COMISIÓN
EUROPEA

Bruselas, 24.7.2019
COM(2019) 374 final

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

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

I. Introducción

El Reglamento general de protección de datos[1] (en lo sucesivo, «el Reglamento») se aplica en toda la Unión Europea desde hace más de un año. Ocupa el lugar central de un panorama de protección de datos en la UE coherente y modernizado que también incluye la Directiva sobre protección de datos en el ámbito policial y judicial[2] y el Reglamento de protección de datos para las instituciones y órganos de la UE[3]. Este marco se completará con el Reglamento sobre la privacidad y las comunicaciones electrónicas, actualmente en proceso legislativo.

Resulta fundamental disponer de unas normas de protección de datos sólidas para garantizar el derecho fundamental a la protección de los datos personales. Son indispensables para una sociedad democrática[4] y un componente importante de una economía cada vez más impulsada por los datos. La UE aspira a aprovechar las numerosas oportunidades que brinda la transformación digital en términos de servicios, puestos de trabajo e innovación al tiempo que aborda los desafíos que estas plantean. Usurpación de identidad, filtración de datos sensibles, discriminación de personas, sesgos sistemáticos, intercambio de contenidos ilícitos y desarrollo de herramientas de vigilancia intrusiva son solo algunos ejemplos de los problemas que cada vez con mayor frecuencia ocupan el debate público y frente a los cuales los ciudadanos esperan obviamente que sus datos estén protegidos.

La protección de datos se ha convertido en un fenómeno verdaderamente global a medida que las personas de todo el mundo conceden mayor valor y estima a la protección y seguridad de sus datos. Muchos países han adoptado normas de protección de datos exhaustivas basadas en

---

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO L 119 de 4.5.2016, p. 1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[2] 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). https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex:32016L0680. Los Estados miembros debían transponer la Directiva el 6 de mayo de 2018 a más tardar. Los informes de la Unión de la Seguridad exponen en qué situación se encuentra su transposición.

[3] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32018R1725. Entró en vigor el 11 de diciembre de 2018.

[4] El Tribunal Supremo de la India, en una sentencia histórica de 24 de agosto de 2017, reconoció la privacidad como un derecho fundamental, una «faceta esencial de la dignidad del ser humano».

principios similares a los contemplados en el Reglamento o en están en vías de hacerlo, lo que supone una convergencia mundial de las normas de protección de datos. Esta situación ofrece nuevas oportunidades para facilitar los flujos de datos, entre operadores comerciales o autoridades públicas, al tiempo que se mejora el nivel de protección de los datos personales en la UE y en todo el planeta.

Nunca antes se había tomado tan en serio la protección de datos, lo que tiene un gran impacto sobre los distintos sectores y partes interesadas. La Comisión está decidida a conducir a la UE a una aplicación satisfactoria del nuevo régimen de protección de datos y a prestar su ayuda para que todos sus aspectos sean plenamente operativos. Con la presente Comunicación, la Comisión hace balance de los resultados conseguidos hasta la fecha por lo que respecta a la aplicación coherente de las normas de protección de datos en toda la UE, el funcionamiento del nuevo sistema de gobernanza, el impacto para los ciudadanos y las empresas, así como los esfuerzos de la UE para promover la convergencia mundial de los regímenes de protección de datos. Da seguimiento a la Comunicación de la Comisión sobre la aplicación del Reglamento, de enero de 2018[5], y para su elaboración se ha tenido en cuenta la labor del Grupo multilateral[6], en particular su contribución al ejercicio de balance del primer año de aplicación del Reglamento, así como los debates mantenidos durante el acto de balance organizado por la Comisión el 13 de junio de 2019[7]. Asimismo, la presente Comunicación es una contribución a la revisión prevista por la Comisión para mayo de 2020[8].

El marco legislativo de protección de datos de la UE es uno de los pilares del enfoque europeo de la innovación centrado en el ser humano. Se está convirtiendo en la base reglamentaria de un abanico cada vez mayor de políticas, como, por ejemplo, la salud y la investigación, la inteligencia artificial, el transporte, la energía, la competencia y la aplicación de la ley. La Comisión ha hecho hincapié sistemáticamente en la importancia de aplicar y hacer cumplir adecuadamente las nuevas normas de protección de datos, como destacó en su Comunicación sobre la aplicación del Reglamento, publicada en enero de 2018 y en sus Orientaciones sobre el uso de datos personales en el contexto electoral, publicadas en septiembre de 2018[9]. En el momento de elaborar la presente Comunicación son numerosos los avances realizados en la consecución de este objetivo, aunque huelga decir que es necesario seguir trabajando para que el Reglamento sea plenamente operativo.

---

[5] Comunicación de la Comisión al Parlamento Europeo y al Consejo «Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento general de protección de datos a partir del 25 de mayo de 2018», COM(2018) 43 final: https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

[6] El Grupo multilateral sobre el Reglamento creado por la Comisión lo componen representantes de la sociedad civil y del sector empresarial, representantes del mundo académico y profesionales. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

[7] http://europa.eu/rapid/press-release_IP-19-2956_en.htm.

[8] Artículo 97 del Reglamento.

[9] «Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral», COM(2018) 638 final: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_es.pdf.

II. Un continente, una ley: el marco de protección de datos está instaurado en los Estados miembros

Uno de los objetivos fundamentales del Reglamento era acabar con un panorama fragmentado de veintiocho legislaciones nacionales distintas que existían en virtud de la anterior Directiva de protección de datos[10] y proporcionar seguridad jurídica a los particulares y a las empresas en toda la UE, objetivo cumplido en gran medida.

La armonización del marco jurídico

Aunque el Reglamento es directamente aplicable en los Estados miembros, les obligaba a adoptar una serie de medidas legales a escala nacional, en particular instituir y dotar de competencias a las autoridades nacionales de protección de datos[11], establecer normas sobre cuestiones específicas, como la conciliación de la protección de los datos personales con la libertad de expresión e información, y modificar o derogar la legislación sectorial con aspectos relativos a la protección de datos. En el momento de redactar la presente Comunicación, todos los Estados miembros salvo tres[12] habían actualizado su legislación nacional general de protección de datos. Se sigue trabajando a nivel nacional para adaptar las disposiciones legislativas sectoriales. A raíz de su adhesión al Acuerdo sobre el Espacio Económico Europeo, la aplicación del Reglamento se amplió a Noruega, Islandia y Liechtenstein, que también han adoptado su legislación nacional de protección de datos.

Con todo, las partes interesadas demandan un grado de armonización más elevado si cabe en algunos ámbitos[13]. Efectivamente, el Reglamento concede a los Estados miembros cierto margen para especificar con mayor detalle su aplicación en determinados ámbitos, como la edad de consentimiento de los menores para los servicios en línea[14] o el tratamiento de datos personales en áreas tales como las de la medicina y la salud pública. En este caso, la actuación de los Estados miembros está condicionada por dos aspectos:

i) toda legislación nacional de especificación debe respetar los requisitos de la Carta de los Derechos Fundamentales[15] (y no sobrepasar los límites fijados por el Reglamento, sustentado en la Carta);
ii) no debe contravenir la libre circulación de datos personales dentro de la UE[16].

---

[10] 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. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046.

[11] Como la competencia para imponer sanciones administrativas.

[12] A fecha de 23 de julio de 2019, Eslovenia, Grecia y Portugal siguen en proceso de adopción de su legislación nacional.

[13] Véase el informe del Grupo multilateral sobre el Reglamento publicado el 13 de junio de 2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

[14] Trece años en el caso de Bélgica, Dinamarca, Estonia, Finlandia, Letonia, Malta, Reino Unido y Suecia; Catorce en el de Austria, Bulgaria, Chipre, España, Italia y Lituania; Quince en el de Chequia y Francia; Dieciséis por lo que se refiere a Alemania, Croacia, Hungría, Eslovaquia, Irlanda, Luxemburgo, Países Bajos, Polonia y Rumanía.

[15] Artículo 8.

[16] En consonancia con el artículo 16, apartado 2, del Tratado de Funcionamiento de la Unión Europea.

En algunas ocasiones, los Estados miembros han introducido requisitos nacionales adicionales al Reglamento, concretamente a través de numerosas leyes sectoriales, lo que se traduce en fragmentación y se materializa en la creación de cargas innecesarias. Un ejemplo de requisito adicional introducido por un Estado miembro, además de las disposiciones del Reglamento, es la obligación recogida por la legislación alemana de nombrar un delegado de protección de datos en las empresas con veinte empleados o más que participe permanentemente en el tratamiento automatizado de datos personales.

Esfuerzos sostenidos en pro de una mayor armonización

La Comisión participa en diálogos bilaterales con las autoridades nacionales en los que presta especial atención a las medidas nacionales respecto a los siguientes aspectos:

- la independencia efectiva de las autoridades de protección de datos, incluidos los recursos financieros, humanos y técnicos adecuados;
- la manera en que las leyes nacionales limitan los derechos de los interesados;
- que la legislación nacional no introduzca requisitos que vayan más allá de lo dispuesto en el Reglamento cuando no haya margen de especificación, como, por ejemplo, condiciones adicionales para el tratamiento;
- el cumplimiento de la obligación de conciliar el derecho a la protección de los datos personales con la libertad de expresión e información, teniendo en cuenta que no se debe abusar de esta obligación para crear un efecto paralizador en la labor periodística.

El trabajo de las autoridades de protección de datos, cooperando en el contexto del Comité Europeo de Protección de Datos («el Comité»), es un factor clave para impulsar una aplicación coherente de las nuevas normas: las medidas de ejecución que afecten a varios Estados miembros pasan por el mecanismo de cooperación y coherencia[17] dentro del Comité y las directrices adoptadas por este contribuyen a una comprensión armonizada del Reglamento. No obstante, existe una expectativa en las partes interesadas de que las autoridades de protección de datos sigan avanzando en esta dirección.

El trabajo de los órganos jurisdiccionales nacionales y del Tribunal de Justicia de la Unión Europea también está ayudando a crear una interpretación coherente de las normas de protección de datos. Dichos órganos han dictado recientemente sentencias que invalidan disposiciones de las legislaciones nacionales que contravienen el Reglamento[18].

III. Todas las piezas del nuevo sistema de gobernanza comienzan a encajar

El Reglamento creó una nueva estructura de gobernanza, colocando en su centro a las autoridades nacionales de protección de datos independientes como garantes del

[17] El artículo 60 del Reglamento prevé que las autoridades de protección de datos cooperen para aplicar una única interpretación del Reglamento en casos concretos. El artículo 64 contempla que el Comité emita dictámenes en determinados casos a fin de garantizar la aplicación coherente del Reglamento. Por último, se otorga al Comité la facultad de adoptar decisiones vinculantes destinadas a las autoridades de protección de datos en caso de discrepancias entre ellas.

[18] Este ha sido el caso de Alemania y España.

cumplimiento del Reglamento y primer punto de contacto para las partes interesadas. Aunque la mayor parte de las autoridades de protección de datos se han beneficiado en el último año de un aumento de los recursos, sigue habiendo grandes diferencias entre los Estados miembros[19].

Las autoridades de protección de datos utilizan sus nuevos poderes

El Reglamento dota a las autoridades de protección de datos de mayores poderes de ejecución. Contrariamente a los temores manifestados por algunas partes interesadas antes de mayo de 2018, las autoridades nacionales de protección de datos han adoptado un enfoque equilibrado respecto a los poderes de ejecución. Se han centrado en el diálogo más que en las sanciones, especialmente en el caso de los operadores de menor tamaño cuya actividad principal no es el tratamiento de datos. Al mismo tiempo, no han dudado en utilizar sus nuevos poderes con eficacia siempre que ha sido necesario, incluso abriendo investigaciones en el ámbito de las redes sociales[20] e imponiendo multas administrativas cuya cuantía oscilaba entre unos pocos miles de euros y varios millones, en función de la gravedad de las vulneraciones de las normas de protección de datos.

Ejemplos de sanciones impuestas por las autoridades de protección de datos[21]:

- 5 000 EUR a un café de apuestas deportivas en Austria, por video vigilancia ilícita;
- 220 000 EUR a una empresa intermediaria de datos en Polonia, por no informar a los particulares de que se estaban tratando sus datos;
- 250 000 EUR a la liga española de fútbol, LaLiga, por falta de transparencia en el diseño de su aplicación para teléfonos móviles;
- 50 millones EUR a Google en Francia, por las condiciones para obtener el consentimiento de los usuarios.

Durante el desarrollo de las investigaciones, resulta fundamental que las autoridades de protección de datos reúnan las pruebas pertinentes, respeten todas las etapas procesales establecidas en la legislación nacional y garanticen la tutela judicial efectiva en expedientes que suelen ser complejos. Esto requiere tiempo y conlleva un volumen de trabajo considerable, lo que explica por qué la mayoría de las investigaciones abiertas después de que el Reglamento empezase a aplicarse aún no se han concluido.

Con todo, el éxito del Reglamento no debería medirse por el número de sanciones impuestas, sino por los cambios conseguidos en la cultura y el comportamiento de todos los actores involucrados. En este contexto, las autoridades de protección de datos disponen de otras herramientas, como, por ejemplo, la imposición de una limitación temporal o definitiva del

[19] https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

[20] Por ejemplo, la Comisión irlandesa de protección de datos abrió 15 investigaciones formales en relación con el cumplimiento del Reglamento por parte de las empresas tecnológicas multinacionales. Véase la página 49 del informe anual de 2018 de la Comisión irlandesa de protección de datos: https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

[21] Varias decisiones por las que se imponen sanciones siguen sujetas a revisión judicial.

tratamiento, incluida su prohibición, o la suspensión de los flujos de datos hacia un destinatario situado en un tercer país[22].

Algunas autoridades de protección de datos han creado instrumentos nuevos, tales como líneas de ayuda y herramientas para las empresas, mientras que otras han desarrollado enfoques novedosos, por ejemplo, entornos reglamentarios de prueba[23] para ayudar a las empresas en sus esfuerzos de cumplimiento. Sin embargo, diversas partes interesadas siguen pensando que no han recibido apoyo e información suficientes, especialmente las pequeñas y medianas empresas de algunos Estados miembros[24]. Para ayudar a remediar esta situación, la Comisión concede subvenciones a las autoridades de protección de datos para que realicen actividades de divulgación entre las partes interesadas, especialmente los particulares y las pymes[25].

El Comité Europeo de Protección de Datos está operativo

Las autoridades de protección de datos han intensificado su trabajo en el Comité Europeo de Protección de Datos[26]. Este intenso trabajo ha permitido que el Comité adopte cerca de veinte directrices sobre aspectos clave del Reglamento[27]. Los futuros ámbitos de actividad del Comité se presentan en un programa de dos años[28], tal como exige el Reglamento.

En los casos transfronterizos, cada una de las autoridades de protección de datos ya no es meramente una autoridad nacional, sino que participa en un proceso de alcance verdaderamente europeo en todas las etapas, desde la investigación hasta que la toma de la decisión. Esta estrecha colaboración se ha convertido en una práctica cotidiana: hasta finales de junio de 2019 se habían gestionado 516 casos transfronterizos a través del mecanismo de cooperación.

La Comisión contribuye activamente al trabajo del Comité[29] para promover la letra y el espíritu del Reglamento y recuerda los principios generales del Derecho de la UE[30].

Hacia la creación de una cultura de protección de datos de la UE

---

[22] Artículo 58, apartado 2, letras f) y j).

[23] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/.

[24] Véase el informe del Grupo multilateral sobre el Reglamento RGPD: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.

[25] 2 millones EUR asignados a nueve autoridades de protección de datos en 2018 para actividades en 2018-2019: Bélgica, Bulgaria, Dinamarca, Eslovenia, Hungría, Islandia Lituania, Letonia y Países Bajos: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
1 millón EUR por asignar en 2019: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

[26] El Comité está dotado de personalidad jurídica y lo integran los directores de las autoridades nacionales de control en materia de protección de datos y el Supervisor Europeo de Protección de Datos.

[27] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_es.

[28] https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_es.

[29] En calidad de participante sin derecho a voto.

[30] Asimismo, la Comisión ha ayudado a que la constitución del Comité sea fluida y apoya su funcionamiento aportando su sistema de comunicación.

El nuevo sistema de gobernanza aún tiene que explotar todo su potencial. Es importante que el Comité racionalice más aun su toma de decisiones y desarrolle entre sus miembros una cultura de protección de datos de la UE común. Las posibilidades para que las autoridades de protección de datos pongan en común sus esfuerzos[31] en cuestiones que afectan a más de un Estado miembro, por ejemplo, para llevar a cabo investigaciones y medidas de ejecución conjuntas, pueden contribuir a este objetivo al tiempo que se mitigan las limitaciones en cuanto a recursos.

Numerosas partes interesadas desean ver una cooperación mayor si cabe y un enfoque uniforme por parte de las autoridades nacionales de protección de datos[32]. Asimismo, piden que el asesoramiento facilitado por las autoridades de protección de datos sea más coherente[33] y que las directrices nacionales estén perfectamente armonizadas con las del Comité. Algunas de ellas también esperan que se precise más detalladamente conceptos clave del Reglamento como el enfoque basado en riesgos, teniendo en cuenta especialmente las inquietudes de las pymes sobre todo.

En este contexto, resulta fundamental permitir una mejor contribución de las partes interesadas al trabajo del Comité. Este es el motivo de que la Comisión acoja con satisfacción la consulta pública sistemática organizada por el Comité sobre directrices. Esta práctica, junto con la organización de talleres con las partes interesadas sobre temas específicos en una fase temprana de la reflexión, debería proseguir y ampliarse para garantizar la transparencia, el carácter inclusivo y la pertinencia del trabajo del Comité.

IV. Los particulares ejercen sus derechos, pero la sensibilización debería continuar

Otro objetivo clave del Reglamento era reforzar los derechos de las personas. La mayoría de las asociaciones de derechos civiles y organizaciones de consumidores consideran que el Reglamento ha supuesto una importante contribución a una sociedad digital justa basada en la confianza mutua.

Un conocimiento más profundo de los derechos en materia de protección de datos

La personas de la UE son cada vez más conscientes de las normas de protección de datos y de sus derechos: el 67 % de los participantes en un Eurobarómetro de mayo de 2019[34] conocen el Reglamento y el 57 % saben de la existencia de una autoridad nacional de protección de datos a la que pueden acudir para informarse o presentar reclamaciones. El 73 % ha oído hablar de al menos uno de los derechos reconocidos por el Reglamento. Sin embargo, un número

[31] Artículo 62 del Reglamento.
[32] Véase el informe del Grupo multilateral sobre el Reglamento: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. Por ejemplo, las empresas creen que las listas nacionales de los tipos de operaciones de tratamiento que requieren una evaluación de impacto relativa a la protección de datos en virtud del artículo 35 el Reglamento podrían haberse armonizado mejor.
[33] También entre las diversas autoridades de los Estados federales.
[34] http://europa.eu/rapid/press-release_IP-19-2956_es.htm.

significativo de personas en la UE siguen sin tomar medidas activas para proteger sus datos personales cuando acceden a internet. Por ejemplo, el 44 % de las personas no han cambiado sus ajustes de privacidad por defecto en las redes sociales.

Las personas ejercen sus derechos cada vez más

Este mayor conocimiento de los derechos ha hecho que las personas los ejerzan cada vez más a través de consultas de los clientes y recurriendo con mayor frecuencia a las autoridades de protección de datos para solicitar información o presentar reclamaciones[35]. Asimismo, las empresas indican que las solicitudes de acceso a datos personales han aumentado en varios sectores, como el de la banca y las telecomunicaciones. También ha aumentado la frecuencia con la que las personas retiran su consentimiento y ejercen su derecho a oponerse a las comunicaciones comerciales[36].

No obstante, algunos operadores han comunicado la existencia de malentendidos por parte de los particulares en cuanto a las normas de protección de datos, como la creencia de que los particulares deben consentir todo tratamiento o que el derecho a la supresión es absoluto (mientras que, por ejemplo, en ocasiones los datos personales han de conservarse debido a obligaciones legales)[37]. Por su parte, las organizaciones de la sociedad civil se quejan de que algunas empresas y autoridades de protección de datos tardan mucho en responder.

Otro aspecto importante es que las organizaciones no gubernamentales, tras recibir el mandato de particulares, pusieron en marcha varias acciones representativas, haciendo uso de una nueva posibilidad recogida en el Reglamento[38]. El recurso a acciones representativas habría sido más fácil si un número mayor de Estados miembros hubiese utilizado la posibilidad prevista en el Reglamento de permitir que las organizaciones no gubernamentales emprendan acciones sin un mandato[39].

Necesidad de mantener las medidas de concienciación

El diálogo y las medidas de concienciación dirigidas al público en general, por consiguiente, deben continuar a escala nacional y de la UE. Para ello, en julio de 2019 la Comisión puso en marcha una nueva campaña en línea[40] para animar a las personas a leer las declaraciones de privacidad y optimizar sus ajustes de privacidad.

V. Las empresas están adaptando sus prácticas

El Reglamento pretende apoyar a las empresas en la economía digital ofreciendo soluciones con garantía de futuro. En líneas generales, las empresas han acogido favorablemente el

[35] https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf.
[36] Véase el informe del Grupo multilateral sobre el Reglamento general de protección de datos.
[37] Véase el informe del Grupo multilateral sobre el Reglamento general de protección de datos.
[38] Artículo 80, apartado 1, del Reglamento.
[39] Artículo 80, apartado 2, del Reglamento.
[40] Es la sucesora de una campaña anterior destinada a divulgar materiales informativos para particulares y empresas disponible en: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_es.

principio de responsabilidad proactiva, alejado del oneroso enfoque *ex ante* aplicado anteriormente (eliminación de requisitos de notificación, escalabilidad de las obligaciones y flexibilidad del principio de protección de datos desde el diseño y por defecto, permitiendo la competencia sobre la base de soluciones respetuosas con la privacidad). Al mismo tiempo, algunas piden mayor seguridad jurídica y directrices adicionales o más claras de las autoridades de protección de datos[41].

Una gestión correcta de los datos

Aunque las empresas han manifestado que el ajuste a las nuevas normas planteaba una serie de desafíos[42], muchas de ellas ponen de relieve que también les brindó la oportunidad de llevar la cuestión de la protección de datos a los consejos de administración, organizarse en cuanto a los datos que obran en su poder, mejorar la seguridad, estar mejor preparadas para los incidentes, reducir la exposición a riesgos innecesarios y establecer relaciones de mayor confianza con sus clientes y socios comerciales. Por lo que respecta a la transparencia, las organizaciones empresariales y de la sociedad civil mencionan el delicado equilibrio que se ha de alcanzar entre facilitar a las personas toda la información necesaria en virtud del Reglamento al tiempo que se utiliza un lenguaje claro y sencillo y una forma que estas puedan entender. Los operadores están desarrollando soluciones innovadoras en este sentido.

En términos generales, las empresas indicaron que eran capaces de aplicar los nuevos derechos de los interesados, aunque en ocasiones resultaba difícil cumplir los plazos por el aumento del número de solicitudes y su naturaleza más amplia[43] o comprobar la identidad del solicitante.

Impacto sobre la innovación

El Reglamento no solo permite, sino que promueve, el desarrollo de nuevas tecnologías al tiempo que se respeta el derecho fundamental a la protección de los datos personales. Este es el caso en ámbitos como el de la inteligencia artificial.

Las empresas han empezado a desarrollar su oferta de servicios nuevos y más respetuosos con la privacidad. Por ejemplo, los motores de búsqueda que no realizan un seguimiento de los usuarios o utilizan publicidad comportamental están ganando progresivamente cuota de mercado en algunos Estados miembros. Otras empresas están desarrollando servicios que se basan en los nuevos derechos concedidos a los particulares, como por ejemplo la portabilidad de sus datos personales. Un número cada vez mayor de empresas han promocionado el respeto de los datos personales como factor competitivo diferenciador y argumento de venta.

[41] Véase el informe del Grupo multilateral sobre el Reglamento.

[42] A menudo se menciona la actualización del sistema informático como uno de los principales desafíos, especialmente por lo que respecta a la aplicación de los principios de protección de datos desde el diseño y por defecto, el derecho de supresión en copias de seguridad, etc.

[43] Las empresas también piden al Comité directrices sobre las solicitudes infundadas o excesivas.

Esta evolución no se limita a la UE, sino que también concierne a economías extranjeras muy innovadoras[44].

La situación específica de las microempresas y pequeñas empresas «de bajo riesgo»

Aunque la situación varía de un Estado miembro a otro, las microempresas y las pequeñas empresas[45] que no tratan datos personales como actividad principal figuran entre las partes interesadas con más dudas sobre la aplicación del Reglamento. Aunque esta situación parece deberse en parte al desconocimiento de las normas de protección de datos, en ocasiones sus inquietudes también están exacerbadas por campañas de consultoras que intentan ofrecer asesoramiento de pago, por la difusión de información incorrecta, por ejemplo, sobre la necesidad de obtener sistemáticamente el consentimiento de las personas[46], y por los requisitos adicionales impuestos a nivel nacional.

En este contexto, las microempresas y las pequeñas empresas piden directrices adaptadas a su situación específica y que proporcionen información muy práctica. Algunas autoridades de protección de datos ya lo han hecho a nivel nacional[47]. Como complemento a las iniciativas nacionales, la Comisión ha publicado material informativo para ayudar a estas empresas a cumplir las nuevas normas a través de una serie de pasos prácticos[48].

Utilización del conjunto de herramientas previsto por el Reglamento

El Reglamento contempla una serie de herramientas para demostrar el cumplimiento, como las cláusulas contractuales tipo, los códigos de conducta y los mecanismos de certificación introducidos por primera vez.

Las cláusulas contractuales tipo son cláusulas modelo que se pueden incluir voluntariamente en un contrato, por ejemplo, entre un responsable del tratamiento de datos y un encargado del tratamiento, y que establecen las obligaciones de las partes contratantes en virtud del Reglamento. El Reglamento amplía las posibilidades de utilizar cláusulas contractuales tipo tanto para las transferencias internacionales como dentro de la UE[49]. En el ámbito de las transferencias internacionales, el amplio uso que se hace de ellas indica[50] que son de gran utilidad para las empresas en sus esfuerzos de cumplimiento y especialmente ventajosas para

[44] Por ejemplo, según un informe publicado por la asociación de la industria de ciberseguridad de Israel, en 2018 el subsector de la protección de datos y la privacidad dentro de la ciberseguridad fue el sector que más rápido creció, en parte como consecuencia de la entrada en vigor del RGPD.

[45] Conforme a la definición de pyme disponible en: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_es.

[46] De hecho, el Reglamento no solo recurre al consentimiento, sino que contempla varios motivos lícitos para el tratamiento de datos personales.

[47] Por ejemplo, la guía elaborada por la autoridad de protección de datos francesa: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

[48] https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-es-n_0.pdf.

[49] Véase el artículo 28 del Reglamento. Las cláusulas contractuales tipo adoptadas por la Comisión gozan de validez en toda la UE. Por el contrario, las adoptadas por una autoridad de protección de datos en virtud del artículo 28, apartado 8, solo vinculan a la autoridad que las adoptó y, por ende, pueden utilizarse como cláusulas contractuales tipo para operaciones de tratamiento que se enmarquen en la jurisdicción de dicha autoridad, de conformidad con los artículos 55 y 56.

[50] De hecho, son la principal herramienta a la que recurren las empresas para sus exportaciones de datos.

las empresas que carecen de los recursos para negociar contratos individuales con cada uno de sus contratistas encargados del tratamiento de datos.

Son varios los sectores que también consideran la adopción de cláusulas contractuales tipo una vía útil para fomentar la armonización, especialmente cuando es la Comisión quien las adopta. La Comisión trabajará en colaboración con las partes interesadas para hacer uso de las opciones que prevé el Reglamento y actualizar las cláusulas existentes.

La adhesión a códigos de conducta es otra herramienta operativa y práctica a disposición de la industria para facilitar la demostración del cumplimiento del Reglamento[51]. Dichos códigos deben ser desarrollados por asociaciones empresariales u organismos que representen a categorías de responsables y encargados del tratamiento y deben describir de qué forma se pueden aplicar las normas de protección de datos en un sector específico. Al alinear las obligaciones con los riesgos[52], también pueden resultar ser una forma muy útil y rentable para que las pequeñas y medianas empresas cumplan sus obligaciones.

Por último, la certificación también puede ser un instrumento útil para demostrar el cumplimiento de requisitos específicos del Reglamento. Puede aumentar la seguridad jurídica para las empresas y promover el Reglamento mundialmente. Las Directrices sobre certificación y acreditación[53] adoptadas recientemente por el Comité Europeo de Protección de Dato permitirán el desarrollo de regímenes de certificación en la UE. La Comisión realizará un seguimiento de dicho desarrollo y, si procede, hará uso de las competencias que le confiere el Reglamento para encuadrar los requisitos para la certificación. Asimismo, la Comisión podrá emitir una solicitud de normalización destinada a los organismos de certificación de la UE sobre elementos pertinentes para el Reglamento.

VI. La convergencia al alza avanza a nivel internacional

La demanda de protección de los datos personales no se limita a la UE. Como muestra una encuesta global sobre seguridad en internet realizada recientemente, el déficit de confianza se está ampliando en todo el mundo, haciendo que las personas cambien su forma de comportarse en línea[54]. Un número creciente de empresas están abordando estas inquietudes

[51] El Comité Europeo de Protección de Datos adoptó directrices sobre los códigos de conducta el 4 de junio de 2019. Estas aclaran los procedimientos y normas por las que se rigen la presentación, aprobación y publicación de los códigos tanto a nivel nacional como de la UE.

[52] Considerando 98 del Reglamento.

[53] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_es; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_es.

[54] Véase la Encuesta Mundial CIGI-Ipsos sobre Seguridad y Confianza en Internet de 2019. De acuerdo con dicha encuesta, al 78 % de las personas encuestadas les preocupaba su privacidad en línea, de las cuales el 49 % aseguraron que su desconfianza les había hecho revelar menos información personal en línea, mientras que el 43 % declaró poner un mayor cuidado a la hora de proteger sus dispositivos y el 39 % afirmó hacer un uso más selectivo de internet, entre otras precauciones. La encuesta se llevó a cabo en veinticinco economías: Alemania, Australia, Brasil, Canadá, China, Egipto, Estados Unidos, Francia, Gran Bretaña, Hong Kong, India, Indonesia, Italia, Japón, Kenia, México, Nigeria, Pakistán, Polonia, República de Corea, Rusia, Sudáfrica, Suecia, Túnez y Turquía.

extendiendo voluntariamente los derechos creados por el Reglamento a sus clientes de terceros países.

Por otro lado, a medida que los países de todo el mundo se enfrentan cada vez con más frecuencia a desafíos similares, se van dotando de nuevas normas de protección de datos o modernizando las existentes. Estas disposiciones legales suelen compartir características comunes con el régimen de protección de datos de la UE, como por ejemplo una legislación global en lugar de normas sectoriales, derechos individuales exigibles y una autoridad de control independiente. Esta tendencia es verdaderamente mundial y se extiende de Corea del Sur a Brasil, de Chile a Tailandia, y de India a Indonesia. La adhesión cada vez más universal al «Convenio 108» del Consejo de Europa[55] —modernizado recientemente[56] con una contribución significativa de la Comisión— es otra señal clara de esta tendencia de convergencia al alza.

Promoción de una circulación de los datos libre y segura a través, entre otros, de las decisiones de adecuación

Esta convergencia que se está produciendo brinda nuevas oportunidades para facilitar los flujos de datos y, en consecuencia, también el comercio y la cooperación entre las autoridades públicas, al tiempo que se mejora el nivel de protección de los datos de las personas en la UE cuando se transfieren al extranjero.

Al aplicar la estrategia establecida en su Comunicación de 2017 titulada «Intercambio y protección de los datos personales en un mundo globalizado»[57], la Comisión intensificó su colaboración con terceros países y otros socios internacionales a partir de los elementos de convergencia entre sistemas de privacidad y desarrollándolos. Esto incluía estudiar la posibilidad de adoptar constataciones de adecuación con terceros países seleccionados[58]. Este trabajo ha arrojado resultados importantes, concretamente la entrada en vigor en febrero de 2019 del acuerdo de adecuación mutua entre la UE y Japón con el que se creó la mayor área mundial de flujos de datos seguros y libres. Las negociaciones de adecuación con Corea del Sur se encuentran en una fase avanzada y ya se han iniciado los trabajos exploratorios para poner en marcha conversaciones en materia de adecuación con varios países latinoamericanos —como Chile o Brasil—, dependiendo de la finalización de procesos legislativos en curso.

---

[55] Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE n.º 108) y el Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos (STE n.º 181). Se trata del único instrumento multilateral vinculante en el ámbito de la protección de datos. Entre los últimos países en ratificar el Convenio figuran Argentina, Cabo Verde, Marruecos y México.

[56] Protocolo por el que se modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE n.º 108), acordado durante la 128.ª sesión del Comité de Ministros en Elsinore, Dinamarca, los días 17 y 18 de mayo de 2018. El texto consolidado del Convenio 108 modernizado está disponible en la siguiente dirección: https://rm.coe.int/16808ade9d.

[57] Comunicación de la Comisión al Parlamento Europeo y al Consejo, «Intercambio y protección de los datos personales en un mundo globalizado», COM/2017/07 final.

[58] Asimismo, el Reglamento ha creado la posibilidad de que las constataciones de adecuación se apliquen también a las organizaciones internacionales, como parte de los esfuerzos de la UE por facilitar los intercambios de datos con dichas entidades.

Los avances también son prometedores en ciertas partes de Asia, como India, Indonesia y Taiwán, así como en los países vecinos del Sur y del Este de Europa, lo que podría abrir la puerta a futuras decisiones de adecuación.

Al mismo tiempo, la Comisión acoge con satisfacción que otros países que han instaurado instrumentos de transferencia similares a la adecuación del Reglamento hayan reconocido que la UE, así como los países reconocidos por esta como «adecuados», garantiza el nivel necesario de protección[59]. Esta situación presenta el potencial de crear una red de países en la que los datos puedan circular libremente.

Además, se está trabajando intensamente con otros terceros países, como por ejemplo Argentina, Canadá, Israel o Nueva Zelanda, para garantizar la continuidad en virtud del Reglamento de las decisiones de adecuación adoptadas al amparo de la Directiva de protección de datos de 1995. Entretanto, el Escudo de la privacidad UE-EE. UU. ha demostrado ser una herramienta útil para garantizar los flujos de datos transatlánticos sobre la base de un nivel elevado de protección, con la participación de más de 4 700 empresas[60]. Su revisión anual garantiza que se comprueba periódicamente el correcto funcionamiento del marco y que los problemas que surjan pueden abordarse a tiempo.

Puesto que no existe una solución única para los flujos de datos, la Comisión también trabaja con las partes interesadas y el Comité para encauzar todo el potencial de las herramientas del Reglamento para las transferencias internacionales. Dicho trabajo gira en torno a instrumentos como las cláusulas contractuales tipo, el desarrollo de regímenes de certificación, códigos de conducta o acuerdos administrativos para los organismos públicos. En ese sentido, la Comisión está interesada en intercambiar experiencias y buenas prácticas con otros sistemas que puedan haber desarrollado un conocimiento técnico específico en alguna de estas herramientas. La Comisión estudiará utilizar las facultades que le confiere el Reglamento por lo que respecta a dichas herramientas de transferencia, especialmente las cláusulas contractuales tipo.

Más allá de las herramientas puramente bilaterales, también podría ser interesante analizar si países afines podrían establecer un marco plurinacional en este ámbito, en un momento en el que los flujos de datos son un componente cada vez más crucial del comercio, las comunicaciones y las interacciones sociales. Un instrumento de esta naturaleza permitiría la libre circulación de los datos entre las partes contratantes, al tiempo que se garantiza el nivel de protección necesario sobre la base de valores compartidos y sistemas convergentes. Podría desarrollarse, por ejemplo, tomando como punto de partida el Convenio 108 modernizado o inspirándose en la iniciativa «libre flujo de datos basado en la confianza» lanzada por Japón a principios de año.

Desarrollo de nuevas sinergias entre los instrumentos comerciales y de protección de datos

[59] Este es el enfoque adoptado, por ejemplo, por Argentina, Colombia, Israel y Suiza.

[60] Esto implica que en sus primeros tres años de existencia, el Escudo de la privacidad cuenta con más empresas participantes que su antecesor, el Puerto Seguro, durante los trece años que estuvo en vigor.

Al tiempo que promueve la convergencia de las prácticas de protección de datos a escala internacional, la Comisión también está decidida a abordar el proteccionismo digital. Para ello, ha desarrollado disposiciones específicas sobre flujos de datos y protección de datos en los acuerdos comerciales que presenta sistemáticamente en sus negociaciones bilaterales y multilaterales, como es el caso de las actuales conversaciones sobre comercio electrónico en la OMC. Estas disposiciones horizontales descartan medidas puramente proteccionistas, como los requisitos de localización forzosa de los datos, al tiempo que mantienen la autonomía reglamentaria de las partes para proteger el derecho fundamental a la protección de los datos.

Aunque los diálogos sobre protección de datos y las negociaciones comerciales deben seguir sendas independientes, pueden complementarse entre sí: el acuerdo de adecuación mutua entre la UE y Japón es el mejor ejemplo de dichas sinergias, facilitando más aun los intercambios comerciales y, de esta manera, ampliando los beneficios del acuerdo de asociación económica. De hecho, este tipo de convergencia, basada en valores compartidos y estándares elevados y respaldada por una ejecución efectiva, proporciona los cimientos más sólidos para el intercambio de datos personales, algo que nuestros socios internacionales reconocen cada vez más[61]. Teniendo en cuenta que la actividad de las empresas tiene un carácter cada vez más transfronterizo y estas prefieren aplicar conjuntos de normas similares en todas sus operaciones comerciales alrededor del mundo, dicha convergencia ayuda a crear un entorno que propicia la inversión directa, facilitando el comercio y reforzando la confianza entre socios comerciales.

Facilitar el intercambio de información para luchar contra la delincuencia y el terrorismo a partir de garantías adecuadas

Aumentar la compatibilidad entre los regímenes de protección de datos también puede facilitar considerablemente los intercambios de información, tan necesarios, entre la UE y las autoridades reguladoras, policiales y judiciales extranjeras y, así, contribuir a una cooperación policial y judicial más eficaz y rápida[62]. Para ello, la Comisión pondera hacer uso de la posibilidad de adoptar decisiones de adecuación en virtud de la Directiva sobre protección de datos en el ámbito policial y judicial para profundizar su cooperación con socios clave en la lucha contra la delincuencia y el terrorismo. Por otro lado, el «Acuerdo marco» entre la UE y los EE. UU.[63], que entró en vigor en febrero de 2017, puede servir de modelo para acuerdos similares con otros socios importantes en materia de seguridad.

---

[61] Como refleja, por ejemplo, la referencia al concepto de «libre flujo de datos basado en la confianza» recogida en la Declaración de los dirigentes del G20 en Osaka: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

[62] Véase la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Agenda Europea de Seguridad», COM(2015) 185 final.

[63] Acuerdo entre la UE y los Estados Unidos sobre la protección de los datos personales cuando se transfieren y tratan con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, incluido el terrorismo, en el marco de la cooperación policial y judicial en materia penal: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:22016A1210(01) (el «Acuerdo marco»). El Acuerdo marco constituye el primer acuerdo internacional bilateral en el ámbito policial y judicial que prevé una extensa lista de derechos y obligaciones en materia de protección de datos en consonancia con el acervo de la UE.

Otros ejemplos que señalan la importancia de contar con unos estándares elevados en el ámbito de la protección de datos como base para una cooperación policial y judicial estable con terceros países son la transferencia de registros de nombres de los pasajeros (PNR)[64] y el intercambio de información operativa entre Europol y socios internacionales importantes. En este sentido, ya se están desarrollando negociaciones sobre acuerdos internacionales con varios países de la vecindad meridional o están a punto de comenzar[65].

Unas garantías sólidas en materia de protección de datos también serán un componente esencial de cualquier acuerdo futuro sobre acceso transfronterizo a pruebas electrónicas en investigaciones penales, a nivel bilateral (acuerdo UE-EE. UU.) o multilateral [Segundo Protocolo Adicional del Convenio sobre la Ciberdelincuencia (Convenio de Budapest) del Consejo de Europa][66].

Fomento de la cooperación entre los encargados del cumplimiento de la protección de datos

En un momento en el que los problemas de respeto de la privacidad o los incidentes de seguridad pueden afectar a un gran número de personas al mismo tiempo en varias jurisdicciones, unas formas de cooperación más estrechas entre las autoridades de control a escala internacional pueden ayudar a garantizar tanto una protección más efectiva de los derechos individuales como un entorno más estable para los operadores empresariales. En este contexto, y manteniendo un contacto estrecho con el Comité, la Comisión estudiará vías para facilitar la cooperación y la asistencia mutua en materia de ejecución entre la UE y las autoridades de control extranjeras, también haciendo uso de los nuevos poderes previstos en este ámbito por el Reglamento[67]. Esto podría abarcar distintas formas de cooperación, desde el desarrollo de herramientas prácticas o de interpretación comunes[68] al intercambio de información sobre investigaciones en curso.

Por último, la Comisión también pretende redoblar su diálogo con organizaciones y redes regionales, como por ejemplo la Asociación de Naciones de Naciones del Asia Sudoriental (ASEAN), la Unión Africana, el Foro de Autoridades de Privacidad de Asia-Pacífico (APPA) o la Red Iberoamericana de Protección de Datos, cuyo papel es cada vez más importante en la formulación de normas comunes de protección de datos, el fomento del intercambio de buenas prácticas y la promoción de la cooperación entre los responsables de la ejecución en

---

Es un ejemplo positivo de cómo se puede reforzar la cooperación policial y judicial con un socio internacional importante negociando un conjunto sólido de garantías en materia de protección de datos.

[64] La Resolución 2396 del Consejo de Seguridad de las Naciones Unidas, de 21 de diciembre de 2017, insta a todos los Estados miembros de las Naciones Unidas a que desarrollen la capacidad de reunir, procesar y analizar los datos del PNR, respetando plenamente los derechos humanos y las libertades fundamentales. Véase asimismo la Comunicación de la Comisión «Agenda Europea de Seguridad», COM (2015)185 final: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_es.pdf.

[65] https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en.

[66] http://europa.eu/rapid/press-release_IP-19-2891_en.htm.

[67] Véase el artículo 50 del Reglamento sobre la cooperación internacional en el ámbito de la protección de datos. Esta disposición abarca un amplio abanico de formas de cooperación, desde la información sobre legislación en materia de protección de datos a la remisión de reclamaciones y la asistencia en investigaciones.

[68] Como por ejemplo modelos comunes para la notificación de infracciones.

este ámbito. Asimismo, trabajará con la Organización para la Cooperación y el Desarrollo Económico y el Foro de Cooperación Económica Asia-Pacífico para desarrollar la convergencia hacia un nivel elevado de protección de datos.

VII. La legislación de protección de datos como parte integral de un amplio abanico de políticas

La protección de los datos personales está garantizada e integrada en varias políticas de la Unión.

Telecomunicaciones y servicios de comunicaciones electrónicas

En enero de 2017, la Comisión adoptó su propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas[69]. La propuesta pretende proteger la confidencialidad de las comunicaciones, tal como prevé la Carta de los Derechos Fundamentales, pero también proteger los datos personales que puedan formar parte de una comunicación así como los equipos terminales de los usuarios finales.

La propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas particulariza y complementa el Reglamento estableciendo normas específicas para los citados fines. Moderniza las normas de la UE en vigor sobre privacidad y comunicaciones electrónicas[70] para reflejar los avances tecnológicos y jurídicos. Refuerza la privacidad de las personas ampliando el ámbito de aplicación de las nuevas normas para que también sean aplicables a los proveedores de servicios de comunicaciones *over-the-top*, creando así igualdad de condiciones para todos los servicios de comunicaciones electrónicas. Aunque que el Parlamento Europeo adoptó un mandato para iniciar diálogos tripartitos en octubre de 2017, el Consejo aún no ha acordado un planteamiento general. La Comisión sigue estando plenamente comprometida con el Reglamento sobre la privacidad y las comunicaciones electrónicas y prestará su apoyo a los colegisladores en sus esfuerzos por alcanzar una rápida adopción de la propuesta de Reglamento.

Salud e investigación

Facilitar los intercambios de datos sanitarios, de carácter sensible en virtud del Reglamento, entre los Estados miembros está ganando importancia en el ámbito de la salud pública por motivos de interés general. Estos incluyen la prestación de asistencia sanitaria o tratamiento, protección frente a amenazas transfronterizas para la salud graves y garantizar niveles elevados de calidad y seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios. El Reglamento establece las normas que garantizan que el tratamiento e intercambio de datos sanitarios en la UE sea lícito y fiable. Estas normas también se aplican al acceso por parte de terceros a los datos médicos de los pacientes, incluidos los datos que

[69] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010.

[70] 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).

figuran en su historial clínico, recetas electrónicas y, a largo plazo, historiales médicos electrónicos completos, así como su utilización con fines de investigación científica. En el ámbito específico de los ensayos clínicos, la Comisión también ha elaborado un documento de preguntas y respuestas específicas sobre la interrelación entre el Reglamento sobre ensayos clínicos[71] y el Reglamento general de protección de datos[72].

Inteligencia artificial (IA)

A medida que la IA adquiere importancia estratégica, resulta fundamental formular normas internacionales para su desarrollo y utilización. Para promover el desarrollo y la adopción de la IA, la Comisión ha optado por un enfoque centrado en el ser humano, lo que implica que las aplicaciones de IA deben respetar los derechos fundamentales[73]. En este contexto, las normas establecidas en el Reglamento proporcionan un marco general e incluyen obligaciones y derechos específicos de especial importancia para el tratamiento de datos personales en la IA. Por ejemplo, el Reglamento incluye el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado salvo en determinadas situaciones[74]. También incluye requisitos de transparencia específicos sobre el uso de la toma de decisiones automatizada, a saber, la obligación de informar de la existencia de tales decisiones y de facilitar información significativa y explicar su importancia y las consecuencias previstas del tratamiento para el interesado[75]. Estos principios fundamentales del Reglamento han sido reconocidos por el Grupo de expertos de alto nivel sobre IA[76], la Organización para la Cooperación y el Desarrollo Económico[77] y el G20[78] como de especial importancia para abordar los retos y las oportunidades que plantea la IA. El Comité Europeo de Protección de Datos ha identificado la IA como uno de los posibles temas en su programa de trabajo para 2019-2020[79].

Transporte

---

[71] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014R0536.

[72] https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

[73] Comunicación de la Comisión, de 8 de abril de 2019, sobre «Generar confianza en la inteligencia artificial centrada en el ser humano»: https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
Directrices éticas para una IA fiable, presentadas por el Grupo de expertos de alto nivel sobre IA el 8 de abril de 2019: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Véase también la Recomendación del Consejo de la OCDE sobre la inteligencia artificial: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, los principios del G20 sobre IA refrendados como parte de la Declaración de los dirigentes del G20 en Osaka: https://www.g20.org/pdf/documents/en/annex_08.pdf y declaración ministerial del G-20 sobre comercio y economía digital: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[74] Artículo 22 del Reglamento.

[75] Artículo 13, apartado 2, letra f), del Reglamento.

[76] https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

[77] Recomendación del Consejo sobre inteligencia artificial: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

[78] Declaración ministerial del G20 sobre comercio y economía digital: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

[79] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf.

El desarrollo de automóviles conectados y ciudades inteligentes depende cada vez más del tratamiento e intercambio de grandes volúmenes de datos personales entre múltiples partes, incluidos los automóviles, los fabricantes de estos, los proveedores de servicios telemáticos y las autoridades públicas responsables de la infraestructura vial. Un entorno de estas características, en el que intervienen diversas partes, implica cierta complejidad por lo que respecta a la asignación de las funciones y responsabilidades de los distintos agentes participantes en el tratamiento de datos personales y sobre cómo garantizar la licitud del tratamiento por parte de todos los agentes. El cumplimiento del Reglamento y la legislación sobre privacidad y comunicaciones electrónicas resulta fundamental para desplegar satisfactoriamente sistemas de transporte inteligentes en todos los modos de transporte y la expansión de herramientas y servicios digitales que posibiliten una movilidad mayor de personas y mercancías[80].

Energía

El desarrollo de soluciones digitales en el sector de la energía depende cada vez en mayor medida del tratamiento de datos personales. La legislación adoptada como parte del paquete «Energía limpia para todos los europeos»[81] incluye disposiciones nuevas que permiten la digitalización del sector de la electricidad y normas sobre acceso a los datos, gestión de datos e interoperabilidad que permiten el manejo de datos en tiempo real de los consumidores a fin de conseguir un ahorro y promover la autogeneración y la participación en el mercado de la energía. Por consiguiente, el respeto de las normas de protección de datos reviste gran importancia de cara a la aplicación satisfactoria de dichas disposiciones.

Competencia

El tratamiento de los datos personales es un elemento que cada vez tiene más peso en la política de competencia[82]. Habida cuenta de que las autoridades de protección de datos son las únicas autoridades a las que se ha encomendado la valoración de una vulneración de las normas de protección de datos, las autoridades de competencia, de consumo y de protección de datos cooperan y seguirán haciéndolo cuando sea necesario en la confluencia de sus respectivas competencias. La Comisión promoverá dicha cooperación y seguirá de cerca su evolución.

Contexto electoral

En sus Orientaciones sobre el uso de datos personales en el contexto electoral[83], publicadas en septiembre de 2018 como parte del paquete electoral[84], la Comisión llamó la atención sobre las normas de especial importancia para los agentes involucrados en las elecciones, incluidas

[80] Por ejemplo, facilitando su planificación y utilización de los diversos medios de transporte a lo largo de su viaje.
[81] En particular la Directiva sobre la electricidad: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0072.
[82] Por ejemplo, el asunto M.8788 – *Apple/Shazam* y el asunto M.8124 – *Microsoft/LinkedIn*.
[83] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0638&qid=1564584418677&from=ES.
[84] http://europa.eu/rapid/press-release_IP-18-5681_es.htm.

cuestiones relativas a la selección muy específica de votantes. El Comité Europeo de Protección de Datos se hizo eco de estas Orientaciones[85] y varias autoridades de protección de datos publicaron orientaciones a escala nacional. En el paquete electoral también se instaba a todos los Estados miembros a que creasen una red electoral nacional integrada por las autoridades nacionales competentes en cuestiones electorales y las responsables de la supervisión y aplicación de las normas, como las de protección de datos, en las actividades en línea importantes de cara a las elecciones. También se adoptaron nuevas medidas para introducir sanciones por la infracción de las normas de protección de datos por parte de los partidos políticos y las fundaciones europeos. La Comisión recomendó que los Estados miembros adoptasen este mismo enfoque a escala nacional. La evaluación de las elecciones al Parlamento Europeo de 2019, cuya publicación está prevista para octubre de 2019, también tendrá en cuenta los aspectos relativos a la protección de datos.

Aplicación de la legislación

Solo se puede construir una Unión de la Seguridad auténtica y eficaz respetando plenamente los derechos fundamentales consagrados en la Carta de la UE y la legislación secundaria de la UE, incluidas las garantías oportunas en materia de protección de datos para permitir el intercambio seguro de datos personales con fines de aplicación de la legislación. Toda limitación del derecho fundamental a la privacidad y la protección de los datos está sujeta a criterios estrictos de necesidad y proporcionalidad.

VIII. Conclusión

A partir de la información disponible hasta la fecha y el diálogo con las partes interesadas, la evaluación preliminar de la Comisión es que, en términos generales, el primer año de aplicación del Reglamento ha sido positivo. Aun así, tal como recoge la presente Comunicación, es preciso seguir avanzando en varios ámbitos.

Aplicación y complemento del marco jurídico

- Los tres Estados miembros que aún no han actualizado su legislación nacional en materia de protección de datos deben hacerlo con carácter urgente. Todos los Estados miembros deben finalizar la armonización de su legislación sectorial con los requisitos del Reglamento.

- La Comisión se valdrá de todas las herramientas a su alcance, incluidos los procedimientos de infracción, para garantizar que todos los Estados miembros respeten el Reglamento y limitar toda fragmentación del marco de protección de datos.

Aprovechar todo el potencial del nuevo sistema de gobernanza:

[85] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

- Los Estados miembros deben asignar suficientes recursos humanos, financieros y técnicos a las autoridades nacionales de protección de datos.

- Las autoridades de protección de datos deben redoblar su cooperación, por ejemplo, llevando a cabo investigaciones conjuntas. Los Estados miembros deben facilitar el desarrollo de dichas investigaciones.

- El Comité debe profundizar el desarrollo de una cultura de protección de datos de la UE y hacer un uso pleno de las herramientas contempladas en el Reglamento para garantizar una aplicación armonizada de las normas. Debe continuar el trabajo que dedica a las directrices, especialmente para las pequeñas y medianas empresas.

- Debe reforzarse el conocimiento técnico de la secretaría del Comité para apoyar y liderar el trabajo del mismo con mayor eficacia.

- La Comisión seguirá prestando su apoyo a las autoridades de protección de datos y al Comité, en particular participando activamente en la actividad del Comité y llamando su atención sobre los requisitos del Derecho de la UE durante la aplicación del Reglamento.

- La Comisión apoyará la interacción entre las autoridades de protección de datos y otras autoridades, especialmente las pertenecientes al ámbito de la competencia, respetando plenamente sus respectivas competencias.

Apoyo y participación de las partes interesadas:

- El Comité debe mejorar la forma de hacer a las partes interesadas partícipes de su trabajo. La Comisión mantendrá su ayuda financiera a las autoridades de protección de datos para ayudarles a llegar hasta las partes interesadas.

- La Comisión continuará sus actividades de sensibilización y su trabajo con las partes interesadas.

Promoción de la convergencia internacional:

- La Comisión intensificará más aun su diálogo sobre adecuación con los socios clave que reúnan las condiciones, también en el ámbito judicial y policial. Concretamente, se ha propuesto concluir las negociaciones en curso con Corea del Sur durante los próximos meses. En 2020 informará sobre la revisión de las once decisiones de adecuación adoptadas al amparo de la Directiva sobre protección de datos.
- La Comisión proseguirá su trabajo, también mediante el intercambio de información y buenas prácticas en materia de asistencia técnica, con los países interesados en adoptar leyes sobre privacidad modernas y fomentar la cooperación con las autoridades de control de terceros países y organizaciones regionales.
- La Comisión colaborará con organizaciones multilaterales y regionales para promover estándares elevados de protección de datos como factores facilitadores del comercio y la

cooperación (p. ej., en el marco de la iniciativa «Libre flujo de datos basado en la confianza» lanzada por Japón en el contexto del G20).

El Reglamento[86] exige que la Comisión presente un informe sobre su aplicación en 2020. Esta será la oportunidad de evaluar los progresos realizados y si después de dos años de aplicación los diversos componentes del nuevo régimen de protección de datos son plenamente operativos. Para ello, la Comisión se mantendrá en contacto con el Parlamento Europeo, el Consejo, los Estados miembros, el Comité Europeo de Protección de Datos, las partes interesadas pertinentes y los ciudadanos.

[86] Artículo 97 del Reglamento.