de las prioridades de la Comisión, en particular porque, con el creciente uso de dispositivos conectados al «Internet de las cosas», cada vez son más los datos generados por los consumidores, que corren el riesgo de verse confrontados a prácticas desleales y a efectos de «bloqueo». La portabilidad podría reportar importantes beneficios de salud y bienestar, de reducción de la huella ambiental y acceso a servicios públicos y privados, una mayor productividad en la fabricación, y una mayor calidad y seguridad de los productos.

La estrategia de datos puso de relieve la necesidad de abordar dificultades como la falta de estándares que permitan el suministro de datos en un formato legible por máquina y de aumentar el uso efectivo del derecho a la portabilidad de los datos, que actualmente se limita a unos pocos sectores (por ejemplo, la banca y las telecomunicaciones). Esto podría hacerse, en particular, mediante el diseño de las herramientas, el formato normalizado y las interfaces adecuados[46]. Este mayor uso también podría conseguirse haciendo obligatoria la utilización de interfaces técnicas y formatos legibles por máquina que permitan la portabilidad de los datos en tiempo real. Una mayor utilización del derecho a la portabilidad podría, entre otras cosas,

---

[44] Agencia de los Derechos Fundamentales de la Unión Europea (FRA) (2020): encuesta sobre los derechos fundamentales de 2019. Protección y tecnología de datos: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

[45] Una vez adoptada, la propuesta de Directiva relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores [COM(2018) 0184 final — 2018/089 (COD)] reforzará el marco de acciones de representación, también en el ámbito de la protección de datos.

[46] Entre estos instrumentos pueden figurar los instrumentos de gestión del consentimiento y las aplicaciones de gestión de la información personal.

hacer más fácil para las personas permitir la utilización de sus datos para el bien común (por ejemplo, para fomentar la investigación en el sector de la salud), en caso de que deseen hacerlo («altruismo en los datos»). En preparación del paquete normativo sobre servicios digitales[47], la Comisión examinará de forma más amplia el papel de los datos y de las prácticas relacionadas con los datos en el ecosistema de plataformas.

[47] https://ec.europa.eu/commission/presscorner/detail/es/ip_20_962

Oportunidades y retos para las organizaciones, en particular para las pymes

El RGPD, junto con el Reglamento relativo a la libre circulación de datos no personales[48], ofrece oportunidades a las empresas mediante el fomento de la competencia y la innovación, garantizando la libre circulación de datos dentro de la UE y creando condiciones de competencia equitativas con las empresas establecidas fuera de la UE[49]. El derecho a la portabilidad, unido al incremento del número de personas en busca de soluciones más respetuosas de la privacidad, puede reducir las barreras de entrada para las empresas y permitir aprovechar las posibilidades de crecimiento basadas en la confianza y la innovación. Algunas partes interesadas informaron de que la aplicación del RGPD plantea algunos retos, especialmente para las pymes. Según el enfoque basado en el riesgo, no sería apropiado establecer excepciones en función del tamaño de los operadores, ya que su tamaño no constituye en sí mismo un indicador de los riesgos que el tratamiento de datos personales que realiza puede crear para los particulares. Varias autoridades de protección de datos han proporcionado instrumentos prácticos para facilitar la aplicación del RGPD por parte de las pymes con actividades de tratamiento de bajo riesgo. Estos esfuerzos deben intensificarse y extenderse, preferiblemente en el marco de un enfoque europeo común a fin de no crear obstáculos al mercado único.

Las autoridades de protección de datos han desarrollado una serie de actividades para ayudar a las pymes a cumplir lo dispuesto en el RGPD mediante, por ejemplo, el suministro de modelos de contratos de tratamiento y de registros para las actividades de tratamiento, así como los seminarios y las líneas directas de consulta. Algunas de estas iniciativas contaron con financiación de la UE[50]. Se deben considerar más actividades para facilitar la aplicación del RGPD a las pymes.

El RGPD ofrece un conjunto de instrumentos a todo tipo de empresas y organizaciones para ayudarles a acreditar el cumplimiento, como los códigos de conducta, los mecanismos de certificación y la cláusula contractual tipo. Este conjunto de instrumentos debe aprovecharse al máximo. Las pymes insisten, en particular, en la importancia y la utilidad de los códigos de conducta adaptados a su situación y que no conlleven costes desproporcionados. Por lo que se refiere a los regímenes de certificación, la seguridad (incluida la ciberseguridad) y la protección de datos desde el diseño son elementos clave que deben tenerse en cuenta en el RGPD, y que se verán reforzados por un enfoque común y ambicioso en toda la UE. La Comisión está trabajando actualmente en las cláusulas contractuales tipo entre los responsables y los encargados del tratamiento[51], basándose en los trabajos en curso

[48] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo relativo a un marco para la libre circulación de datos no personales en la Unión Europea (DO L 303 de 28.11.2018- 59).

[49] Véase el punto 5 del Documento de trabajo de los servicios de la Comisión. Véase también COM(2019) 250 final, Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea, en las que se explican las normas que rigen el tratamiento de conjuntos de datos mixtos, compuestos por datos tanto personales como no personales, que lo hacen práctico para las empresas, incluidas las pymes.

[50] La Comisión ha prestado apoyo financiero a través de tres series de subvenciones por un total de 5 millones EUR, con las dos más recientes destinadas específicamente a apoyar a las autoridades nacionales de protección de datos en sus esfuerzos por llegar a los particulares y a las pymes: https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en. En 2020 se asignará 1 millón de euros adicionales.

[51] Con arreglo al artículo 28 del RGPD.

para la modernización de las cláusulas contractuales tipo para las transferencias internacionales[52].

Aplicación del RGPD a las nuevas tecnologías

Al haber sido concebido de manera tecnológicamente neutra, el RPGD se basa en principios y, por lo tanto, está diseñado para cubrir nuevas tecnologías a medida que estas vayan desarrollándose.

Es considerado como un instrumento esencial y flexible para garantizar que el desarrollo de nuevas tecnologías respete los derechos fundamentales. El marco normativo sobre protección de datos y privacidad demostró su importancia y flexibilidad durante la crisis de la COVID-19, especialmente en relación con el diseño de las aplicaciones de rastreo y otras soluciones tecnológicas para luchar contra la pandemia. En el futuro, se plantearán nuevos desafíos a la hora de ver cómo aplicar los principios probados a tecnologías específicas como la inteligencia artificial, la cadena de bloques, el internet de las cosas o el reconocimiento facial, que requieren un seguimiento continuo. El Libro Blanco de la Comisión sobre la Inteligencia Artificial[53], por ejemplo, impulsó un debate público sobre las circunstancias específicas —en caso de haberlas— que podrían justificar el uso de inteligencia artificial para fines de identificación biométrica remota (como el reconocimiento facial) en lugares públicos, y sobre salvaguardias comunes. A este respecto, las autoridades de protección de datos deben estar preparadas para llevar a cabo un seguimiento de los procesos de diseño técnico desde una fase temprana.

Por otra parte, una aplicación estricta y eficaz del RGPD con respecto a las grandes plataformas digitales y las empresas integradas, incluido en ámbitos como la publicidad en línea y la microsegmentación, es un elemento esencial para proteger a los particulares.

Desarrollo de un conjunto de instrumentos moderno para la transferencia internacional de datos

El RGPD ofrece un conjunto de instrumentos modernizado para facilitar la transferencia de datos personales desde la UE a un tercer país u organización internacional, garantizando al mismo tiempo que los datos sigan gozando de un elevado nivel de protección. En los dos últimos años, la Comisión ha intensificado su trabajo para aprovechar plenamente el potencial de los instrumentos disponibles en el marco del RGPD.

Parte de este trabajo ha consistido en la colaboración activa con socios clave a fin de alcanzar una «decisión de adecuación». El efecto de dicha decisión es permitir la circulación segura y libre de datos personales al tercer país de que se trate sin necesidad de que el exportador de datos ofrezca más garantías u obtenga una autorización. En particular, las decisiones de adecuación mutua UE-Japón, que entraron en vigor en febrero de 2019, han creado la mayor zona mundial de circulación libre y segura de datos. Además, el proceso de adecuación con la

[52] Con arreglo al artículo 46 del RGPD.
[53] Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza [COM(2020) 65 final].

República de Corea se encuentra en una fase avanzada y continúan las conversaciones exploratorias con otros socios importantes en Asia y América Latina.

La adecuación también desempeña un papel importante en el contexto de la futura relación con el Reino Unido, siempre que se cumplan las condiciones aplicables. Constituye un factor favorecedor del comercio, incluido el comercio digital, y un requisito previo esencial para una cooperación estrecha y ambiciosa en el ámbito de la seguridad y la aplicación de la ley. Además, un alto grado de convergencia en la protección de datos constituye un elemento importante para garantizar unas condiciones de competencia equitativas entre dos economías tan estrechamente integradas. En consonancia con la Declaración política sobre las relaciones futuras entre la UE y el Reino Unido, la Comisión está llevando a cabo una evaluación de adecuación tanto con arreglo al RGPD como a la Directiva sobre protección de datos[54].

Como parte de la primera evaluación del RGPD, la Comisión también está obligada a revisar las decisiones de adecuación adoptadas con arreglo a las anteriores normas[55]. Los servicios de la Comisión han entablado un intenso diálogo con cada uno de los 11 terceros países y territorios afectados[56] a fin de evaluar la manera en que han evolucionado sus sistemas de protección de datos desde la adopción de la decisión de adecuación y si se ajustan a los estándares fijados por el RGPD. La necesidad de garantizar la continuidad de estas decisiones como instrumento clave para el comercio y la cooperación internacional es uno de los factores que han llevado a varios de estos países y territorios a modernizar y reforzar su normativa en materia de privacidad. Se están debatiendo salvaguardias adicionales con algunos de estos países y territorios para abordar las diferencias pertinentes en materia de protección. No obstante, dado que el Tribunal de Justicia, en una sentencia que se espera para el 16 de julio, podría aportar aclaraciones potencialmente pertinentes para determinados elementos de la norma de adecuación, la Comisión informará por separado sobre la evaluación de las decisiones de adecuación existentes una vez que el Tribunal de Justicia haya dictado su sentencia en dicho asunto[57].

Además de su trabajo en materia de adecuación, la Comisión está llevando a cabo una modernización completa de las cláusulas contractuales tipo a fin de actualizarlas a la luz de los nuevos requisitos introducidos por el RGPD. El objetivo es reflejar mejor la realidad de las operaciones de tratamiento en la economía digital moderna y considerar la posible necesidad, en función también de la jurisprudencia que sentará

[54] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, p. 89).

[55] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

[56] Estos países y territorios son: Andorra, Argentina, Canadá, Guernsey, Islas Feroe, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay.

[57] Véase el asunto C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems («Schrems II»), relativo a una petición de decisión prejudicial sobre las conocidas como cláusulas contractuales tipo. Sin embargo, determinados elementos del estándar de adecuación pueden también ser objeto de más aclaraciones por parte del Tribunal.

próximamente el Tribunal de Justicia[58], de aclarar más determinadas garantías. Estas cláusulas representan, con mucho, el mecanismo de transferencia de datos más utilizado, al existir miles de empresas de la UE que dependen de ellas para ofrecer una amplia gama de servicios a sus clientes, proveedores, socios y empleados.

El Comité también ha desempeñado un papel activo en el desarrollo de los aspectos internacionales del RGPD. Esto incluye la actualización de las directrices sobre los mecanismos de transferencia existentes, tales como las normas corporativas vinculantes y las denominadas «excepciones», así como el desarrollo de la infraestructura jurídica para la utilización de los nuevos instrumentos introducidos por el RGPD, a saber, los códigos de conducta y certificación.

Para que las partes interesadas puedan hacer pleno uso del conjunto de instrumentos de transferencia del RGPD, es importante que el Comité intensifique sus trabajos en curso sobre los distintos mecanismos de transferencia, en particular mediante una mayor racionalización del proceso de aprobación de normas corporativas vinculantes, la finalización de las directrices sobre códigos de conducta y certificación como instrumentos para las transferencias, y la aclaración de la interacción entre las normas sobre transferencias internacionales de datos (capítulo V) y el ámbito de aplicación territorial del RGPD (artículo 3).

Otro aspecto importante de la dimensión internacional de las normas de protección de datos de la UE es el ámbito territorial ampliado del RGPD, que abarca también las actividades de tratamiento de los operadores extranjeros activos en el mercado de la UE. A fin de garantizar el cumplimiento efectivo del RGPD y unas condiciones de competencia verdaderamente equitativas, es esencial que esta ampliación se refleje adecuadamente en las medidas de aplicación de la normativa por parte de las autoridades de protección de datos. En particular, estas deben velar por la participación, en caso necesario, del representante en la UE del responsable o del encargado del tratamiento, y debe ser posible dirigirse a dicho representante además de —o en lugar de— a la empresa establecida fuera de la UE. Este enfoque debe seguirse más vigorosamente para que quede claro que la falta de establecimiento en la UE no exime a los operadores extranjeros de sus responsabilidades con arreglo al RGPD.

Promover la convergencia y la cooperación internacional en el ámbito de la protección de datos

El RGPD se ha convertido ya en un punto de referencia clave a nivel internacional y ha servido de catalizador para que muchos países del mundo consideren la adopción de normas de privacidad modernas. Esta tendencia hacia la convergencia mundial es un acontecimiento muy positivo que ofrece nuevas oportunidades para proteger más a las personas en la UE cuando sus datos se transfieren al extranjero, facilitando al mismo tiempo la circulación de los datos.

Aprovechando esta tendencia, la Comisión ha intensificado su diálogo en una serie de foros bilaterales, regionales y multilaterales a fin de fomentar una cultura mundial de respeto a la privacidad y desarrollar elementos de convergencia entre los distintos sistemas de protección de la privacidad. Al realizar estos esfuerzos, la Comisión se ha

[58] Véase el asunto «Schrems II».

basado —y seguirá haciéndolo— en el apoyo activo del Servicio Europeo de Acción Exterior, de la red de delegaciones de la UE en terceros países y de las misiones a organizaciones internacionales. Esto también ha permitido una mayor coherencia y complementariedad entre los distintos aspectos de la dimensión exterior de las políticas de la UE, desde el comercio hasta la nueva Asociación África-UE. El G-20 y el G-7 también han reconocido recientemente la contribución de la protección de datos a la confianza en la economía digital y la circulación de datos, en particular a través del concepto de «libre circulación de datos con confianza», propuesto por primera vez por la Presidencia japonesa del G-20[59]. La estrategia de datos pone de relieve la intención de la Comisión de seguir promoviendo el intercambio de datos con socios de confianza y luchar al mismo tiempo contra los abusos, como el acceso desproporcionado de los poderes públicos (extranjeros) a datos personales.

Al tiempo que promueve la convergencia de las normas de protección de datos a nivel internacional como forma de facilitar la circulación de datos y, con ello, el comercio, la Comisión también está decidida a abordar el proteccionismo digital, como se ha puesto de relieve recientemente en la Estrategia de datos[60]. Para ello, ha desarrollado disposiciones específicas sobre la circulación de datos y la protección de datos en los acuerdos comerciales[61], que presenta sistemáticamente en su negociaciones bilaterales —las más recientes de ellas con Australia, Nueva Zelanda y el Reino Unido— y multilaterales, como las actuales conversaciones sobre comercio electrónico en la OMC[62]. Estas disposiciones horizontales excluyen las restricciones injustificadas, como los requisitos de localización de datos obligatoria, al tiempo que mantienen la autonomía normativa de las partes para proteger el derecho fundamental a la protección de los datos.

Así pues, deben seguir examinándose las sinergias entre los instrumentos de comercio y los de protección de datos a fin de garantizar una circulación internacional libre y segura de aquellos datos que sean esenciales para las operaciones empresariales y la competitividad y el crecimiento de las empresas europeas —incluidas las pymes— en una economía cada vez más digitalizada.

Del mismo modo, es importante garantizar que, cuando se pida a las empresas activas en el mercado europeo que, a raíz de una solicitud legítima, compartan datos para permitir la aplicación de la ley, puedan hacerlo sin enfrentarse a conflictos normativos y respetando plenamente los derechos fundamentales de la UE. Con el fin de mejorar estas transferencias, la Comisión se ha comprometido a desarrollar marcos jurídicos adecuados con sus socios internacionales para evitar los conflictos normativos y apoyar las formas eficaces de cooperación, en particular estableciendo las garantías

---

[59] Véase, por ejemplo, la declaración de los dirigentes del G-20 en Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf

[60] Estrategia de datos, p. 23.

[61] Véase el texto de las disposiciones horizontales sobre los flujos transfronterizos de datos y la protección de los datos personales (en los acuerdos comerciales y de inversión de la UE): https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf

[62] En estos momentos, 84 miembros de la OMC están participando en las negociaciones multilaterales sobre comercio electrónico, a raíz de una declaración de iniciativa conjunta adoptada por ministros el 25 de enero de 2019 en Davos. Como parte de este proceso, la UE presentó su propuesta de texto sobre las futuras normas y obligaciones en materia de comercio electrónico el 3 de mayo de 2019. La propuesta incluye disposiciones horizontales sobre circulación de datos y protección de datos personales: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

necesarias en materia de protección de datos, contribuyendo así a una lucha más eficaz contra la delincuencia.

Por último, en un momento en que los problemas de observancia de las normas sobre privacidad o los incidentes relacionadas con la seguridad de los datos pueden afectar a un gran número de personas al mismo tiempo en varias jurisdicciones, debe seguir reforzándose la cooperación «sobre el terreno» entre los reguladores europeos e internacionales. En particular, esto requiere que se desarrollen instrumentos jurídicos adecuados para establecer formas más estrechas de cooperación y asistencia mutua, en particular permitiendo los intercambios de información necesarios en el contexto de las investigaciones. También con esta intención, la Comisión está creando una «Academia de Protección de Datos», una plataforma en la que las autoridades de protección de datos de la UE y de terceros países podrán compartir conocimientos, experiencias y mejores prácticas para facilitar y apoyar la cooperación entre las autoridades responsables de proteger la privacidad.

3 PERSPECTIVAS DE FUTURO

Para aprovechar plenamente el potencial del RGPD, es importante crear un enfoque armonizado y una cultura común europea de protección de datos, así como fomentar una gestión más eficaz y armonizada de los casos transfronterizos. Esto es lo que lo esperan los particulares y las empresas y constituye un objetivo esencial de la reforma de las normas de protección de datos de la UE. Es igualmente importante garantizar que todos los instrumentos disponibles en el RGPD se aprovechen al máximo para garantizar una aplicación eficaz a los particulares y a las empresas.

La Comisión continuará sus intercambios bilaterales con los Estados miembros sobre la aplicación del RGPD y, en caso necesario, seguirá utilizando todos los instrumentos a su disposición para fomentar el cumplimiento por parte de los Estados miembros de sus obligaciones en virtud del RGPD.

Dada la evaluación en curso de la legislación nacional, el breve período de experiencia práctica desde la entrada en vigor del RGPD y el hecho de que la legislación sectorial está aún siendo revisada en muchos Estados miembros, todavía es demasiado pronto para extraer conclusiones definitivas sobre el nivel actual de fragmentación. Por lo que se refiere al posible conflicto normativo debido a la aplicación de cláusulas de especificación por parte de los Estados miembros, es necesario, en primer lugar, comprender mejor las consecuencias para los responsables y los encargados del tratamiento[63].

Al realizar un seguimiento de estas cuestiones, la jurisprudencia pertinente de los tribunales nacionales y del Tribunal de Justicia contribuye a crear una interpretación coherente de las normas de protección de datos. Órganos jurisdiccionales nacionales han dictado recientemente sentencias que invalidan disposiciones de las legislaciones nacionales que contravienen el RGPD[64].

[63] Véanse la posición y las conclusiones del Consejo sobre la aplicación del RGPD.
[64] Así ha ocurrido en Alemania y en España o en Austria, donde se ha colmado una laguna en la legislación nacional.

Por lo que se refiere a la dimensión internacional, la Comisión seguirá centrándose en promover la convergencia de las normas de protección de datos como forma de garantizar la seguridad de la circulación de datos. Esto incluye diversas formas de trabajo «ascendente», por ejemplo en el contexto de las reformas en curso para la adopción de leyes de protección de datos nuevas o actualizadas, o la promoción del concepto de «libre circulación de datos con confianza» en los foros multilaterales. También abarca varios diálogos sobre adecuación y la modernización y ampliación de nuestro conjunto de instrumentos de transferencia mediante la actualización de las cláusulas contractuales tipo y el trabajo de preparación de los mecanismos de certificación. Este trabajo también incluye las negociaciones internacionales, como, por ejemplo, en el ámbito del acceso transfronterizo a las pruebas electrónicas a fin de garantizar que las transferencias de datos se produzcan con garantías adecuadas en materia de protección de datos. Por último, al entablar negociaciones sobre cooperación internacional y asistencia mutua entre los responsables de la protección de datos, la Comisión se esforzará por lograr la convergencia «entre las normas y la práctica».

Sobre la base de esta evaluación de la aplicación del RGPD desde mayo de 2018, se ha llegado a la conclusión de que las medidas que se enumeran a continuación son necesarias para apoyar su aplicación. La Comisión supervisará su aplicación, también con vistas al próximo informe de evaluación en 2024.

Aplicación y complemento del marco jurídico

Los Estados miembros deben

- completar la adaptación de sus legislaciones sectoriales al RGPD;
- considerar la posibilidad de limitar el uso de cláusulas de especificación que puedan generar fragmentación y poner en peligro la libre circulación de datos dentro de la UE;
- evaluar si la legislación nacional por la que se aplica el RGPD se encuentra en todas las circunstancias dentro de los márgenes previstos para la legislación de los Estados miembros.

La Comisión

- llevará a cabo intercambios bilaterales con los Estados miembros sobre la conformidad de la legislación nacional con el RGPD, en particular sobre la independencia y los recursos de las autoridades nacionales de protección de datos; utilizará todos los instrumentos a su disposición, incluidos los procedimientos de infracción, para garantizar que los Estados miembros cumplan el RGPD;
- apoyará la realización de más intercambios de puntos de vista y de prácticas nacionales entre los Estados miembros sobre asuntos que son objeto de una mayor especificación a nivel nacional a fin de reducir el nivel de fragmentación del mercado único, como el tratamiento de datos personales relativos a la salud y la investigación, o que deban ponderarse con otros derechos, como la libertad de expresión;

- apoyará una aplicación coherente del marco de protección de datos en relación con las nuevas tecnologías para apoyar la innovación y el desarrollo tecnológico;
- utilizará el grupo de expertos de los Estados miembros sobre el RGPD (establecido durante la fase transitoria anterior a la entrada en vigor del RGPD) para facilitar el debate y el intercambio de experiencias entre los Estados miembros y con la Comisión;
- estudiará si, a la luz de la experiencia y de la jurisprudencia pertinente que se vayan acumulando, podría ser conveniente proponer en el futuro modificaciones específicas de determinadas disposiciones del RGPD, en particular en relación con los registros de tratamiento por parte de las pymes que no tienen el tratamiento de datos personales como su actividad principal (bajo riesgo)[65], y la posible armonización de la edad de consentimiento de los niños en relación con los servicios de la sociedad de la información.

Aprovechar todo el potencial del nuevo sistema de gobernanza

Se invita al Comité y a las autoridades de protección de datos a

- elaborar acuerdos eficaces entre las autoridades de protección de datos en lo relativo al funcionamiento de los mecanismos de cooperación y coherencia, incluido en los aspectos procedimentales, basándose en la experiencia de sus miembros y reforzando la participación de su secretaría;
- apoyar la armonización en la aplicación y la ejecución del RGPD utilizando todos los medios a su alcance, en particular aclarando en mayor medida conceptos clave del RGPD y garantizando que las orientaciones nacionales se ajusten plenamente a las directrices adoptadas por el Comité;
- fomentar el uso de todos los instrumentos previstos en el RGPD para garantizar su aplicación coherente;
- intensificar la cooperación entre las autoridades de protección de datos mediante, por ejemplo, las investigaciones conjuntas.

La Comisión

- seguirá supervisando de cerca la independencia efectiva y plena de las autoridades nacionales de protección de datos;
- fomentará la cooperación entre los reguladores (en particular en ámbitos como la competencia, las comunicaciones electrónicas, la seguridad de las redes y los sistemas de información y la política de consumidores);
- apoyará la reflexión en el seno del Comité sobre los procedimientos aplicados por las autoridades nacionales de protección de datos con el fin de mejorar la cooperación en los casos transfronterizos.

Los Estados miembros

[65] Artículo 30, apartado 5, del RGPD.

- asignarán a las autoridades de protección de datos recursos suficientes para que estas desempeñen sus funciones.

Apoyo a las partes interesadas

Se invita al Comité y a las autoridades de protección de datos a

- adoptar más directrices prácticas, fácilmente comprensibles y que ofrezcan respuestas claras y eviten la ambigüedad en cuestiones relacionadas con la aplicación del RGPD, por ejemplo en cuanto al tratamiento de datos de los niños y los derechos de los titulares de los datos, incluido el ejercicio del derecho de acceso y el derecho de supresión, consultando a las partes interesadas en el proceso;
- revisar las directrices cuando sean necesarias aclaraciones adicionales en vista de la experiencia adquirida y de la evolución de la situación, incluida la jurisprudencia del Tribunal de Justicia;
- desarrollar instrumentos prácticos, como formularios armonizados para la violación de la seguridad de los datos y registros simplificados de las actividades de tratamiento, para ayudar a las pymes de bajo riesgo a que cumplan sus obligaciones.

La Comisión

- proporcionará cláusulas contractuales tipo tanto para las transferencias internacionales como para las relaciones entre los responsables y los encargados del tratamiento;
- proporcionará instrumentos para aclarar o apoyar la aplicación de las normas de protección de datos a los niños[66];
- estudiará, en consonancia con la estrategia de datos, los medios prácticos para facilitar una mayor utilización del derecho a la portabilidad por parte de los particulares, por ejemplo dándoles un mayor control sobre quién puede acceder a los datos generados por máquinas y utilizarlos;
- apoyará la normalización/certificación, en particular en aspectos relativos a la ciberseguridad, mediante la cooperación entre la Agencia de la Unión Europea para la Ciberseguridad (ENISA), las autoridades de protección de datos y el Comité;
- hará uso, cuando proceda, de su derecho a solicitar al Comité que elabore directrices y dictámenes sobre cuestiones específicas de importancia para las partes interesadas;
- ofrecerá orientación cuando sea necesario, respetando plenamente la función del Comité;

[66] Proyecto de la Comisión sobre instrumentos de determinación de la edad: proyecto piloto para demostrar una infraestructura técnica interoperable de protección de la infancia, incluida la verificación de la edad y el consentimiento parental. Se espera que esto apoye la aplicación de los mecanismos de protección de la infancia basados en la legislación vigente pertinente de la UE para la protección en línea de la infancia.

- apoyará las actividades de las autoridades de protección de datos que faciliten la aplicación de las obligaciones del RGPD por parte de las pymes mediante el apoyo financiero, especialmente para la orientación práctica y los instrumentos digitales que puedan reproducirse en otros Estados miembros.

Incentivos a la innovación

La Comisión

- supervisará la aplicación del RGPD a las nuevas tecnologías, teniendo también en cuenta posibles iniciativas futuras en el ámbito de la inteligencia artificial y en el marco de la estrategia de datos;
- fomentará, también a través del apoyo financiero, la elaboración de códigos de conducta de la UE en el ámbito de la salud y la investigación;
- seguirá de cerca el desarrollo y la utilización de aplicaciones en el contexto de la pandemia de COVID-19.

Se invita al Comité a

- elaborar directrices sobre la aplicación del RGPD en los ámbitos de la investigación científica, la inteligencia artificial, la cadena de bloques y otros posibles avances tecnológicos;
- revisar las directrices cuando sean necesarias aclaraciones adicionales en vista de los avances tecnológicos.

Continuar el desarrollo del conjunto de instrumentos para las transferencias de datos

La Comisión

- mantendrá diálogos en materia de adecuación con los terceros países interesados, en consonancia con la estrategia establecida en su Comunicación de 2017 titulada «Intercambio y protección de los datos personales en un mundo globalizado», incluida, cuando sea posible, la transferencia de datos a las autoridades encargadas de hacer cumplir las leyes penales (con arreglo a la Directiva sobre protección de datos en el ámbito penal) y a otras autoridades públicas; esto incluye la finalización del proceso de adecuación con la República de Corea lo antes posible;
- finalizará la evaluación en curso de las decisiones de adecuación existentes e informará al Parlamento Europeo y al Consejo;
- concluirá los trabajos sobre la modernización de las cláusulas contractuales tipo con vistas a su actualización a la luz del RGPD, a abarcar todas las hipótesis de transferencia pertinentes y a reflejar mejor las prácticas empresariales modernas.

Se invita al Comité a

- aclarar más la interacción entre las normas sobre transferencias internacionales de datos (capítulo V) y el ámbito de aplicación territorial del RGPD (artículo 3);

- garantizar el cumplimiento efectivo de las normas por parte de los operadores establecidos en terceros países que entran en el ámbito territorial de aplicación del RGPD, también, cuando proceda, en lo que se refiere a la designación de un representante (artículo 27);
- racionalizar la evaluación y la eventual aprobación de normas corporativas vinculantes con vistas a acelerar el proceso;
- completar el trabajo sobre la arquitectura, los procedimientos y los criterios de evaluación de los códigos de conducta y los mecanismos de certificación como instrumentos para las transferencias de datos.

Promover la convergencia y desarrollar la cooperación internacional

La Comisión

- 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 mejores prácticas;
- colaborará con los socios africanos para promover la convergencia normativa y apoyar el desarrollo de capacidades de las autoridades de supervisión en el marco del capítulo digital de la nueva Asociación África-UE;
- evaluará las formas en que podría facilitarse la cooperación entre los operadores privados y las autoridades encargadas de hacer cumplir la ley, en particular mediante la negociación de marcos bilaterales y multilaterales para las transferencias de datos en el contexto del acceso de las autoridades extranjeras encargadas de hacer cumplir la ley a las pruebas electrónicas a fin de evitar conflictos normativos, velando al mismo tiempo por la aplicación de garantías adecuadas en materia de protección de datos;
- colaborará con organizaciones internacionales y regionales como la OCDE, la ASEAN o el G-20 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»;
- creará una «Academia de Protección de Datos» para facilitar y apoyar los intercambios entre reguladores europeos e internacionales;
- promoverá la cooperación internacional en materia de cumplimiento de la normativa entre las autoridades de supervisión, incluido mediante la negociación de acuerdos de cooperación y asistencia mutua.