LA PROTECCIÓN DE LOS DATOS PERSONALES

La protección de los datos personales y el respeto de la vida privada son derechos fundamentales europeos. El Parlamento Europeo ha insistido siempre en la necesidad de lograr un equilibrio entre el refuerzo de la seguridad y la tutela de los derechos humanos, incluida la protección de los datos y de la vida privada. Las nuevas normas de la Unión en materia de protección de datos, que refuerzan los derechos de los ciudadanos y simplifican las normas para las empresas en la era digital, entraron en vigor en mayo de 2018. La investigación llevada a cabo por el Parlamento Europeo señala que la legislación de la Unión en materia de regulación de flujos de datos aporta 51 600 millones EUR al PIB de la Unión. La investigación llevada a cabo por la Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes (Comisión PEGA) del Parlamento Europeo confirma la importancia de la protección de datos para la defensa de la democracia y las libertades individuales en la Unión.

BASE JURÍDICA

Artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE).

Artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

OBJETIVOS

La Unión debe garantizar la aplicación sistemática del derecho fundamental a la protección de datos, consagrado en la Carta de los Derechos Fundamentales de la Unión Europea. Es necesario reforzar la posición de la Unión sobre la protección de los datos personales en el marco de todas sus políticas, incluidas la aplicación de la ley y la prevención de la delincuencia, así como en sus relaciones internacionales, especialmente en una sociedad global caracterizada por la rápida evolución de la tecnología.

RESULTADOS

A. Marco institucional

1. Tratado de Lisboa

Antes de la entrada en vigor del Tratado de Lisboa, la legislación relativa a la protección de datos en el espacio de libertad, seguridad y justicia estaba repartida entre el primer pilar (protección de datos con fines privados y comerciales, con aplicación del método comunitario) y el tercer pilar (protección de datos con fines de aplicación de la ley, con

toma de decisiones intergubernamental). En consecuencia, el proceso decisorio de las dos áreas se regía por dos normativas diferentes. La estructura de pilares desapareció con el Tratado de Lisboa, que aporta una base más sólida para desarrollar un sistema de protección de datos más claro y eficaz, al tiempo que prevé nuevas competencias para el Parlamento Europeo, que se convierte en colegislador. En el artículo 16 del TFUE se dispone que el Parlamento Europeo y el Consejo establecen las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión.

2. Orientaciones estratégicas en el espacio de libertad, seguridad y justicia

Tras los programas de Tampere y La Haya (octubre de 1999 y noviembre de 2004, respectivamente), el Consejo Europeo adoptó en diciembre de 2009 el programa plurianual en el ámbito del espacio de libertad, seguridad y justicia para el período 2010-2014, conocido como el programa de Estocolmo. En sus Conclusiones de junio de 2014, el Consejo Europeo definió las orientaciones estratégicas de la programación legislativa y operativa para los años venideros en el espacio de libertad, seguridad y justicia, con arreglo al artículo 68 del TFUE. Uno de los objetivos clave es una mejor protección de los datos personales en la Unión.

B. Principales instrumentos legislativos en materia de protección de datos

1. Carta de los Derechos Fundamentales de la Unión Europea

Los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconocen el respeto de la vida privada y la protección de los datos de carácter personal como derechos fundamentales estrechamente relacionados, pero independientes.

2. Consejo de Europa

a. Convenio n.o 108 de 1981

El Convenio n.º 108 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 fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Tiene como fin garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. Con el Protocolo que ha modificado el Convenio se pretende ampliar su ámbito de aplicación, aumentar el nivel de protección de los datos y mejorar su eficacia.

b. Convenio Europeo de Derechos Humanos (CEDH)

El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), de 4 de noviembre de 1950, consagra el derecho de toda persona al respeto de la vida privada y familiar, de su domicilio y de su correspondencia.

3. Instrumentos legislativos vigentes de la Unión en materia de protección de datos

a. Reglamento general de protección de datos (RGPD)

En mayo de 2018 entró en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Su objetivo es proteger a todos los ciudadanos de la Unión frente a las violaciones de la privacidad y de los datos personales en un mundo cada vez más basado en los datos, creando al mismo tiempo un marco más claro y coherente para las empresas. Entre los derechos de los que disfrutan los ciudadanos figuran la exigencia de un consentimiento claro y expreso para el tratamiento de sus datos y el derecho a recibir información clara y comprensible sobre el mismo; el derecho al olvido: un ciudadano puede solicitar que se supriman sus datos; la libertad de transferir los datos de un proveedor de servicios a otro (por ejemplo, al cambiar de una red social a otra); y el derecho a saber si los datos han sido pirateados. Las nuevas normas se aplican a todas las empresas que operan en la Unión, incluso a las que tengan su sede fuera de ella. Asimismo, pueden imponerse medidas correctoras, tales como advertencias y órdenes, o sanciones a las empresas que infrinjan las normas. El 24 de junio de 2020, la Comisión presentó un informe sobre la evaluación y revisión del Reglamento[1].

b. Directiva sobre protección de datos en el ámbito penal

En mayo de 2018 también entró en vigor la 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 la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. La Directiva protege el derecho fundamental de los ciudadanos a la protección de datos cuando los utilizan las autoridades encargadas de hacer cumplir la ley. Garantiza que los datos personales de víctimas, testigos y sospechosos de delitos sean debidamente protegidos, y facilita la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo. El 25 de julio de 2022, la Comisión Europea publicó su informe sobre la aplicación y el funcionamiento de la Directiva sobre protección de datos en el ámbito penal, pendiente desde hacía tiempo. Le siguió un estudio de evaluación encargado por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) sobre la evaluación de la aplicación de la Directiva sobre protección de datos en el ámbito penal[2].

c. Directiva sobre la privacidad y las comunicaciones electrónicas

La 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

---

[1]Comunicación de la Comisión, de 24 de junio de 2020, titulada «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)0115).

[2]Vogiatzoglou, P. et al., Assessment of the implementation of the Law Enforcement Directive (Evaluación de la aplicación de la Directiva sobre protección de datos en el ámbito penal), Parlamento Europeo, Dirección General de Políticas Interiores de la Unión, Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales, 7 de diciembre de 2022.

el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) fue modificada mediante la Directiva 2009/136/CE, de 25 de noviembre de 2009. Plantea la delicada cuestión de la conservación de datos, que se ha presentado reiteradamente ante el TJUE y ha dado lugar a una serie de sentencias, la más reciente en 2020, en las que se declara que el Derecho de la Unión se opone a la conservación generalizada e indiscriminada de datos de tráfico y de localización.

En la actualidad se está examinando la nueva 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).

d. Reglamento relativo al tratamiento de los datos personales por las instituciones y órganos de la Unión

El 11 de diciembre de 2018 entró en vigor el 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.

e. Artículos relativos a la protección de datos en actos legislativos sectoriales

Aparte de los principales actos legislativos en materia de protección de datos antes mencionados, también se establecen disposiciones específicas en esta materia en actos legislativos sectoriales, como, por ejemplo:

— el artículo 13 (sobre la protección de los datos personales) de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave;

— el capítulo VI (sobre las garantías en materia de protección de datos) del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol);

— el capítulo VIII (sobre protección de datos) del Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea.

4. Principales acuerdos internacionales de la Unión sobre transferencias de datos

a. Transferencias comerciales de datos: decisiones de adecuación

De conformidad con el artículo 45 del RGPD, la Comisión está facultada para determinar si un país no perteneciente a la Unión ofrece un nivel adecuado de protección de datos, teniendo en cuenta su legislación nacional o los compromisos internacionales que haya contraído.

El Parlamento ha adoptado varias resoluciones en las que manifiesta su preocupación por los flujos transatlánticos de datos. En particular, ha considerado que la Decisión sobre el Escudo de la privacidad UE-EE. UU. no ofrece el nivel adecuado de protección exigido por el Derecho de la Unión, mientras que el TJUE ha invalidado reiteradamente las decisiones de adecuación de la Comisión Europea relativas a los Estados Unidos (véanse sus sentencias de 2015 sobre el puerto seguro en el asunto Schrems y de 2020 sobre el Escudo de la privacidad UE-EE. UU. en el asunto Schrems II).

Tras el acuerdo de principio sobre un nuevo marco de privacidad de datos UE-EE. UU. anunciado el 25 de marzo de 2022 por la presidenta Von der Leyen y el presidente Biden, y el Decreto n.º 14086 del presidente Biden sobre la refuerzo de las salvaguardias para las actividades de inteligencia de señales de los Estados Unidos, de 7 de octubre de 2022, la Comisión Europea puso en marcha, el 13 de diciembre de 2022, el proceso de adopción de una decisión de adecuación para el marco de privacidad de datos UE-EE. UU.

b. Acuerdo marco UE-EE. UU.

En el contexto del procedimiento de aprobación, el Parlamento participó en la aprobación del acuerdo entre los Estados Unidos y la Unión sobre la protección de los datos personales relacionados con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales, también conocido como «acuerdo marco». Dicho acuerdo tiene por objeto garantizar un elevado nivel de protección de la información personal que se transfiere en el marco de la cooperación transatlántica a efectos de aplicación de la ley, en concreto en la lucha contra el terrorismo y la delincuencia organizada.

c. Acuerdos UE-EE. UU., UE-Australia y UE-Canadá sobre el registro de nombres de los pasajeros (PNR)

La Unión ha firmado acuerdos bilaterales sobre el registro de nombres de los pasajeros (PNR) con los Estados Unidos, Australia y Canadá. Los datos PNR consisten en la información facilitada por los pasajeros al reservar vuelos o proceder a la facturación y en los datos recogidos por las compañías aéreas para sus propios fines comerciales. Los datos PNR pueden ser utilizados por las autoridades encargadas de hacer cumplir la ley en su lucha contra la delincuencia grave y el terrorismo.

d. Programa UE-EE. UU. de Seguimiento de la Financiación del Terrorismo

La Unión ha firmado un acuerdo bilateral con los Estados Unidos sobre el tratamiento y la transferencia de datos de mensajería financiera con origen en la Unión y destino en los Estados Unidos a efectos del programa de seguimiento de la financiación del terrorismo.

5. Resoluciones sectoriales que abordan aspectos relativos a la protección de datos

Varias resoluciones del Parlamento relativas a otros ámbitos de actuación también abordan la protección de los datos personales a fin de garantizar la coherencia con la legislación general de la Unión en materia de protección de datos y la protección de la intimidad en esos ámbitos específicos.

6. Autoridades de la Unión de supervisión de la protección de datos

El Supervisor Europeo de Protección de Datos (SEPD) es una autoridad de control independiente encargada de garantizar que las instituciones y los órganos de la Unión cumplen sus obligaciones en materia de protección de datos. Los cometidos principales del SEPD son el control, la consulta y la cooperación.

El Comité Europeo de Protección de Datos, anteriormente el Grupo de Trabajo del Artículo 29, tiene la categoría de órgano de la Unión con personalidad jurídica y dispone de una secretaría independiente. El Comité está compuesto por representantes de las autoridades nacionales de protección de datos de la Unión, el SEPD y la Comisión. El Comité dispone de amplios poderes para resolver litigios entre autoridades nacionales de supervisión y para brindar asesoramiento y orientación acerca de conceptos clave del Reglamento general de protección de datos y de la Directiva sobre protección de datos en el ámbito penal.

PAPEL DEL PARLAMENTO EUROPEO

El Parlamento ha contribuido de modo fundamental a la definición de la legislación de la Unión en el ámbito de la protección de los datos personales, al hacer de la protección de la intimidad una prioridad política. Además, en el marco del procedimiento legislativo ordinario, ha trabajado en la reforma de la protección de datos en pie de igualdad con el Consejo. En 2017 concluyó sus trabajos relativos a la última pieza importante de este rompecabezas, el nuevo Reglamento sobre la privacidad y las comunicaciones electrónicas, y aguarda con impaciencia el fin de los trabajos del Consejo para poder iniciar las negociaciones interinstitucionales.

El Parlamento ha seguido de cerca los acuerdos internacionales sobre transferencias de datos y no ha dudado en hacer oír su voz, ya sea a través del procedimiento de aprobación o de informes de propia iniciativa. Además, antes de votar el Acuerdo PNR entre la Unión y Canadá, decidió solicitar un dictamen al TJUE con arreglo a lo dispuesto en el artículo 218, apartado 1, del TFUE, mediante la Resolución de 25 de noviembre de 2014. En el dictamen correspondiente, emitido el 26 de julio de 2017, el Tribunal de Justicia declaró que el Acuerdo PNR no podía celebrarse en la forma examinada porque varias de sus disposiciones eran incompatibles con el derecho fundamental a la protección de los datos personales.

En numerosas resoluciones, el Parlamento ha expresado sus dudas sobre la adecuación de la protección ofrecida a los ciudadanos de la Unión en el marco de puerto seguro UE-EE. UU. y, posteriormente, en el Escudo de la privacidad UE-EE. UU. Después de que el asunto Schrems II condujera a la invalidación de la Decisión de Ejecución (UE) 2016/1250 de la Comisión Europea sobre la adecuación de la protección proporcionada por el acuerdo Escudo de la privacidad UE-EE. UU., sobre la base de la preocupación de que los poderes de vigilancia del Gobierno de los Estados Unidos. no estuvieran limitados, como exige la legislación de la UE, y de que los ciudadanos de la UE no tuvieran medios efectivos de reparación, el Parlamento Europeo adoptó una resolución en la que lamentaba que la Comisión hubiera antepuesto las relaciones con los Estados Unidos. a los intereses de los ciudadanos de la UE, y que la Comisión hubiera dejado así la tarea de defender la legislación

de la UE a los ciudadanos individuales. Destacó que cualquier futura decisión de adecuación de la Comisión no debe basarse en un sistema de autocertificación, como ocurrió tanto con el sistema de puerto seguro como con el Escudo de la privacidad. El Parlamento pidió a la Comisión que implicara plenamente al CEPD en la evaluación del cumplimiento y la ejecución de cualquier nueva decisión de adecuación en relación con los Estados Unidos[3]. El Parlamento también encargó que se realizase una investigación que puso de manifiesto el complicado panorama de los operadores que comercian con datos personales transferidos a los Estados Unidos[4] y las reformas que debían introducirse en el sistema federal de los Estados Unidos para restituir la confianza en las transferencias de datos transatlánticas[5].

La Comisión LIBE del Parlamento mantiene un debate crítico sobre el proyecto de Decisión de Ejecución de la Comisión Europea relativa a la adecuación de la protección de los datos personales en el marco de privacidad de datos UE-EE. UU., a la luz del Dictamen 5/2023 del Comité Europeo de Protección de Datos. Tras la presentación de la propuesta de la Comisión LIBE el 11 de mayo de 2023, el Parlamento aprobó una Resolución sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU. (2023/2501(RSP)), en la que concluía que el marco de privacidad de datos UE-EE. UU. no crea una equivalencia esencial en el nivel de protección y pide a la Comisión que prosiga las negociaciones con sus homólogos estadounidenses, pero que se abstenga de adoptar la decisión de adecuación hasta que se apliquen plenamente todas las recomendaciones formuladas en la resolución y en el dictamen del CEPD.

El Parlamento ha constituido una Comisión de Investigación Encargada de Examinar el Uso del Programa Espía de Vigilancia Pegasus y Otros Programas Equivalentes en los Estados miembros de la Unión. Presidida por el diputado al Parlamento Europeo Jeroen Lenaers, la Comisión PEGA ha investigado exhaustivamente las prácticas de utilizar programas espía para investigar a miembros de la oposición, periodistas, abogados y activistas de la sociedad civil, así como la manera en que dichas prácticas afectan a los procesos democráticos y a los derechos individuales en la UE. Durante su investigación, la Comisión PEGA consultó a destacados académicos, profesionales y autoridades de la UE y de todo el mundo. El 8 de mayo de 2023, la Comisión PEGA votó a favor de aprobar su informe final, sumamente crítico, con recomendaciones sobre la investigación de las alegaciones de infracción y mala administración en la aplicación del Derecho de la UE en relación con el uso del programa espía de vigilancia Pegasus y otros programas equivalentes, elaborado por la ponente Sophie in 't Veld, y que incluía, entre otros muchos puntos, la recomendación de crear un laboratorio

---

[3]Resolución del Parlamento Europeo, de 20 de mayo de 2021, sobre la sentencia del Tribunal de Justicia de 16 de julio de 2020, Data Protection Commissioner/Facebook Ireland Limited y Maximillian Schrems («Schrems II»), C-311/18(apartado 28).

[4]Sartor, G., et al.: *Regulating targeted and behavioural advertising in digital services: how to ensure users' informed consent* (Regular la publicidad dirigida y comportamental en los servicios digitales: cómo garantizar el consentimiento informado de los usuarios), estudio encargado por el Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo a petición de la Comisión de Asuntos Jurídicos, publicado el 30 de agosto de 2021.

[5]Brown, I. et al.: *Exchanges of Personal Data after the Schrems II Judgment* (Intercambios de datos personales después de la sentencia Schrems II), estudio encargado por el Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo a petición de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, publicado el 8 de julio de 2021.

tecnológico de la UE para la investigación y el seguimiento del uso de programas espía contra los ciudadanos de la UE.

El Parlamento ha encargado una serie de estudios con el fin de disponer de una base científica para sus actividades legislativas, entre los que figuran: The impact of algorithms for online content filtering or moderation — Upload filters (El impacto de los algoritmos para el filtrado o la moderación de contenidos en línea — Cargar filtros), The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (El impacto del Reglamento General de Protección de Datos (RGPD) en la inteligencia artificial) y Biometric Recognition and Behavioural Detection (Reconocimiento biométrico y detección de comportamientos sospechosos).

La preparación de esta ficha temática ha corrido a cargo del Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo.

Mariusz Maciejewski
04/2023