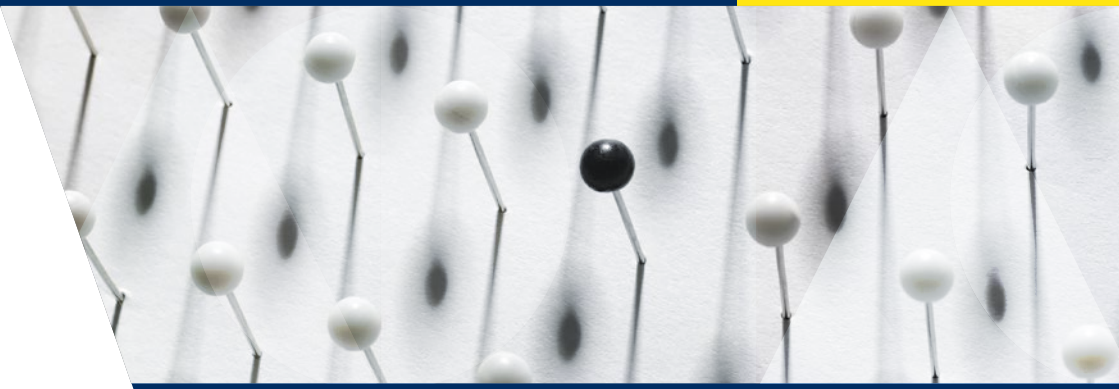
MANUAL



Manual de legislación europea en materia de protección de datos

Edición de 2018

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

El manuscrito de este manual se concluyó en abril de 2018.

Las actualizaciones estarán disponibles en un futuro en la página web de la Agencia de los Derechos Fundamentales de la Unión Europea en: fra.europa.eu, en la página web del Consejo de Europa en: coe.int/dataprotection, en la página web del Tribunal Europeo de Derechos Humanos en el menú Jurisprudencia en: echr.coe.int y en la página web del Supervisor Europeo de Protección de Datos (SEPD) en: edps.europa.eu

Fotografía (cubierta e interior): © iStockphoto

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2019

CdE:	ISBN 978-92-871-9822-8		
FRA – print:	ISBN 978-92-9474-300-8	doi:10.2811/824752	TK-05-17-225-ES-C
FRA – pdf:	ISBN 978-92-9474-298-8	doi:10.2811/60145	TK-05-17-225-ES-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Manual de legislación europea en materia de protección de datos

Edición de 2018

Prólogo

Nuestras sociedades están cada vez más digitalizadas. El ritmo de los desarrollos tecnológicos y la forma en que se procesan los datos personales nos afecta a cada uno de nosotros todos los días y de muchas maneras en razón de estos cambios. Los marcos legales de la Unión Europea (UE) y del Consejo de Europa que salvaguardan la protección de la privacidad y los datos personales se han revisado recientemente.

Europa está a la vanguardia de la protección de datos en todo el mundo. Las normas de protección de datos de la UE se basan en el Convenio 108 del Consejo de Europa, instrumentos de la UE, incluido el Reglamento general de protección de datos y la Directiva de protección de datos para autoridades policiales y penales, así como en la jurisprudencia respectiva del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea.

Las reformas relativas a la protección de datos desarrolladas por la UE y el Consejo de Europa son extensas y, en ocasiones complejas, con amplios beneficios e impacto sobre las personas y las empresas. Este manual pretende crear un estado de opinión y mejorar el conocimiento de las normas de protección de datos, especialmente entre los profesionales del derecho no especializados que tienen que abordar las cuestiones de protección de datos en su trabajo.

El manual ha sido preparado por la Agencia de los Derechos Fundamentales de la Unión Europea (FRA), el Consejo de Europa (junto con el Registro del Tribunal Europeo de Derechos Humanos) y el Supervisor Europeo de Protección de Datos. El manual actualiza una edición de 2014 y forma parte de una serie de manuales jurídicos coproducidos por FRA y el Consejo de Europa.

Queremos manifestar nuestro agradecimiento a las autoridades de protección de datos de Bélgica, Estonia, Francia, Georgia, Hungría, Irlanda, Italia, Mónaco, Suiza y el Reino Unido por sus útiles comentarios sobre la versión preliminar del manual. Además, expresamos nuestro agradecimiento a la Unidad de Protección de Datos de la Comisión Europea y su Unidad de Protección y Flujo de Datos Internacionales. Agradecemos al Tribunal de Justicia de la Unión Europea el apoyo documental proporcionado durante los trabajos preparatorios de este manual.

Christos Giakoumopoulos
Director general de Derechos Humanos y Estado de Derecho del Consejo de Europa

Giovanni Buttarelli
Supervisor europeo de protección de datos

Michael O'Flaherty
Director de la Agencia de los Derechos Fundamentales de la Unión Europea

Índice

Abreviaturas y acrónimos

ACC	Autoridad común de control
Carta	Carta de los Derechos Fundamentales de la Unión Europea
CCTV	Circuito cerrado de televisión
CdE	Consejo de Europa
CE	Comunidad Europea
CEDH	Convenio Europeo de Derechos Humanos
CEPD	Comité Europeo de Protección de Datos
Convenio 108	Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Consejo de Europa). El protocolo de modificación del Convenio 108 fue adoptado por el Comité de Ministros del Consejo de Europa el 18 de abril de 2018 (CETS n.º 223) y las referencias al «Convenio 108 modernizado» se entienden hechas al Convenio tal y como ha sido modificado por el citado protocolo.
C-SIS	Sistema Central de Información de Schengen
DO	Diario Oficial
DUDH	Declaración Universal de Derechos Humanos
EEE	Espacio Económico Europeo
EFSA	Autoridad Europea de Seguridad Alimentaria
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
ESMA	Autoridad Europea de Valores y Mercados
eTEN	Redes transeuropeas de telecomunicaciones
eu-LISA	Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia
EuroPriSe	Sello Europeo de Privacidad
FE	Fiscalía Europea
FRA	Agencia de los Derechos Fundamentales de la Unión Europea
GCS	Grupo coordinador de supervisión

GPS	Sistema de posicionamiento global
GRC	Gestión de relaciones con los clientes
ISP	Proveedor de servicios de internet
N-SIS	Sistema Nacional de Información de Schengen
OCDE	Organización para la Cooperación y el Desarrollo Económicos
ONG	Organización no gubernamental
PIDCP	Pacto Internacional de Derechos Civiles y Políticos
PIN	Número de identificación personal
PNR	Registro de nombres de los pasajeros
RGPD	Reglamento general de protección de datos
SEPA	Zona única de pagos en euros
SEPD	Supervisor Europeo de Protección de Datos
SIA	Sistema de Información Aduanero
SIS	Sistema de Información de Schengen
STCE	Serie de tratados del Consejo de Europa
SWIFT	Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnología de la información y las comunicaciones
TJUE	Tribunal de Justicia de la Unión Europa (hasta diciembre de 2009, Tribunal de Justicia de las Comunidades Europeas o TJCE)
TUE	Tratado de la Unión Europea
UE	Unión Europea
UNE	Unidad Nacional de Europol
VIS	Sistema de Información de Visados

Cómo utilizar este manual

Este manual describe las normas jurídicas que regulan la protección de datos adoptadas por la Unión Europea (UE) y el Consejo de Europa (CdE). Está destinado a los profesionales del Derecho no especializados en el ámbito de la protección de datos, como abogados, jueces, etc., así como a personas que trabajen para otros organismos, como las organizaciones no gubernamentales (ONG), a quienes se les puedan plantear dudas jurídicas relacionadas con la protección de datos.

El manual constituye un primer punto de referencia sobre la legislación europea pertinente y el Convenio Europeo de Derechos Humanos (CEDH), así como el Convenio del CdE para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) y otros instrumentos del CdE.

Cada capítulo comienza con un cuadro en el que se relacionan las normas jurídicas pertinentes para los temas tratados en dicho capítulo. Estos cuadros recogen disposiciones del CdE y de la UE e incluyen jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) y del Tribunal de Justicia de la Unión Europea (TJUE). A continuación, se presentan sucesivamente las disposiciones pertinentes de los dos distintos ordenamientos europeos, según se aplican a los temas concretos tratados. De este modo, el lector puede apreciar las diferencias y las semejanzas entre los dos sistemas jurídicos. Además, el lector podrá encontrar la información relativa a su situación, especialmente si solo está sujeto a la legislación del CdE. En algunos capítulos puede que los temas tratados se presenten en los cuadros en un orden algo distinto del que se sigue en el capítulo propiamente dicho, si con ello se contribuye a presentar el contenido con concisión. Este manual también ofrece una breve panorámica del marco de las Naciones Unidas.

Los profesionales de los Estados que no sean miembros de la UE y que sean Estados miembros del CdE y partes del CEDH y del Convenio 108 pueden acceder a la información correspondiente a su país consultando directamente los apartados relativos al CdE. Los profesionales residentes en Estados que no sean miembros de la UE también deberán tener en cuenta que, desde que se adoptó el Reglamento general de protección de datos, la legislación europea en materia de protección de datos se aplicará a organizaciones y otras entidades no radicadas en la UE en el caso de que procesen datos personales y ofrezcan bienes y servicios a interesados residentes en la Unión o que supervisen el comportamiento de dichos interesados.

Será necesario, pues, que los profesionales de los Estados miembros de la UE consulten ambas secciones, ya que estos Estados quedan vinculados por ambos ordenamientos jurídicos. Hay que señalar que las reformas y la modernización de la legislación europea en materia de protección de datos, realizadas tanto en el marco del Consejo de Europa (Convenio 108 modernizado tal y como ha sido modificado por el Protocolo CETS n.º 223 adoptado por el comité de Ministros del Consejo de Europa 18 de abril de 2018) como de la UE (adopción del Reglamento general de protección de datos y de la Directiva 2016/680/UE), se llevaron a cabo en paralelo. Los reguladores de ambos sistemas jurídicos han hecho todo lo posible por asegurar la coherencia y la compatibilidad entre los dos marcos jurídicos. Las reformas han contribuido así a lograr mayor armonía entre la legislación sobre protección de datos del CdE y de la UE. Quienes precisen más información sobre un tema en particular podrán encontrar una lista de materiales más especializados en el apartado «Bibliografía recomendada». Para conocer las disposiciones del Convenio 108 y de su protocolo adicional del año 2001, que seguirán siendo aplicables hasta la entrada en vigor de las disposiciones del protocolo de modificación, los lectores deben acudir a la versión de éste manual del año 2014.

La legislación del CdE se presenta por medio de breves referencias a casos del TEDH seleccionados entre el elevado número de sentencias y resoluciones de este órgano jurisdiccional en cuestiones relacionadas con la protección de datos.

La legislación pertinente de la UE comprende medidas legislativas adoptadas, disposiciones pertinentes de los Tratados y la Carta de los Derechos Fundamentales de la Unión Europea, de acuerdo con su interpretación en la jurisprudencia del TJUE. Además, este manual presenta dictámenes y directrices adoptados por el Grupo de Trabajo del Artículo 29, el órgano consultivo encargado, con arreglo a la Directiva sobre protección de datos, de prestar asesoramiento especializado a los Estados miembros de la UE; dicho órgano será sustituido por el Comité Europeo de Protección de Datos (CEPD) a partir del 25 de mayo de 2018. Los dictámenes del Supervisor Europeo de Protección de Datos también contienen importantes reflexiones sobre la interpretación de la legislación europea y, por este motivo, se incluyen en este manual.

Los casos citados o descritos en este manual ofrecen ejemplos del importante corpus de jurisprudencia del TEDH y del TJUE. Las directrices incluidas al final del presente manual tienen por objeto ayudar al lector en sus búsquedas de jurisprudencia en línea. La jurisprudencia del TJUE presentada se refiere a la antigua Directiva sobre protección de datos. Sin embargo, las interpretaciones del TJUE siguen siendo

aplicables a los derechos y obligaciones correspondientes establecidos por el Reglamento general de protección de datos.

Además, los cuadros de texto con fondo azul contienen ejemplos ilustrativos con escenarios hipotéticos que aclaran la aplicación práctica de la legislación europea en materia de protección de datos, sobre todo cuando no existe jurisprudencia del TEDH o del TJUE que tenga relevancia específica. Otros cuadros de texto —con fondo gris— contienen ejemplos de otras fuentes distintas de la jurisprudencia del TEDH y el TJUE, como disposiciones legales y dictámenes emitidos por el Grupo de Trabajo del Artículo 29.

El manual comienza con una breve descripción del papel de los dos sistemas jurídicos, tal como se establece en el TEDH y en la legislación europea (capítulo 1). En los capítulos 2 a 10 se abordan las siguientes cuestiones:

- la terminología de la protección de datos;
- los principios fundamentales de la legislación europea en materia de protección de datos;
- las disposiciones de la legislación europea en materia de protección de datos;
- control independiente;
- los derechos de los interesados y su observancia;
- la transmisión y circulación transfronteriza de datos personales;
- la protección de datos en el contexto de la policía y la justicia penal;
- otras normas europeas de protección de datos en ámbitos concretos;
- retos modernos en la protección de los datos personales.

1

Contexto y antecedentes de la legislación europea en materia de protección de datos

UE	Materias tratadas	CdE
El derecho a la protección de los datos		
Tratado de Funcionamiento de la Unión Europea, artículo 16 Carta de los Derechos Fundamentales de la Unión Europea (la Carta), artículo 8 (derecho a la protección de los datos personales) Directiva 95/46/CE 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 (Directiva sobre protección de datos), DO 1995 L 281 (en vigor hasta mayo de 2018) Decisión Marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO 2008 L 350 (en vigor hasta mayo de 2018) Reglamento (UE) 2016/679 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 2016 L 119		CEDH, artículo 8 (derecho al respeto de la vida privada y familiar, el domicilio y la correspondencia) Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108 modernizado)

UE	Materias tratadas	CdE
Directiva (UE) 2016/680 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 (protección de datos para las autoridades policiales y judiciales), DO 2016 L 119 Directiva 2002/58/CE 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 2002 L 201 Reglamento (CE) n.º 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (Reglamento de protección de datos de las instituciones de la UE), DO 2001 L 8		
Limitaciones al derecho de protección de los datos personales		
La Carta, artículo 52, apartado 1 Reglamento general de protección de datos, artículo 23 TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 2010		CEDH, artículo 8, apartado 2 Convenio 108 modernizado, artículo 11 TEDH, *S. y Marper contra Reino Unido* [GS], números 30562/04 y 30566/04, 2008
Ponderación entre derechos		
TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 2010	En general	
TJUE, C-73/07, *Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy* [GS], 2008 TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 2014	Libertad de expresión	TEDH, *Axel Springer AG contra Alemania* [GS], n.º 39954/08, 2012 TEDH, *Mosley contra Reino Unido*, n.º 48009/08, 2011 TEDH, *Bohlen contra Alemania*, n.º 53495/09, 2015

UE	Materias tratadas	CdE
TUE, C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd* [GS], 2010 TJUE , C-615/13 P, *ClientEarth, PAN Europe contra EFSA*, 2015	Acceso a los documentos	TEDH, *Magyar Helsinki Bizottság contra Hungría* [GS], n.º 18030/11, 2016
Reglamento general de protección de datos, artículo 90	Secreto profesional	TEDH, *Pruteanu contra Rumanía*, n.º 30181/05, 2015
Reglamento general de protección de datos, artículo 91	Libertad de religión y convicciones	
	Libertad de las artes y de las ciencias	TEDH, *Vereinigung bildender Künstler contra Austria*, n.º 68345/01, 2007
TJUE, C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU* [GS], 2008	Protección de la propiedad	
TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 2014 TJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 2017	Derechos económicos	

1.1. El derecho a la protección de los datos personales

Puntos clave

- De conformidad con el artículo 8 del CEDH, el derecho de protección de una persona con respecto al tratamiento de los datos personales forma parte del derecho al respeto de la vida privada y familiar, el domicilio y la correspondencia.
- El Convenio 108 del CdE es el primer —y, hasta la fecha, único— instrumento internacional jurídicamente vinculante que regula la protección de datos. Este Convenio se sometió a un proceso de modernización que se completó el 18 de abril de 2018 con la adopción del protocolo de modificación.

- En el Derecho de la UE, la protección de datos ha sido reconocida como un derecho fundamental específico. Está recogido en el artículo 16 del Tratado de Funcionamiento de la UE, así como en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.
- En el Derecho de la UE, la protección de datos se reguló por primera vez en la Directiva sobre protección de datos de 1995.
- En vista de los rápidos avances tecnológicos, la UE adoptó en 2016 nueva legislación para adaptar la normativa de protección de datos a la era digital. El Reglamento general de protección de datos entró en vigor en mayo de 2018 y vino a derogar la Directiva sobre protección de datos.
- Junto con el Reglamento general de protección de datos, la UE adoptó legislación relativa al tratamiento de datos personales por parte de las autoridades estatales para los fines de los cuerpos de seguridad. La Directiva (UE) 2017/680 establece las normas y los principios de protección de datos que regulan el tratamiento de datos personales para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

1.1.1. El derecho al respeto de la vida privada y el derecho a la protección de los datos personales: breve introducción

El derecho al respeto de la vida privada y el derecho a la protección de los datos personales, aunque están estrechamente relacionados, son derechos distintos. El derecho a la privacidad —recogido en el Derecho de la UE como el derecho al respecto de la vida privada— apareció en la legislación internacional sobre derechos humanos en la Declaración Universal de Derechos Humanos (DUDH), adoptada en 1948, como uno de los derechos humanos fundamentales protegidos. Poco después de la adopción de la DUDH, Europa también reconoció este derecho en el Convenio Europeo de Derechos Humanos (CEDH), un tratado que vincula jurídicamente a sus Partes Contratantes y que se redactó en 1950. El CEDH establece que todo el mundo tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Se prohíbe la injerencia de la autoridad pública en el ejercicio de este derecho salvo cuando dicha injerencia esté prevista por la ley y sea necesaria en una sociedad democrática para la protección de intereses generales importantes y legítimos.

La DUDH y el CEDH se adoptaron mucho antes de la llegada de los ordenadores y de internet y del auge de la sociedad de la información. Estos avances han supuesto

considerables ventajas para los ciudadanos y para la sociedad, que han mejorado la calidad de vida, la eficiencia y la productividad. Al mismo tiempo, generan nuevos riesgos para el derecho al respeto de la vida privada. En respuesta a la necesidad de contar con normas que regulen específicamente la recopilación y el uso de información personal, emergió un nuevo concepto de privacidad, conocido en algunas jurisdicciones como «privacidad de la información» y en otras como el «derecho a la autodeterminación en materia de información» ([1]). Este concepto dio lugar a que se elaborasen normas jurídicas específicas para regular la protección de los datos personales.

La protección de datos en Europa comenzó en la década de 1970, con la adopción —en algunos Estados— de legislación para controlar el tratamiento de los datos de carácter personal por los poderes públicos y las grandes empresas ([2]). Entonces se adoptaron instrumentos de protección de datos a escala europea ([3]) y, con el paso de los años, la protección de datos adquirió un valor distinto que no está subsumido en el derecho a la vida privada. En el ordenamiento jurídico de la UE, la protección de datos está reconocida como un derecho fundamental distinto del derecho fundamental al respeto de la vida privada. Esta distinción plantea la cuestión de la relación y las diferencias entre estos dos derechos.

El derecho al respeto de la vida privada y el derecho a la protección de los datos personales están estrechamente relacionados. Ambos tienen por objeto proteger valores similares, es decir, la autonomía y la dignidad humana de las personas físicas, otorgándoles una esfera personal en la que puedan desarrollar libremente su personalidad, pensar y formular sus opiniones. Por tanto, son indispensables para el

([1]) El Tribunal Constitucional Federal de Alemania reconoció el derecho a la autodeterminación en materia de información en la sentencia de 1983 *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Este tribunal consideró que la autodeterminación en materia de información se deriva del derecho fundamental al respecto de la personalidad, protegido en la Constitución alemana. En una sentencia de 2017, el TEDH reconoció que el artículo 8 del CEDH «contempla el derecho a una forma de autodeterminación en materia de información». Véase TEDH, *Satakunnan Markkinapörssi Oy y Satamedia Oy contra Finlandia* [GS], n.º 931/13, 27 de junio de 2017, apartado 137.

([2]) El estado alemán de Hesse adoptó la primera ley sobre protección de datos en 1970, que solo era de aplicación en ese estado. En 1973, Suecia adoptó la primera ley del mundo de ámbito nacional en materia de protección de datos. A finales de la década de 1980, varios Estados europeos (Alemania, Francia, los Países Bajos y el Reino Unido) también habían adoptado legislación sobre protección de datos.

([3]) El Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) se adoptó en 1981. La UE adoptó su primer instrumento integral de protección de datos en 1995: la Directiva 95/46/CE 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.

ejercicio de otras libertades fundamentales, como la libertad de expresión, la libertad de reunión y de asociación pacíficas y la libertad religiosa.

Estos dos derechos se diferencian en su formulación y alcance. El derecho al respeto de la vida privada consiste en una prohibición genérica de la injerencia, sujeta a ciertos criterios de interés general que pueden justificar la injerencia en determinados casos. La protección de los datos personales se considera un derecho moderno y activo ([4]), que establece un sistema con mecanismos de control para proteger a los ciudadanos cuando sus datos personales sean objeto de tratamiento. Este tratamiento debe cumplir los componentes esenciales de protección de los datos personales, concretamente el control independiente y el respeto a los derechos del interesado ([5]).

El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (la Carta) no solo reconoce el derecho a la protección de los datos personales, sino que además señala expresamente los valores fundamentales asociados a este derecho. Establece que el tratamiento de los datos personales debe ser leal, destinarse a fines concretos y contar con el consentimiento de la persona afectada o regirse por un fundamento de derecho legítimo. Los ciudadanos deben tener derecho de acceso y rectificación de sus datos personales y el cumplimiento de este derecho debe ser controlado por una autoridad independiente.

El derecho a la protección de los datos personales entra en juego siempre que se traten datos personales y es, por tanto, más amplio que el derecho al respeto de la vida privada. Cualquier operación de tratamiento de datos personales está sujeta a una protección adecuada. La protección de datos afecta al tratamiento de todo tipo de datos y datos personales, sea cual sea la relación que tenga con la privacidad y sus efectos sobre ella. El tratamiento de datos personales también puede violar el derecho a la vida privada, como reflejan los ejemplos descritos a continuación. Sin embargo, no es necesario demostrar una violación de la vida privada para que se apliquen las normas de protección de datos.

([4]) La Abogada General Sharpston explicó que en el caso intervenían dos derechos distintos: el derecho «clásico» a la protección de la intimidad y un derecho más «moderno», el derecho a la protección de los datos. Véase TJUE, asuntos acumulados C-92/09 y C-93/02, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], *Conclusiones de la Abogado General Sharpston*, 17 de junio de 2010, apartado 71.

([5]) Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, julio de 2013.

El derecho a la privacidad se refiere a situaciones en las que se ha visto lesionado un interés particular o «la vida privada» de una persona. Como se demuestra a lo largo del presente manual, el concepto de «vida privada» ha tenido una interpretación amplia en la jurisprudencia en el sentido de que se aplica a situaciones íntimas, información sensible o confidencial, información que podría perjudicar la percepción de la ciudadanía respecto de una persona e incluso aspectos de la propia vida profesional y conducta pública. Sin embargo, la determinación de si existe o ha existido (o no) una injerencia en la «vida privada» depende del contexto y de los hechos de cada caso.

Por el contrario, cualquier operación que implique el tratamiento de datos personales podría entrar en el ámbito de aplicación de la normativa de protección de datos y dar lugar a que se aplique el derecho a la protección de los datos personales. Por ejemplo, cuando una empresa registre información relativa a los nombres de sus empleados y a la remuneración que reciban, el mero registro de esta información no podrá considerarse injerencia en su vida privada. Sin embargo, sí podría alegarse que existe tal injerencia, por ejemplo, en el caso de que el empresario comunicase información personal de los empleados a terceros. En cualquier caso, los empresarios deben cumplir la normativa de protección de datos, puesto que el registro de información de los empleados constituye tratamiento de datos.

Ejemplo: En *Digital Rights Ireland* ([6]), el TJUE debía resolver sobre la validez de la Directiva 2006/24/CE en vista de los derechos fundamentales a la protección de los datos personales y al respeto de la vida privada, reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea. Esta Directiva obligaba a los proveedores de servicios de comunicaciones electrónicas de acceso público o a las redes públicas de comunicaciones a conservar los datos de telecomunicaciones de los ciudadanos durante un periodo de hasta dos años, con fines de prevención, investigación y enjuiciamiento de delitos graves. Esta medida solo afectaba a los metadatos, datos de localización y otros datos necesarios para identificar al abonado o usuario. No se aplicaba al contenido de las comunicaciones electrónicas.

([6]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros* y *Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.

El TJUE consideró la Directiva una injerencia en el derecho fundamental a la protección de los datos personales «puesto que establece un tratamiento de datos de carácter personal» ([7]). Además, dictaminó que la Directiva constituía una injerencia en el derecho al respeto de la vida privada ([8]). Considerados en conjunto, los datos personales conservados con arreglo a la Directiva, a los que podrían tener acceso las autoridades competentes, podrían «permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan» ([9]). La injerencia en los dos derechos era de gran magnitud y especialmente grave.

El TJUE declaró la Directiva 2006/24/CE nula porque, si bien perseguía un fin legítimo, la injerencia en los derechos a la protección de los datos personales y a la vida privada era grave y no se limitaba a lo estrictamente necesario.

1.1.2. Marco jurídico internacional: Naciones Unidas

El marco de las Naciones Unidas no reconoce la protección de los datos personales como un derecho fundamental, aunque el derecho a la privacidad es un derecho fundamental consolidado en el ordenamiento jurídico internacional. El derecho de las personas físicas a la protección de su esfera privada contra la intrusión de otros, especialmente del Estado, se estableció por primera vez en un instrumento internacional en el artículo 12 de la DUDH relativo al respeto de la vida privada y familiar ([10]). Aunque la DUDH es una declaración no vinculante, tiene un estatuto considerable como instrumento fundacional del Derecho internacional en materia de derechos humanos y ha influido en el desarrollo de otros instrumentos de derechos humanos en Europa. El Pacto Internacional de Derechos Civiles y Políticos (PIDCP), que entró en vigor en 1976, proclama que nadie puede ser objeto de injerencias arbitrarias o ilícitas en su vida privada, su domicilio o su correspondencia, ni de ataques ilícitos a su honra y reputación. El PIDCP es un tratado internacional que compromete a sus 169 partes a respetar y garantizar el ejercicio de los derechos civiles de las personas físicas, incluida la privacidad.

([7]) Ibíd., apartado 36.

([8]) Ibíd., apartados 32-35.

([9]) Ibíd., apartado 27.

([10]) Naciones Unidas, Declaración Universal de Derechos Humanos (DUDH), 10 de diciembre de 1948.

Desde 2013, las Naciones Unidas han adoptado dos resoluciones tituladas «El derecho a la privacidad en la era digital» ([11]) en respuesta a la aparición de nuevas tecnologías y a las revelaciones sobre la vigilancia a gran escala realizada por algunos Estados (las revelaciones de Snowden). Estas resoluciones condenan con firmeza las actividades de vigilancia a gran escala y ponen de relieve las repercusiones que tiene dicha vigilancia para los derechos fundamentales a la privacidad y la libertad de expresión, así como para el funcionamiento de una sociedad democrática pujante. Aunque no son legalmente vinculantes, desencadenaron un importante debate político internacional de alto nivel acerca de la privacidad, las nuevas tecnologías y la vigilancia. También dieron lugar al nombramiento de un Relator Especial sobre el derecho a la privacidad, con el mandato de promover y proteger este derecho. Este Relator tiene la misión concreta de recopilar información sobre prácticas y experiencias nacionales en relación con la privacidad y los retos derivados de las nuevas tecnologías, el intercambio y fomento de buenas prácticas y la detección de obstáculos potenciales.

Aunque en resoluciones anteriores se trataron los efectos negativos de la vigilancia a gran escala y la responsabilidad de los Estados de limitar las competencias de las autoridades de inteligencia, resoluciones más recientes reflejan un avance clave en el debate sobre la privacidad en las Naciones Unidas ([12]). Las resoluciones adoptadas en 2016 y 2017 reafirman la necesidad de limitar las competencias de las agencias de inteligencia y condenan la vigilancia masiva. Sin embargo, también señalan de forma explícita que «la creciente capacidad de las empresas para recopilar, procesar y usar datos personales puede suponer un riesgo para el disfrute del derecho a la privacidad en la era digital». De este modo, además de la responsabilidad de las autoridades estatales, las resoluciones apuntan a la responsabilidad del sector privado de respetar los derechos humanos y exhorta a las empresas a informar a los usuarios sobre la recopilación, el uso, el intercambio y la retención de los datos personales y a adoptar políticas de transparencia en el tratamiento de estos datos.

([11]) Véase Naciones Unidas, Asamblea General, Resolución sobre el derecho a la privacidad en la era digital, A/RES/68/167, Nueva York, 18 de diciembre de 2013; y Naciones Unidas, Asamblea General, Proyecto de resolución revisada sobre el derecho a la privacidad en la era digital, A/C.3/69/L.26/Rev.1, Nueva York, 19 de noviembre de 2014.

([12]) Naciones Unidas, Asamblea General, Proyecto de resolución revisada sobre el derecho a la privacidad en la era digital, A/C.3/71/L.39/Rev.1, Nueva York, 16 de noviembre de 2016; Naciones Unidas, Consejo de Derechos Humanos, «El derecho a la privacidad en la era digital», A/HRC/34/L.7/Rev.1, 22 de marzo de 2017.

1.1.3. El Convenio Europeo de Derechos Humanos

El Consejo de Europa se formó después de la Segunda Guerra Mundial con el fin de reunir a los Estados de Europa para promover el Estado de derecho, la democracia, los derechos humanos y el desarrollo social. Para ello, en 1950 adoptó el CEDH, que entró en vigor en 1953.

Las Partes Contratantes tienen la obligación internacional de cumplir el CEDH. Todos los Estados miembros del CdE han incorporado o aplicado ya el CEDH en su legislación nacional, por lo que están obligados a actuar de conformidad con las disposiciones del Convenio. Las Partes Contratantes deben respetar los derechos estipulados en el Convenio en el ejercicio de cualquier actividad o facultad, incluidas las actividades realizadas por razones de seguridad nacional. El Tribunal Europeo de Derechos Humanos (TEDH) ha dictado algunas sentencias históricas relativas a las actividades del Estado en las áreas sensibles de la legislación y la práctica de la seguridad nacional ([13]). El Tribunal no ha dudado en afirmar que las actividades de vigilancia constituyen una injerencia en el respeto de la vida privada ([14]).

Para garantizar que las Partes Contratantes cumplan con sus obligaciones de conformidad con el CEDH, se creó en 1959 el TEDH en Estrasburgo (Francia). El TEDH vela por que los Estados cumplan con sus obligaciones, de conformidad con el Convenio, examinando las demandas de personas físicas, grupos de personas físicas, ONG o personas jurídicas que denuncian violaciones del Convenio. El TEDH también puede examinar asuntos interestatales presentados por uno o más Estados miembros del CdE contra otro Estado miembro.

En 2018, el Consejo de Europa está compuesto por 47 Partes Contratantes, 28 de las cuales también son Estados miembros de la UE. Las partes demandantes que se presentan ante el TEDH no tienen por qué ser nacionales de una de las Partes Contratantes, aunque las presuntas violaciones deben haberse producido en la jurisdicción de una de las Partes Contratantes.

El derecho a la protección de los datos personales forma parte de los derechos protegidos al amparo del artículo 8 del CEDH, que garantiza el derecho al respeto de la

([13]) Véase, por ejemplo: TEDH, *Klass y otros contra Alemania*, n.º 5029/71, 6 de septiembre de 1978; TEDH, *Rotaru contra Rumanía* [GS], n.º 28341/95, 4 de mayo de 2000; y TEDH, *Szabó y Vissy contra Hungría*, n.º 37138/14, 12 de enero de 2016.

([14]) Ibíd.

vida privada y familiar, el domicilio y la correspondencia y determina las condiciones en las que podrían ser aceptables las limitaciones de este derecho ([15]).

El TEDH ha examinado numerosas situaciones relacionadas con la protección de datos, en particular referidas a la intervención de las comunicaciones ([16]), varias formas de vigilancia por parte de los sectores público y privado ([17]) y la protección frente a la conservación de datos personales por los poderes públicos ([18]). Dado que el respeto de la vida privada no es un derecho absoluto, cuando el ejercicio del derecho a la privacidad puede lesionar otros derechos —como la libertad de expresión y el acceso a la información y viceversa—, el Tribunal trata de alcanzar un equilibrio entre los distintos derechos enfrentados. El Tribunal ha aclarado que el artículo 8 del CEDH no solo obliga a los Estados a que se abstengan de realizar cualquier acción que pueda vulnerar este derecho del Convenio sino también a que, en determinadas circunstancias, bajo obligaciones positivas, garanticen activamente el respeto efectivo de la vida privada y familiar ([19]). Muchos de estos casos se describen con detalle en los capítulos correspondientes.

1.1.4. Convenio 108 del Consejo de Europa

Con el auge de la tecnología de la información en la década de 1960, se generó una creciente necesidad de contar con normas más detalladas para salvaguardar a las personas físicas protegiendo sus datos personales. A mediados de la década de 1970, el Comité de Ministros del Consejo de Europa adoptó diversas resoluciones en materia de protección de datos personales referidas al artículo 8 del CEDH ([20]). En 1981 quedó abierto para su firma el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

([15]) Consejo de Europa, Convenio Europeo de Derechos Humanos, STCE n.º 005, 1950.

([16]) Véase, por ejemplo: TEDH, *Malone contra Reino Unido*, n.º 8691/79, 2 de agosto de 1984; TEDH, *Copland contra Reino Unido*, n.º 62617/00, 3 de abril de 2007; o TEDH, *Mustafa Sezgin Tanrıkulu contra Turquía*, n.º 27473/06, 18 de julio de 2017.

([17]) Véase, por ejemplo: TEDH, *Klass y otros contra Alemania*, n.º 5029/71, 6 de septiembre de 1978; TEDH, *Uzun contra Alemania*, n.º 35623/05, 2 de septiembre de 2010.

([18]) Véase, por ejemplo: TEDH, *Roman Zakharov contra Rusia* [GS], n.º 47143/06, 4 de diciembre de 2015; TEDH, *Szabó y Vissy contra Hungría*, n.º 37138/14, 12 de enero de 2016.

([19]) Véase, por ejemplo: TEDH, *I contra Finlandia*, n.º 20511/03, 17 de julio de 2008; TEDH, *K.U. contra Finlandia*, n.º 2872/02, 2 de diciembre de 2008.

([20]) Consejo de Europa, Comité de Ministros (1973), Resolución (73) 22 relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector privado, de 26 de septiembre de 1973; Consejo de Europa, Comité de Ministros (1974), Resolución (74) 29 relativa a la protección de la vida privada de las personas físicas en relación con los bancos de datos electrónicos en el sector público, de 20 de septiembre de 1974.

(Convenio 108) ([21]). El Convenio 108 fue y sigue siendo el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos.

El Convenio 108 se aplica a todo tratamiento de datos realizado por los sectores público y privado, incluidas las autoridades judiciales y los cuerpos de seguridad. Protege a las personas físicas contra los abusos que pueden llevarse a cabo en el tratamiento de datos personales, y busca, al mismo tiempo, regular los flujos transfronterizos de datos personales. En lo que respecta al tratamiento de datos personales, los principios establecidos en el Convenio se refieren, en particular, a la recopilación y el tratamiento automático de datos de manera lícita y leal, con fines legítimos especificados. Esto significa que los datos no deben utilizarse con propósitos incompatibles con estos fines y que no deben conservarse más tiempo del necesario. También se refieren a la calidad de los datos, que concretamente deben ser adecuados, pertinentes y no excesivos (proporcionalidad), además de exactos.

No solo establece garantías en relación con el tratamiento de datos personales y obligaciones relativas a la seguridad de los datos, sino que prohíbe, a falta de garantías jurídicas adecuadas, el tratamiento de los datos «sensibles» de una persona, como la raza, las opiniones políticas, la salud, la religión, la vida sexual o los antecedentes penales.

El Convenio consagra también el derecho de las personas físicas a conocer los datos que se conservan sobre ellas y, en su caso, a rectificarlos. Solo es posible limitar los derechos establecidos en el Convenio si entran en juego intereses superiores, como la seguridad o la defensa del Estado. Además, el Convenio establece la libre circulación de datos personales entre sus Partes Contratantes e impone algunas limitaciones a la circulación de los datos en Estados donde la normativa no establezca una protección equivalente.

Hay que señalar que el Convenio 108 es vinculante para los Estados que lo han ratificado. No está sujeto al control judicial del TEDH, pero se ha tomado en consideración en la jurisprudencia del TEDH en el contexto del artículo 8 del CEDH. A lo largo de los años, el Tribunal ha determinado que la protección de los datos personales es parte importante del derecho al respeto de la vida privada (artículo 8) y se ha regido por

([21]) Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, STCE n.º 108, 1981.

los principios del Convenio 108 para determinar si se ha producido o no injerencia en este derecho fundamental ([22]).

Para un mayor desarrollo de los principios generales y las normas que establece el Convenio 108, el Comité de Ministros del CdE ha adoptado diversas recomendaciones que no son jurídicamente vinculantes. Estas recomendaciones han influido en el desarrollo de la legislación de protección de datos en Europa. Por ejemplo, la Recomendación sobre la policía fue durante años el único instrumento de Europa que ofrecía orientaciones sobre el uso de datos personales en el sector de la policía ([23]). Los principios que contiene dicha recomendación, como los medios de conservación de los ficheros de datos y la necesidad de establecer normas claras sobre las personas autorizadas a obtener acceso a dichos ficheros, se han desarrollado y reflejado en la legislación europea posterior ([24]). Otras recomendaciones más recientes tratan de los retos de la era digital; por ejemplo, en relación con el tratamiento de datos personales en el contexto del empleo (véase el capítulo 9).

Todos los Estados miembros de la Unión Europea han ratificado el Convenio 108. En 1999 se modificó el Convenio 108 para que la UE pudiera ser Parte del mismo ([25]). En 2001 se adoptó un Protocolo Adicional al Convenio 108 que introdujo disposiciones sobre los flujos de datos transfronterizos a los Estados no Partes, los denominados terceros países, y sobre la obligatoriedad de crear autoridades nacionales de control de la protección de los datos ([26]).

El Convenio 108 está abierto para la adhesión de Partes no Contratantes del CdE. El potencial del Convenio como norma universal, junto con su carácter abierto, podría servir de base para promover la protección de datos a escala mundial. Hasta la fecha hay 51 países partes del Convenio 108, entre los que se encuentran todos los

([22]) Véase, por ejemplo: TEDH, *Z contra Finlandia*, n.º 22009/93, 25 de febrero de 1997.

([23]) Consejo de Europa, Comité de Ministros (1987), Recomendación Rec(87)15 a los Estados miembros dirigida a regular la utilización de datos de carácter personal en el sector de la policía, Estrasburgo, 17 de septiembre de 1987.

([24]) 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, 23 de noviembre de 1995.

([25]) Consejo de Europa, Modificaciones del Convenio para la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal (STCE n.º 108) para permitir la adhesión de las Comunidades Europeas, adoptado por el Comité de Ministros el 15 de junio de 1999 en Estrasburgo; artículo 23, apartado 2, del Convenio 108 en su versión modificada.

([26]) Consejo de Europa, Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en lo que respecta a las autoridades de control y los flujos de datos transfronterizos, STCE n.º 181, 2001.

Estados miembros del Consejo de Europa (47 países) más Uruguay, que fue el primer país no europeo en adherirse en agosto de 2013, así como Mauricio, Túnez y Senegal, que se incorporaron en 2016 y 2017.

Este Convenio se sometió recientemente a un proceso de modernización. La consulta pública realizada en 2011 confirmó los dos objetivos principales de esos trabajos: reforzar la protección de la privacidad en el ámbito digital y fortalecer el mecanismo de seguimiento del Convenio. El proceso de modernización se centró en estos objetivos y se completó el 18 de abril de 2018 con la adopción del protocolo de modificación del Convenio 108 (Protocolo CETS n.º 223). Los trabajos se llevaron a cabo en paralelo con otras reformas de instrumentos internacionales de protección de datos y conjuntamente con la reforma de la normativa de protección de datos de la UE adoptada en 2012. Los reguladores del Consejo de Europa y de la UE han hecho todo lo posible por asegurar la coherencia y la compatibilidad entre los dos marcos jurídicos. La modernización preserva el carácter genérico y flexible del Convenio y refuerza su potencial como instrumento universal de regulación de la protección de datos. Reafirma y estabiliza principios importantes y confiere nuevos derechos a las personas físicas, al tiempo que aumenta las responsabilidades de las entidades que tratan datos personales y garantiza una mayor rendición de cuentas. Por ejemplo, las personas cuyos datos personales son objeto de tratamiento tienen derecho a saber el motivo por el que se efectúa dicho tratamiento y a oponerse al mismo. Para contrarrestar la creciente práctica de creación de perfiles en internet, el Convenio también establece el derecho de las personas a no estar sujetas a decisiones adoptadas únicamente en función del tratamiento automatizado sin tener en cuenta sus propias opiniones. El control efectivo del cumplimiento de la normativa de protección de datos por parte de autoridades de control independientes en las Partes Contratantes se considera esencial para la aplicación práctica del Convenio. Con este fin, el Convenio modernizado subraya la necesidad de que se confieran a las autoridades de control competencias y atribuciones efectivas y que gocen de auténtica independencia en el cumplimiento de su misión.

1.1.5. Legislación sobre protección de datos de la Unión Europea

El Derecho de la UE está compuesto por Derecho primario y Derecho derivado. Los Tratados, en concreto el Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE), han sido ratificados por todos los Estados miembros de la UE y constituyen el «Derecho primario de la Unión Europea». Los

reglamentos, directivas y decisiones de la UE han sido adoptados por las instituciones de la UE en las que se ha delegado tal autoridad en virtud de los Tratados, y constituyen el «Derecho derivado de la UE».

La protección de datos en el Derecho primario de la UE

Los tratados originales de las Comunidades Europeas no contenían referencia alguna a los derechos humanos o su protección, debido a que la Comunidad Económica Europea se concibió en un principio como una organización regional orientada a la integración económica y a la creación de un mercado común. Uno de los principios fundamentales en los que se sustenta la creación y el desarrollo de las Comunidades Europeas —y que sigue siendo válido hoy en día— es el principio de atribución. En virtud de este principio, la UE actúa exclusivamente dentro de los límites de las competencias que le son atribuidas por los Estados miembros y reflejadas en los Tratados de la Unión. A diferencia del Consejo de Europa, los Tratados de la UE no incluyen competencias expresas en materia de derechos fundamentales.

Sin embargo, el TJUE realizó importantes interpretaciones de los Tratados a raíz de los asuntos que juzgó en relación con presuntas violaciones de los derechos humanos en materias reguladas por la legislación de la UE. Para conceder protección a las personas físicas, se incorporaron los derechos fundamentales a los denominados principios generales del Derecho europeo. Según el TJUE, estos principios generales reflejan el contenido de la protección de los derechos humanos que recogen las constituciones nacionales y los tratados de derechos humanos, en particular, el CEDH. El TJUE declaró que velaría por el cumplimiento del Derecho de la UE con estos principios.

En reconocimiento de que sus políticas podrían repercutir en los derechos humanos y en un esfuerzo por que los ciudadanos se sintieran «más cerca» de la Unión Europea, la UE proclamó en 2000 la Carta de Derechos Fundamentales de la Unión Europea (la Carta). Esta Carta incorpora todos los derechos civiles, políticos, económicos y sociales de los ciudadanos europeos, y constituye la síntesis de las tradiciones constitucionales y obligaciones internacionales que son comunes a los Estados miembros. Los derechos descritos en la carta se dividen en seis capítulos: dignidad, libertades, igualdad, solidaridad, ciudadanía y justicia.

En su origen, la Carta era un documento de carácter estrictamente político, pero pasó a ser jurídicamente vinculante ([27]) como Derecho primario de la UE (véase el artículo 6, apartado 1, del TUE) con la entrada en vigor del Tratado de Lisboa el 1 de diciembre de 2009 ([28]). Las disposiciones de la Carta tienen como destinatarios a las instituciones y los organismos de la UE, a los que obliga a respetar los derechos en ella recogidos en el desempeño de sus funciones. Las disposiciones de la Carta también son vinculantes para los Estados miembros en la aplicación del Derecho de la UE.

La Carta no solo garantiza el respeto de la vida privada y familiar (artículo 7), sino que establece además el derecho a la protección de los datos personales (artículo 8), con lo que eleva expresamente el nivel de dicha protección al de un derecho fundamental en el Derecho de la UE. Las instituciones y los organismos de la UE deben garantizar y respetar este derecho, al igual que los Estados miembros en la aplicación del Derecho de la Unión (artículo 51 de la Carta). Al haberse formulado varios años después de la Directiva sobre protección de datos, debe entenderse que el artículo 8 de la Carta incorpora la legislación preexistente de la UE en materia de protección de datos. Por lo tanto, la Carta no solo menciona expresamente el derecho a la protección de los datos en el artículo 8, apartado 1, sino que también hace referencia a los principios clave de la protección de datos en el apartado 2 de dicho artículo. Por último, el artículo 8, apartado 3, de la Carta exige que la aplicación de dichos principios esté sujeta al control de una autoridad independiente.

La adopción del Tratado de Lisboa es un hito en la evolución de las leyes sobre protección de datos, no solo porque confiere a la carta el estatuto de documento jurídico vinculante, al nivel del Derecho primario, sino también porque establece el derecho a la protección de los datos personales. Este derecho está específicamente contemplado en el artículo 16 del TFUE, en la parte dedicada a los principios generales de la UE. El artículo 16 también crea una nueva base jurídica, por la que se otorga a la UE la facultad de legislar en materia de protección de datos. Este es un avance importante, porque la normativa de protección de datos de la UE —en particular, la Directiva sobre protección de datos— se basó en principio en el fundamento jurídico del mercado interior y en la necesidad de armonizar las legislaciones nacionales para no limitar la libre circulación de datos en la Unión Europea. El artículo 16 del TFUE establece ahora una base jurídica independiente para una formulación moderna

([27]) UE (2012), Carta de los Derechos Fundamentales de la Unión Europea, DO 2012 C 326.

([28]) Véanse Comunidades Europeas (2012), versiones consolidadas del Tratado de la Unión Europea (TUE), y del Tratado de Funcionamiento de la Unión Europea (TFUE), DO 2012 C 326.

e integral de la protección de datos, que comprenda todas las materias de competencia de la UE, incluida la cooperación policial y judicial en materia penal. Dicho artículo del TFUE también afirma que el cumplimiento de la normativa de protección de datos adoptada en virtud del mismo debe estar sujeta al control de autoridades de supervisión independientes. El artículo 16 sirvió de base jurídica para la adopción de la reforma integral de la normativa de protección de datos en 2016, es decir, del Reglamento general de protección de datos y de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal (véase a continuación).

El Reglamento general de protección de datos

Desde 1995 hasta mayo de 2018, el principal instrumento jurídico de la UE en materia de protección de datos fue la 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 (Directiva sobre protección de datos) ([29]). Se adoptó en 1995, en un momento en el que varios Estados miembros habían adoptado ya leyes nacionales de protección de datos ([30]) y surgió en respuesta a la necesidad de armonizar dichas leyes para garantizar un elevado nivel de protección y la libre circulación de datos personales entre los diferentes Estados miembros. La libre circulación de bienes y servicios, capitales y personas en el mercado interior requería la libre circulación de datos, que no podía llevarse a cabo si los Estados miembros no podían confiar en un nivel elevado y uniforme de protección de los datos.

La Directiva sobre protección de datos reflejaba los principios de protección de datos que ya contenían las leyes nacionales y el Convenio 108, aunque en muchos casos los ampliaba. Aprovechaba la posibilidad, contemplada en el artículo 11 del Convenio 108, de añadir instrumentos de protección. En particular, la introducción en la Directiva del control independiente como instrumento de mejora del cumplimiento de las normas de protección de datos demostró ser una importante aportación al funcionamiento efectivo de la legislación europea en materia de protección de datos. En consecuencia, esta característica fue incorporada al Derecho del CdE en

([29]) 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 1995 L 281.

([30]) El estado alemán de Hesse adoptó la primera ley del mundo sobre protección de datos en 1970, que solo era de aplicación en ese estado. Suecia adoptó la *Datalagen* en 1973; Alemania la *Bundesdatenschutzgestez* en 1976; y Francia la *Loi relative à l'informatique, aux fichiers et aux libertés* en 1977. En el Reino Unido, la *Data Protection Act* se adoptó en 1984. Por último, los Países Bajos adoptaron los *Wet Persoonregistraties* en 1989.

2001 a través del Protocolo adicional al Convenio 108. Esto es ilustrativo de la estrecha interacción y positiva influencia de ambos instrumentos entre sí a lo largo de los años.

La Directiva sobre protección de datos establecía un amplio y detallado sistema de protección de datos en la UE. Sin embargo, de acuerdo con el régimen jurídico de la UE, las Directivas no son de aplicación directa, sino que deben ser transpuestas a las legislaciones nacionales de los Estados miembros. Inevitablemente, los Estados miembros tienen cierta discrecionalidad en la transposición de las disposiciones de la Directiva. Aunque la Directiva tenía por objeto conseguir una armonización completa ([31]) (y un nivel de protección total), en la práctica se transpuso de forma diferente en los distintos Estados miembros. Esto dio lugar a que se adoptasen diversas normas de protección de datos en el conjunto de la UE, con normas y definiciones interpretadas de manera diferente en las legislaciones nacionales. También se aplicaron distintos niveles de control de su aplicación y de gravedad de las sanciones según los Estados miembros. Por último, las tecnologías de la información han experimentado cambios significativos desde que se redactó la Directiva a mediados de la década de 1990. Todas estas razones llevaron a reformar la legislación de la UE en materia de protección de datos.

Esta reforma dio lugar a la adopción del Reglamento general de protección de datos en abril de 2016, después de años de intensos debates. Los debates sobre la necesidad de modernizar la normativa de protección de datos de la UE comenzaron en 2009, cuando la Comisión puso en marcha una consulta pública sobre el marco jurídico futuro para el derecho fundamental a la protección de los datos personales. La propuesta de Reglamento fue publicada por la Comisión en enero de 2012, como inicio de un largo proceso legislativo de negociación entre el Parlamento Europeo y el Consejo de la UE. Tras su adopción, el Reglamento general de protección de datos contemplaba un periodo de transición de dos años. Su plena entrada en vigor se produjo el 25 de mayo de 2018, momento en que se derogó la Directiva sobre protección de datos.

Con la adopción del Reglamento general de protección de datos en 2016, se modernizó la legislación de la UE en materia de protección de datos, adecuándola para proteger los derechos fundamentales en el contexto de los retos económicos y sociales de la era digital. El RGPD preserva y desarrolla los principios y derechos esenciales

([31]) TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 24 de noviembre de 2011, apdo. 29.

del interesado que estaban recogidos en la Directiva sobre protección de datos. Además, introduce nuevas disposiciones que obligan a las organizaciones a aplicar la protección de los datos desde el diseño y por defecto, a nombrar un delegado de protección de datos en determinadas circunstancias, a respetar un nuevo derecho a la portabilidad de los datos y a atenerse al principio de responsabilidad proactiva. En el Derecho de la UE, los Reglamentos son de aplicación directa y no necesitan transposición nacional. El Reglamento general de protección de datos establece por tanto un único conjunto de normas de protección de datos para toda la UE. De este modo se crea una normativa de protección de datos coherente en todo el territorio de la UE, con lo que se establece un entorno de seguridad jurídica del que pueden beneficiarse los operadores económicos y las personas físicas como «interesados».

Sin embargo, aunque el Reglamento general de protección de datos es de aplicación directa, cabe esperar que los Estados miembros actualicen su legislación nacional vigente en materia de protección de datos para que se ajuste debidamente al Reglamento, además de aplicar el margen de discrecionalidad para la adopción de disposiciones específicas que se contempla en el considerando 10. Las principales normas y principios establecidos en el Reglamento y los firmes derechos que confiere a las personas físicas son el objeto de gran parte de este manual y se presentan en los capítulos siguientes. El Reglamento contiene amplias disposiciones sobre el alcance territorial. Se aplica a las empresas radicadas en la UE, así como a los responsables y encargados del tratamiento de datos no radicados en la UE que ofrecen bienes o servicios a los interesados en la UE o que observan su comportamiento. Dado que varias empresas tecnológicas extranjeras tienen una importante cuota del mercado europeo y millones de clientes en la UE, es importante someter a estas organizaciones a la normativa de protección de datos de la UE a fin de garantizar la protección de las personas físicas y la competencia en igualdad de condiciones.

La protección de datos en los cuerpos de seguridad: la Directiva 2016/680

La Directiva sobre protección de datos derogada establecía un régimen de protección de datos muy amplio. Este régimen se ha ampliado todavía más con la adopción del Reglamento general de protección de datos. Aunque ya era muy extenso, el ámbito de aplicación de la Directiva sobre protección de datos derogada se limitaba a las actividades circunscritas al mercado interior y a las actividades de autoridades públicas distintas de los cuerpos de seguridad. Por tanto, era preciso adoptar instrumentos especiales para conseguir la claridad y el equilibrio necesarios entre la protección de datos y otros intereses legítimos y para resolver problemas

especialmente pertinentes en determinados sectores. Este es el caso de las normas que regulan el tratamiento de datos personales por parte de los cuerpos de seguridad.

El primer instrumento jurídico de la UE en regular esta materia fue la Decisión marco 2008/977/JAI del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Sus disposiciones se aplicaban exclusivamente al intercambio de datos policiales y judiciales entre Estados miembros. El tratamiento de datos personales por los cuerpos de seguridad a escala nacional estaba excluido de su ámbito de aplicación.

Esta situación se corrigió con la Directiva 2016/680 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 ([32]), conocida como Directiva sobre protección de datos para las autoridades policiales y de justicia penal. Adoptada en paralelo al Reglamento general de protección de datos, esta Directiva derogó la Decisión marco 2008/977/JAI y estableció un sistema integral de protección de los datos personales en el contexto de los cuerpos de seguridad, al tiempo que reconocía las particularidades del tratamiento de datos relacionado con la seguridad pública. Aunque el Reglamento general de protección de datos establece disposiciones generales para proteger a las personas en relación con el tratamiento de sus datos personales y garantizar la libre circulación de dichos datos en la UE, la Directiva establece disposiciones específicas para la protección de datos en los ámbitos de la cooperación judicial en materia penal y la cooperación policial. Cuando una autoridad competente trate datos personales para los fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, se aplicará la Directiva 2016/680. Cuando una autoridad competente trate datos personales con fines distintos de los antes mencionados, se aplicará el régimen general establecido por el Reglamento general de protección de datos. A diferencia de su predecesora (Decisión marco 2008/977/JAI del Consejo), el ámbito de aplicación de la Directiva 2016/680 se extiende al tratamiento de datos personales a escala nacional por los cuerpos de seguridad y no se limita al intercambio de dichos datos entre Estados miembros. Además, la Directiva

([32]) 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, DO L 119, 4.5.2016.

trata de alcanzar un equilibrio entre los derechos de las personas físicas y los legítimos objetivos del tratamiento de datos relacionado con la seguridad.

Con este fin, la Directiva reconoce el derecho a la protección de los datos personales y los principios fundamentales por los que debe regirse el tratamiento de los datos, ateniéndose estrictamente a las disposiciones y los principios consagrados en el Reglamento general de protección de datos. Los derechos de las personas físicas y las obligaciones impuestas a los responsables del tratamiento —por ejemplo, en relación con la seguridad de los datos, la protección de los datos por diseño y por defecto y las notificaciones de violación de datos personales— reflejan los derechos y obligaciones que contiene el Reglamento general de protección de datos. La Directiva también tiene en cuenta y trata de hacer frente a importantes retos tecnológicos emergentes que pueden tener efectos especialmente onerosos sobre las personas físicas, como el uso de técnicas de creación de perfiles por parte de los cuerpos de seguridad. En principio, deben prohibirse las decisiones basadas únicamente en un tratamiento automatizado, incluida la creación de perfiles ([33]). Además, no deben estar basadas en datos sensibles. Estos principios están sujetos a determinadas excepciones contempladas en la Directiva. Además, este tratamiento de datos personales no debe dar lugar a que se discrimine a ninguna persona ([34]).

Esta Directiva también contiene disposiciones destinadas a garantizar la rendición de cuentas de los responsables del tratamiento. Deben nombrar un delegado de protección de datos responsable de controlar el cumplimiento de las normas de protección de datos, de informar y asesorar a la entidad y los empleados que lleven a cabo el tratamiento acerca de sus obligaciones y de cooperar con la autoridad de control. El tratamiento de datos personales en el sector de la policía y la justicia penal está sujeto ahora al control de autoridades de supervisión independientes. Tanto el régimen jurídico general de protección de datos como el régimen especial de protección de datos para los cuerpos de seguridad y la justicia penal deben cumplir por igual con los requisitos previstos en la Carta de los Derechos Fundamentales de la Unión Europea.

El régimen especial aplicable al tratamiento de datos personales en el contexto de la cooperación policial y judicial que establece la Directiva sobre protección de datos para las autoridades policiales y de justicia penal se describe con detalle en el capítulo 8.

([33]) Directiva sobre protección de datos para las autoridades policiales y de justicia penal, artículo 11, apartado 1.

([34]) Ibíd., artículo 11, apartados 2 y 3.

Directiva sobre la privacidad y las comunicaciones electrónicas

También se consideró necesario adoptar normas de protección de datos especiales en el sector de las comunicaciones electrónicas. Con el desarrollo de internet y de la telefonía fija y móvil, era importante garantizar el respeto de los derechos de los usuarios a la privacidad y la confidencialidad. La Directiva 2002/58/CE ([35]) 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) establece normas sobre la seguridad de los datos personales en estas redes, la notificación de violaciones de los datos personales y la confidencialidad de las comunicaciones.

En lo que respecta a la seguridad, los operadores de servicios de comunicaciones electrónicas deben, entre otras cosas, garantizar que el acceso a los datos personales se limite exclusivamente a personas autorizadas y adoptar medidas para evitar que los datos personales se destruyan, se pierdan o se deterioren accidentalmente ([36]). Cuando exista un riesgo específico de vulneración de la seguridad de la red pública de comunicaciones, los operadores deben informar a los abonados de dicho riesgo ([37]). Si a pesar de las medidas de seguridad adoptadas se produjera un quebrantamiento de la seguridad, los operadores deberán notificar la violación de los datos personales a la autoridad nacional competente responsable de la aplicación y del cumplimiento de la Directiva. En ocasiones, los operadores también deben notificar la violación de datos personales a los interesados, en concreto cuando dicha violación pueda afectar negativamente a sus datos personales o su privacidad ([38]). La confidencialidad de las comunicaciones exige que, en principio, se prohíba la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los metadatos. La Directiva también prohíbe las comunicaciones no solicitadas (a menudo conocidas como *spam*), a menos que el usuario haya otorgado su consentimiento, y contiene disposiciones sobre el almacenamiento de *cookies* en ordenadores y otros dispositivos. Estas obligaciones negativas fundamentales indican claramente que la confidencialidad de las comunicaciones está vinculada de manera significativa a la protección del derecho al respeto de la vida

([35]) 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.

([36]) Directiva sobre la privacidad y las comunicaciones electrónicas, artículo 4, apartado 1.

([37]) Ibíd., artículo 4, apartado 2.

([38]) Ibíd., artículo 4, apartado 3.

privada consagrado en el artículo 7 de la Carta y del derecho a la protección de los datos personales consagrado en el artículo 8 de la Carta.

En enero de 2017, la Comisión publicó una propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas, destinado a sustituir a la Directiva sobre la privacidad y las comunicaciones electrónicas. La reforma pretende armonizar las normas que regulan las comunicaciones electrónicas con el nuevo régimen de protección de datos establecido en el Reglamento general de protección de datos. Este nuevo Reglamento será de aplicación directa en todo el territorio de la UE; todas las personas físicas gozarán del mismo nivel de protección de sus comunicaciones electrónicas, mientras que los operadores y empresas de telecomunicaciones se beneficiarán de la claridad, la seguridad jurídica y la existencia de un solo cuerpo normativo en toda la UE. Las normas propuestas sobre confidencialidad de las comunicaciones electrónicas también se aplicarán a los nuevos operadores que presten servicios de comunicaciones electrónicas no contemplados en la Directiva sobre la privacidad y las comunicaciones electrónicas. Esta última solo contemplaba a los proveedores de servicios de telecomunicaciones tradicionales. Con el uso masivo de servicios como Skype, WhatsApp, Facebook Messenger y Viber para enviar mensajes o realizar llamadas, estos servicios de transmisión libre (OTT, por sus siglas en inglés) se regirán ahora por el Reglamento y deberán cumplir sus requisitos en materia de protección, privacidad y seguridad de los datos. En el momento de publicarse el presente manual, el proceso legislativo sobre la privacidad y las comunicaciones electrónicas seguía su curso.

Reglamento n.º 45/2001

Dado que la Directiva sobre protección de datos solo podía aplicarse a los Estados miembros de la UE, era necesario adoptar un instrumento jurídico adicional para establecer la protección de datos en el tratamiento de datos personales por parte de las instituciones y organismos de la UE. El Reglamento (CE) n.º 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (Reglamento de protección de datos de las instituciones de la UE) cumple esa función ([39]).

([39]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO 2001 L 8.

El Reglamento n.º 45/2001 se ajusta estrictamente a los principios del régimen general de protección de datos de la UE y aplica dichos principios al tratamiento de datos personales que realizan las instituciones y los organismos de la UE en el ejercicio de sus funciones. Además, establece una autoridad de control independiente encargada de controlar la aplicación de sus disposiciones: el Supervisor Europeo de Protección de Datos (SEPD). El SEPD tiene competencias de control y la obligación de vigilar el tratamiento de datos personales en las instituciones y organismos de la UE, así como de conocer e investigar las reclamaciones por presuntas violaciones de las normas de protección de datos. También asesora a las instituciones y organismos de la UE en todas las cuestiones relativas a la protección de los datos personales, desde propuestas de nueva legislación hasta la elaboración de normas internas sobre tratamiento de datos personales.

En enero de 2017, la Comisión Europea presentó una propuesta de nuevo Reglamento relativo al tratamiento de datos personales por las instituciones de la UE, que derogará el Reglamento vigente. Como en el caso de la reforma de la Directiva sobre la privacidad y las comunicaciones electrónicas, la reforma del Reglamento n.º 45/2001 vendrá a modernizar y armonizar sus disposiciones con el nuevo régimen de protección de datos establecido en virtud del Reglamento general de protección de datos.

El papel del TJUE

El TJUE tiene jurisdicción para determinar si un Estado miembro ha cumplido o no sus obligaciones conforme a la legislación de protección de datos de la UE y para interpretar la legislación de la UE con el fin de asegurar su aplicación efectiva y uniforme en todos los Estados miembros. Desde que se adoptó la Directiva sobre protección de datos en 1995, se ha acumulado un considerable cuerpo de jurisprudencia que aclara el alcance y significado de los principios de protección de datos y el derecho fundamental a la protección de los datos personales consagrado en el artículo 8 de la Carta. Aunque la Directiva ha quedado derogada y hay un nuevo instrumento jurídico en vigor (el Reglamento general de protección de datos), esa jurisprudencia preexistente sigue siendo pertinente y válida para la interpretación y aplicación de los principios de protección de datos de la UE, en la medida en que los principios y conceptos fundamentales de la Directiva sobre protección de datos se mantuvieron en el RGPD.

1.2. Limitaciones al derecho a la protección de los datos personales

Puntos clave

- El derecho a la protección de los datos personales no es un derecho absoluto; puede limitarse si es necesario para alcanzar un objetivo de interés general o para proteger los derechos y libertades de los demás.
- Las condiciones para limitar los derechos al respeto de la vida privada y a la protección de los datos personales están recogidas en el artículo 8 del CEDH y en el artículo 52, apartado 1, de la Carta. Se han desarrollado e interpretado en la jurisprudencia del TEDH y del TJUE.
- En la legislación sobre protección de datos del CdE, el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si:
  - se realiza de conformidad con la ley;
  - sirve a un fin legítimo;
  - respeta la esencia de los derechos y libertades fundamentales;
  - es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo.
- El ordenamiento jurídico de la UE impone condiciones similares a las limitaciones del ejercicio de los derechos fundamentales protegidos por la Carta. La limitación de un derecho fundamental, incluido el derecho a la protección de los datos personales, solo puede ser lícita si:
  - se realiza de conformidad con la ley;
  - respeta la esencia del derecho;
  - es necesaria en virtud del principio de proporcionalidad; y
  - sirve a un objetivo de interés general reconocido por la Unión o a la necesidad de proteger los derechos de los demás.

El derecho fundamental a la protección de los datos personales, con arreglo al artículo 8 de la Carta, no es un derecho absoluto, «sino que debe ser considerado en relación con su función en la sociedad» ([40]). El artículo 52, apartado 1, de la Carta

([40]) Véase, por ejemplo, TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 9 de noviembre de 2010, apartado 48.

reconoce por tanto que se podrán imponer limitaciones al ejercicio de derechos, como las contempladas en los artículos 7 y 8 de la Carta, siempre y cuando dichas limitaciones se establezcan por ley, respeten la esencia de los derechos y libertades en cuestión, respeten el principio de proporcionalidad, sean necesarias y respondan realmente a objetivos de interés general reconocidos por la UE o a la necesidad de proteger los derechos y libertades de otras personas ([41]) Del mismo modo, en el régimen del CEDH, la protección de datos está garantizada por el artículo 8, y el ejercicio de ese derecho puede limitarse cuando sirva a un fin legítimo. Esta sección trata de las condiciones que justifican la injerencia conforme al CEDH, según se interpretan en la jurisprudencia del TEDH, así como a las condiciones para imponer limitaciones lícitas en virtud del artículo 52 de la Carta.

1.2.1. Requisitos para una injerencia justificada con arreglo al CEDH

El tratamiento de datos personales puede constituir una injerencia en el derecho del interesado al respeto de su vida privada, protegido por el artículo 8 del CEDH ([42]). Como se ha explicado anteriormente (véanse las secciones 1.1.1 y 1.1.4.), en contra de lo dispuesto en el ordenamiento jurídico de la UE, el CEDH no afirma que la protección de datos personales sea un derecho fundamental específico. En lugar de ello, la protección de los datos personales forma parte de los derechos protegidos por el derecho al respeto de la vida privada. Por tanto, no cualquier operación que implique el tratamiento de datos personales puede inscribirse en el ámbito de aplicación del artículo 8 del CEDH. Para que se aplique el artículo 8, primero se ha de determinar si se ha lesionado un interés particular o la vida privada de una persona. A través de su jurisprudencia, el TEDH ha tratado la idea de «vida privada» como un concepto amplio, que comprende incluso aspectos de la vida profesional y de la conducta pública. También ha dictaminado que la protección de los datos personales es una parte importante del derecho al respeto de la vida privada. Sin embargo, pese a esta interpretación amplia del concepto de vida privada, no todos los tipos de tratamiento llevarían *per se* a lesionar los derechos protegidos por el artículo 8.

Cuando el TEDH considere que una operación concreta de tratamiento de datos personales afecta al derecho de las personas físicas al respeto de la vida privada, examinará si la injerencia está justificada. El respeto de la vida privada no es un derecho

([41]) Ibíd., apartado 50.

([42]) TEDH, *S. y Marper contra Reino Unido* [GS], números 30562/04 y 30566/04, 8 de diciembre de 2008, apartado 67.

absoluto, sino que debe ponderarse y conciliarse con otros intereses y derechos legítimos, ya sean de otras personas (intereses privados) o de una sociedad en su conjunto (intereses públicos).

Las condiciones acumulativas en las que podría justificarse una injerencia son:

De conformidad con la ley

Según la jurisprudencia del TEDH, la injerencia se realizará de conformidad con la ley si está basada en una disposición del Derecho nacional que posea determinadas características. La ley deberá ser «accesible para las personas a las cuales concierna y previsible en cuanto a sus efectos» ([43]). Una norma es previsible «si se formula con la suficiente precisión que permita al ciudadano —si es necesario con asesoramiento apropiado— adecuar su conducta» ([44]). Además, «[e]l grado de precisión exigible de "la ley" en este sentido dependerá de la materia concreta» ([45]).

Ejemplos: *En Rotaru contra Rumanía* [GS] ([46]), el demandante denunció que la tenencia y uso de un expediente con sus datos personales por el Servicio de Inteligencia rumano suponía una violación de su derecho al respeto de su vida privada. El TEDH dictaminó que, si bien la legislación nacional permitía la recopilación, grabación y archivo en expedientes secretos de información que afectase a la seguridad nacional, no establecía límite alguno al ejercicio de dichas facultades, que quedaba a criterio de las autoridades. Por ejemplo, la legislación nacional no definía el tipo de información que se podía tratar, ni las categorías de personas contra las que podían adoptarse medidas de vigilancia, ni las circunstancias en que podían adoptarse dichas medidas ni

([43]) TEDH, *Amann contra Suiza* [GS], n.º 27798/95, 16 de febrero de 2000, apdo. 50; véase también TEDH, *Kopp contra Suiza*, n.º 23224/94, 25 de marzo de 1998, apdo. 55; y TEDH, *Iordachi y otros contra Moldavia*, n.º 25198/02, 10 de febrero de 2009, apdo. 50.

([44]) TEDH, *Amann contra Suiza* [GS], n.º 27798/95, 16 de febrero de 2000, apdo. 56; véase, asimismo, TEDH, *Malone contra Reino Unido*, n.º 8691/79, 2 de agosto de 1984, apdo. 66; TEDH, *Silver y otros contra Reino Unido*, números 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 de marzo de 1983, apdo. 88.

([45]) TEDH, *The Sunday Times contra Reino Unido*, n.º 6538/74, 26 de abril de 1979, apdo. 49; véase, asimismo, TEDH, *Silver y otros contra Reino Unido*, números 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 de marzo de 1983, apdo. 88.

([46]) TEDH, *Rotaru contra Rumanía* [GS], n.º 28341/95, 4 de mayo de 2000, apdo. 57; véase asimismo TEDH, *Association for European Integration and Human Rights y Ekimdzhiev contra Bulgaria*, n.º 62540/00, 28 de junio de 2007; TEDH, *Shimovolos contra Rusia*, n.º 30194/09, 21 de junio de 2011; y TEDH, *Vetter contra Francia*, n.º 59842/00, 31 de mayo de 2005.

el procedimiento que debía seguirse. Por tanto, el Tribunal concluyó que la legislación nacional no cumplía el requisito de previsibilidad establecido en el artículo 8 del CEDH y que se había infringido lo dispuesto en dicho artículo.

En *Taylor-Sabori contra Reino Unido* ([47]), el demandante había sido objeto de vigilancia por parte de la policía. Utilizando una «copia» del buscapersonas del demandante, la policía pudo intervenir los mensajes que se le habían enviado a dicho demandante. Este fue posteriormente detenido y acusado de conspiración para suministrar una droga controlada. La acusación incluía notas escritas contemporáneas de los mensajes del buscapersonas, que habían sido transcritas por la policía. Sin embargo, en el momento del juicio al demandante, no existía en la legislación británica ninguna disposición que regulase la intervención de comunicaciones transmitidas a través de un sistema de telecomunicaciones privado. La injerencia en sus derechos no se había realizado, por lo tanto, «de conformidad con la ley». El TEDH concluyó que esto constituía una violación del artículo 8 del CEDH.

Vukota-Bojić contra Suiza ([48]) trataba de la vigilancia secreta de un demandante de la Seguridad Social por parte de investigadores privados contratados por su compañía de seguros. El TEDH dictaminó que, si bien la medida de vigilancia objeto de la demanda había sido ordenada por una compañía de seguros privada, el Estado había otorgado a dicha compañía el derecho de ofrecer prestaciones derivadas del seguro de enfermedad obligatorio y cobrar primas de seguro. El Estado no podía exonerarse a sí mismo de responsabilidad en virtud del Convenio delegando sus obligaciones en particulares o entidades privadas. La legislación nacional debía establecer garantías suficientes contra el abuso de la injerencia en los derechos recogidos en el artículo 8 del CEDH para que fuera «de conformidad con la ley». En el caso que nos ocupa, el TEDH concluyó que había existido una violación del artículo 8 del CEDH, porque la legislación nacional no había indicado con suficiente claridad el alcance y la forma de ejercicio de la discrecionalidad otorgada a las compañías de seguros que actúan a modo de autoridades públicas en los litigios de seguros para llevar a cabo vigilancias secretas de personas aseguradas. En particular, no incluía suficientes garantías contra el abuso.

([47]) TEDH, *Taylor-Sabori contra Reino Unido*, n.º 47114/99, 22 de octubre de 2002.

([48]) TEDH, *Vukota-Bojić contra Suiza*, n.º 61838/10, 18 de octubre de 2016, apdo. 77.

Servir a un fin legítimo

El fin legítimo puede ser tanto uno de los intereses públicos mencionados como la protección de los derechos y libertades de los demás. Fines legítimos que podrían justificar una injerencia son, en virtud del artículo 8, apartado 2, del CEDH, los intereses de la seguridad nacional, la seguridad pública o el bienestar económico de un país, la prevención de delitos o desórdenes, la protección de la salud o de la moral, y la protección de los derechos y libertades de los demás.

Ejemplo: En *Peck contra Reino Unido* ([49]), el demandante había intentado suicidarse en la calle cortándose las muñecas, sin darse cuenta de que una cámara de CCTV le estaba filmando. La policía, que estaba observando las cámaras de vigilancia de CCTV, le rescató y transmitió la grabación a los medios de comunicación, que la publicaron sin ocultar el rostro del demandante. El TEDH consideró que no existían motivos relevantes ni suficientes que pudieran justificar la difusión directa al público de la grabación por parte de las autoridades sin haber obtenido el consentimiento del demandante ni ocultar su identidad. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

Necesaria en una sociedad democrática

El TEDH ha declarado que «el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue» ([50]). A la hora de valorar si una medida es necesaria para dar respuesta a una necesidad acuciante, el TEDH examina su pertinencia y su idoneidad en relación con el objetivo perseguido. Con este fin, puede tomar en consideración si la injerencia trata de resolver un problema que, de no resolverse, podría tener efectos perjudiciales para la sociedad, si existen pruebas de que dicha injerencia podría mitigar dichos efectos perjudiciales y cuáles son los puntos de vista de la sociedad en general sobre el problema ([51]). Por ejemplo, la recopilación y la conservación de datos personales por los servicios de seguridad de determinadas personas que tienen vínculos con movimientos terroristas sería una injerencia en el

([49]) TEDH, *Peck contra Reino Unido*, n.º 44647/98, 28 de enero de 2003, apdo. 85.

([50]) TEDH, *Leander contra Suecia*, n.º 9248/81, 26 de marzo de 1987, apdo. 58.

([51]) Grupo de Trabajo de Protección de Datos del Artículo 29 (Grupo de Trabajo del Artículo 29) (2014), *Dictamen sobre la aplicación de los conceptos de necesidad y proporcionalidad y protección de datos en el sector de los cuerpos de seguridad*, WP 211, Bruselas, 27 de febrero de 2014, pp. 7-8.

derecho de las personas al respeto de la vida privada que, no obstante, sirve a una necesidad grave e imperiosa: la seguridad nacional y la lucha contra el terrorismo. Para cumplir el criterio de necesidad, la injerencia también ha de ser proporcionada. En la jurisprudencia del TEDH, la proporcionalidad se contempla dentro del concepto de necesidad. La proporcionalidad requiere que la injerencia en los derechos protegidos por el CEDH no vaya más lejos de lo necesario para cumplir el fin legítimo perseguido. Entre los factores importantes que deben tenerse en cuenta para determinar si se cumple el criterio de proporcionalidad figuran el alcance de la injerencia, en particular el número de personas afectadas, y las garantías o advertencias establecidas para limitar su alcance o sus efectos perjudiciales para los derechos de las personas ([52]).

Ejemplo: En *Khelili contra Suiza* ([53]), durante un control policial, la policía descubrió que la demandante llevaba tarjetas de visita en las que podía leerse: «Mujer bonita y agradable, bien entrada en la treintena, desearía encontrar a un hombre para tomar una copa o salir de vez en cuando. N.º de teléfono [...]» La demandante alegó que, a raíz de ese descubrimiento, la policía le abrió un expediente como prostituta, una profesión a la que ella había negado dedicarse de forma reiterada. La demandante pidió que se eliminase la palabra «prostituta» de los registros informáticos de la policía. El TEDH reconoció en principio que la conservación de los datos personales de un particular sobre la base de que dicha persona podría cometer otro delito podría ser proporcionada en determinadas circunstancias. Sin embargo, en el caso de la demandante, la alegación de prostitución ilícita parecía demasiado vaga y general, no se apoyaba en hechos concretos ya que aquella jamás había sido condenada por prostitución ilícita y, por lo tanto, no podía considerarse que existiera una «necesidad social imperiosa», en el sentido del artículo 8 del CEDH. En vista de que correspondía a las autoridades demostrar la exactitud de los datos conservados sobre la demandante, así como de la gravedad de la injerencia en los derechos de esta persona, el Tribunal dictaminó que la conservación de la palabra «prostituta» en el expediente policial no había sido necesaria en una sociedad democrática. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

([52]) Ibíd., pp. 9-11.

([53]) TEDH, *Khelili contra Suiza*, n.º 16188/07, 18 de octubre de 2011.

Ejemplo: En *S. y Marper contra Reino Unido* ([54]), los dos demandantes fueron detenidos y acusados de delitos penales. La policía tomó sus impresiones dactilares y muestras de ADN, de acuerdo con lo estipulado por la Ley de policía y pruebas penales. Los demandantes nunca fueron condenados por los delitos: uno fue absuelto en juicio y la acusación penal contra el segundo fue retirada. No obstante, la policía conservó sus impresiones dactilares, perfiles de ADN y muestras celulares en una base de datos y la legislación nacional autorizaba su conservación sin que se aplicase límite de tiempo alguno. Aunque el Reino Unido alegó que la conservación de estos datos era útil para la identificación de futuros delincuentes y, por tanto, servía al fin legítimo de prevención y detección de la delincuencia, el TEDH consideró que la injerencia en el derecho de los demandantes al respeto de su vida privada no estaba justificada. Recordó que los principios básicos de la protección de datos exigen que la conservación de los datos personales sea proporcionada en relación con el fin de la recopilación y que los periodos de conservación deben ser limitados. El Tribunal aceptó que el hecho de ampliar la base de datos para incluir perfiles de ADN no solo de personas condenadas, sino también de todas aquellas personas que hubieran sido sospechosas pero no condenadas, podría haber contribuido a la detección y prevención de la delincuencia en el Reino Unido. Sin embargo, le sorprendió «el carácter genérico e indiscriminado de la facultad de conservación» ([55]).

Dada la abundancia de información genética y de salud que contienen las muestras celulares, la injerencia en el derecho de los demandantes a la vida privada resultaba especialmente invasiva. Se podían tomar impresiones dactilares y muestras de personas detenidas y conservarlas con carácter indefinido en la base de datos policial, fuera cual fuese la naturaleza y gravedad del delito, e incluso por delitos menores no sujetos a condenas de prisión. Más aún, las personas absueltas tenían pocas posibilidades de lograr que sus datos fueran eliminados de la base de datos. Por último, el TEDH tomó en especial consideración el hecho de que uno de los demandantes tuviera once años cuando fue detenido. Conservar los datos personales de un menor que no ha sido condenado puede ser especialmente perjudicial, dada su vulnerabilidad y la importancia de su desarrollo e integración en la

([54]) TEDH, *S. y Marper contra Reino Unido* [GS], números 30562/04 y 30566/04, 4 de diciembre de 2008.

([55]) Ibíd., apartado 119.

sociedad ([56]). El Tribunal dictaminó, por unanimidad, que la conservación de esos datos constituía una injerencia desproporcionada en el derecho a la vida privada que no podía considerarse necesaria en una sociedad democrática.

Ejemplo: En *Leander contra Suecia* ([57]), el TEDH resolvió que el control secreto de personas que se postulan a puestos de importancia de la seguridad nacional no es contrario, en sí mismo, al requisito de ser necesario en una sociedad democrática. Las garantías específicas establecidas en la legislación nacional para proteger los intereses del titular de los datos —por ejemplo, los controles ejercidos por el Parlamento y el Ministro de Justicia— llevaron al TEDH a concluir que el sistema de control de personal de Suecia cumplía los requisitos del artículo 8, apartado 2, del CEDH. Visto el amplio margen de apreciación de que disponía, el Estado demandado estaba autorizado a considerar que, en el caso del demandante, los intereses de la seguridad nacional prevalecían sobre los intereses individuales. El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH.

1.2.2. Condiciones para imponer limitaciones lícitas con arreglo a la Carta de los Derechos Fundamentales de la Unión Europea

La estructura y el texto de la Carta son distintos de los del CEDH. La Carta no utiliza el concepto de injerencia en los derechos garantizados, pero incluye una disposición sobre la limitación del ejercicio de los derechos y libertades en ella reconocidos.

De conformidad con el artículo 52, apartado 1, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta y, en consecuencia, del ejercicio del derecho a la protección de los datos personales, se admitirá únicamente si:

- está establecida por la ley; y
- respeta el contenido esencial de dichos derechos y libertades; y

([56]) Ibíd., apartado 124.

([57]) TEDH, *Leander contra Suecia*, n.º 9248/81, 26 de marzo de 1987, apartados 59 y 67.

- es necesaria en virtud del principio de proporcionalidad ([58]); y

- responden a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de los demás.

Dado que la protección de los datos personales es un derecho fundamental específico e independiente en el ordenamiento jurídico de la UE, protegido con arreglo al artículo 8 de la Carta, cualquier tratamiento de datos personales constituye de por sí una injerencia en este derecho. No importa si los datos personales en cuestión tienen que ver con la vida privada de una persona física, si son sensibles o si se ha molestado a los interesados de algún modo. Para que sea lícita, la injerencia ha de cumplir todas las condiciones establecidas en el artículo 52, apartado 1, de la Carta.

Establecidas por la ley

Las limitaciones al derecho a la protección de los datos personales deben estar establecidas por la ley. Este requisito implica que las limitaciones deben estar basadas en el fundamento jurídico de que sean adecuadamente accesibles y previsibles y formuladas con suficiente precisión para que las personas puedan entender sus obligaciones y adecuar su conducta. La base jurídica también debe definir con claridad el alcance y la forma de ejercicio de la facultad por las autoridades competentes para proteger a las personas contra injerencias arbitrarias. Esta interpretación es similar al requisito de «injerencia lícita» establecido en la jurisprudencia del TEDH ([59]) y se ha argumentado que la expresión «establecida por la ley» que se utiliza en la Carta debe tener el mismo significado que se le atribuye en relación con el CEDH ([60]). La jurisprudencia del TEDH —y especialmente el concepto de «calidad de la ley» que ha desarrollado a lo largo de los años— es una consideración pertinente que debe tener en cuenta el TJUE en su interpretación del ámbito de aplicación del artículo 52, apartado 1, de la Carta ([61]).

([58]) Sobre la determinación de la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales, véase: SEPD (2017), *Herramientas para determinar la necesidad*, Bruselas, 11 de abril de 2017.

([59]) SEPD (2017), *Herramientas para determinar la necesidad*, Bruselas, 11 de abril de 2017, p. 4; véase también TJUE, *Dictamen 1/15 del Tribunal de Justicia (Gran Sala)*, 26 de julio de 2017.

([60]) TJUE, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB contra Post- och telestyrelsen y Secretary of State for the Home Department contra Tom Watson y otros [GS] *Conclusiones del Abogado General Saugmandsgaard Øe*, presentadas el 19 de julio de 2016, apdo. 140.

([61]) TJUE, C-70/10, *Scarlet Extended SA contra Société belge des auteurs compositeurs et éditeurs (SABAM)*, *Conclusiones del Abogado General Cruz Villalón*, presentadas el 14 de abril de 2011, apdo. 100.

Respetar el contenido esencial del derecho

En el ordenamiento jurídico de la Unión, cualquier limitación de los derechos fundamentales protegidos por la Carta debe respetar el contenido esencial de tales derechos. Esto significa que no son justificables las limitaciones que sean tan amplias e invasivas que vacíen un derecho fundamental de su contenido básico. Si se lesiona el contenido esencial del derecho, la limitación deberá considerarse ilícita, sin necesidad de valorar si sirve a un objetivo de interés general y satisface los criterios de necesidad y proporcionalidad.

Ejemplo: El asunto *Schrems* ([62]) trataba de la protección de las personas en relación con la transferencia de sus datos personales a terceros países: en este caso, los Estados Unidos. Schrems, un ciudadano austriaco que había sido usuario de Facebook durante varios años, presentó una reclamación a la autoridad irlandesa de control de la protección de datos para denunciar la transferencia de sus datos personales por parte de la filial irlandesa de Facebook a Facebook Inc. y a los servidores radicados en los Estados Unidos, donde fueron objeto de tratamiento. Alegó que, en vista de las revelaciones realizadas en 2013 por el estadounidense Edward Snowden en relación con las actividades de vigilancia de los servicios de vigilancia de los EE. UU., la legislación y la práctica de ese país no ofrecía protección suficiente a los datos personales transferidos a su territorio. Snowden había revelado que la Agencia de Seguridad Nacional tenía acceso directo a los servidores de empresas como Facebook y podía leer el contenido de los chats y los mensajes privados.

Las transferencias de datos a los EE. UU. se basaron en una decisión adoptada por la Comisión en 2000 sobre el carácter adecuado de la protección, que permitía dichas transferencias a empresas estadounidenses que autocertificasen que protegerían los datos personales transferidos desde la Unión Europea y cumplirían los llamados «principios de puerto seguro». Cuando se presentó el asunto ante el TJUE, este examinó la validez de la decisión adoptada por la Comisión en virtud de la Carta y recordó que la protección de los derechos fundamentales en la Unión exige que las excepciones y limitaciones de tales derechos no excedan de lo estrictamente necesario. El TJUE consideró que la legislación que permite que las

([62]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commisioner* [GS], 6 de octubre de 2015.

autoridades públicas tengan acceso, con carácter general, al contenido de las comunicaciones electrónicas «lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta». Ese derecho dejaría de tener sentido si se autorizase a las autoridades públicas de los Estados Unidos a obtener acceso a las comunicaciones de manera aleatoria, sin ninguna justificación objetiva fundada en razones concretas de seguridad nacional o prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que esas prácticas de vigilancia se rodeasen de garantías adecuadas contra el abuso de poder.

Además, el TJUE observó que «una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión» es incompatible con el derecho fundamental a la tutela judicial efectiva (artículo 47 de la Carta). De este modo, la Decisión de puerto seguro no garantizaba un nivel de protección de los derechos fundamentales por parte de los Estados Unidos sustancialmente equivalente al garantizado en la Unión por la Directiva interpretada a la luz de la Carta. En consecuencia, el TJUE anuló la Decisión ([63]).

Ejemplo: En *Digital Rights Ireland* ([64]) el TJUE examinó la compatibilidad de la Directiva 2006/24/CE (Directiva de conservación de datos) con los artículos 7 y 8 de la Carta. Esta Directiva obligaba a los proveedores de servicios de comunicaciones electrónicas a conservar los datos de tráfico y localización durante un mínimo de seis meses y un máximo de veinticuatro meses, así como a permitir el acceso de las autoridades nacionales competentes a dichos datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves. La Directiva no permitía conservar el contenido de las comunicaciones electrónicas. El TJUE observó que algunos de los datos que los proveedores debían conservar de conformidad con la Directiva

([63]) La resolución del TJUE de invalidar la Decisión 520/2000/CE de la Comisión también se basó en otros motivos que se examinarán en otras secciones del presente manual. En particular, el TJUE consideró que esa Decisión limitaba de forma ilícita las competencias de las autoridades nacionales de control de la protección de datos. Además, de conformidad con el régimen de puerto seguro, las personas interesadas no disponían de recursos jurisdiccionales para el caso de que desearan acceder a los datos personales que les concerniesen o conseguir su rectificación o supresión. Por tanto, también se lesionaba el contenido esencial del derecho fundamental a la tutela judicial efectiva, consagrado en el artículo 47 de la Carta.

([64]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros* y *Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.

eran los necesarios para rastrear e identificar el origen y el destino de una comunicación, la fecha, hora y duración de la comunicación, el número de teléfono de llamada, los números marcados y las direcciones IP. Estos datos, «considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan».

De este modo, la conservación de datos personales con arreglo a la Directiva constituía una injerencia especialmente grave en los derechos a la privacidad y a la protección de los datos personales. Sin embargo, el TJUE dictaminó que la injerencia no vulneraba el contenido esencial de esos derechos. En lo que respecta al derecho a la vida privada, no se vulneraba su contenido esencial porque la Directiva no permitía conocer el contenido de las comunicaciones electrónicas como tal. Tampoco se vulneraba el contenido esencial del derecho a la protección de los datos de carácter personal, ya que la Directiva obligaba a los proveedores de servicios de comunicaciones electrónicas a respetar determinados principios de protección y seguridad de los datos y adoptar medidas técnicas y organizativas adecuadas para tal fin.

Necesidad y proporcionalidad

El artículo 52, apartado 1, de la Carta establece que, respetando el principio de proporcionalidad, solo se podrán introducir limitaciones al ejercicio de los derechos y libertades fundamentales reconocidos en la Carta cuando sean necesarias.

Una limitación puede ser **necesaria** si existe la necesidad de adoptar medidas para alcanzar un objetivo de interés general, pero la necesidad, según la interpretación del TJUE, implica además que las medidas adoptadas deben ser menos invasivas que otras opciones para alcanzar el mismo objetivo. En relación con las limitaciones del derecho al respeto de la vida privada y del derecho a la protección de los datos personales, el TJUE aplica un criterio de necesidad estricto y exige que «las excepciones y limitaciones de tales derechos no excedan de lo estrictamente necesario». Si una limitación se considera estrictamente necesaria, también será necesario determinar si es proporcionada.

La **proporcionalidad** implica que las ventajas derivadas de la limitación deben ser superiores a las desventajas que acarree para el ejercicio de los derechos fundamentales en cuestión ([65]). Para reducir las desventajas y los riesgos del disfrute de los derechos a la privacidad y a la protección de los datos personales, es importante que las limitaciones vayan acompañadas de garantías adecuadas.

Ejemplo: En *Volker und Markus Schecke* ([66]), el TJUE concluyó que al imponer la obligación de publicar datos de carácter personal de todas las personas físicas beneficiarias de ayudas de determinados fondos agrícolas, sin establecer distinciones en función de criterios pertinentes, tales como los periodos durante los cuales dichas personas percibieron estas ayudas, su frecuencia o, incluso, el tipo y magnitud de las mismas, el Consejo y la Comisión habían sobrepasado los límites que impone el principio de proporcionalidad.

Por lo tanto, el TJUE consideró que procedía declarar inválidas determinadas disposiciones del Reglamento (CE) n.º 1290/2005 y declarar inválido el Reglamento (CE) n.º 259/2008 en su totalidad ([67]).

Ejemplo: En *Digital Rights Ireland* ([68]), el TJUE dictaminó que la injerencia en el derecho al respeto de la vida privada causada por la Directiva de conservación de datos no vulneraba el contenido esencial de ese derecho, ya que prohibía la conservación del contenido de las comunicaciones electrónicas. Sin embargo, concluyó que la Directiva era incompatible con los artículos 7 y 8 de la Carta y la declaró inválida. Dado que los datos de tráfico y localización, agregados y considerados en su conjunto, podían ser analizados y ofrecer una imagen detallada de la vida privada de las personas, constituían una grave injerencia en esos derechos. El TJUE tuvo en cuenta que la Directiva obligaba a conservar todos los metadatos relativos a telefonía fija,

([65]) SEPD (2017), *Herramientas para determinar la necesidad*, p. 5.

([66]) TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 9 de noviembre de 2010, apartados 89 y 86.

([67]) Reglamento (CE) n.º 1290/2005 de la Comisión, de 21 de junio de 2005, sobre la financiación de la política agrícola común, DO 2005 L 209; Reglamento (CE) n.º 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento (CE) n.º 1290/2005 del Consejo en lo que se refiere a la publicación de información sobre los beneficiarios de fondos procedentes del Fondo Europeo Agrícola de Garantía (FEAGA) y del Fondo Europeo Agrícola de Desarrollo Rural (Feader), DO 2008 L 76.

([68]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd v. contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros, 8 de abril de 2014, apartado 39.*

telefonía móvil, acceso a internet, correo electrónico por internet y telefonía por internet aplicables a todos los medios de comunicación electrónica, cuyo uso está muy extendido en la vida cotidiana de los ciudadanos. En la práctica, esto constituía una injerencia que afectaba a toda la población europea. Considerando el alcance y la gravedad de esta injerencia, la conservación de los datos de tráfico y localización solo podía justificarse, según el TJUE, con el fin de combatir los delitos graves. Además, la Directiva no establecía ningún criterio objetivo que garantizase que el acceso de las autoridades nacionales competentes a los datos conservados se limitase a lo estrictamente necesario. Más aún, tampoco precisaba condiciones materiales y de procedimiento que regulasen el acceso y uso de los datos conservados por parte de las autoridades nacionales, que no se supeditaban a un control previo efectuado por un órgano jurisdiccional u otro órgano autónomo.

El TJUE llegó a una conclusión similar en los asuntos acumulados *Tele2 Sverige AB contra Post- och telestyrelsen* y *Secretary of State for the Home Department contra Tom Watson y otros* [GS] ([69]). Estos asuntos trataban de la conservación de datos de tráfico y localización de «todos los abonados y usuarios registrados y [...] todos los medios de comunicación electrónica» sin «diferenciación, limitación o excepción en función del objetivo que se pretende lograr» ([70]). En el asunto que nos ocupa, la conservación de los datos de una persona no estaba condicionada a que dicha persona estuviera vinculada o no, de manera directa o indirecta, con infracciones penales graves, o que sus comunicaciones fueran o no pertinentes para la seguridad nacional. En vista de que no se exigía una vinculación entre los datos conservados y una amenaza para la seguridad pública o un periodo de tiempo o restricciones geográficas, el TJUE concluyó que la legislación nacional excedía de los límites de lo estrictamente necesario con el fin de combatir los delitos graves ([71]).

El Supervisor Europeo de Protección de Datos adopta un enfoque similar, en lo que respecta a la necesidad, en sus *Herramientas para determinar la necesidad* ([72]). Esta

([69]) TJUE, asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB contra Post- och telestyrelsen y Secretary of State for the Home Department contra Tom Watson y otros*[GS], 21 de diciembre de 2016, apartados 105-106.

([70]) Ibíd., apartado 105.

([71]) Ibíd., apartado 107.

([72]) SEPD (2017), *Herramientas para determinar la necesidad*, Bruselas, 11 de abril de 2017.

publicación tiene por objeto ayudar a determinar si las medidas propuestas cumplen con la legislación sobre protección de datos de la UE. Su finalidad es preparar mejor a los reguladores y legisladores de la UE que tienen la responsabilidad de preparar o examinar medidas que conlleven el tratamiento de datos personales y limiten el derecho a la protección de los datos personales y otros derechos y libertades reconocidos en la Carta.

Objetivos de interés general

Para que esté justificada, toda limitación del ejercicio de los derechos reconocidos en la Carta debe además responder efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de los demás. En relación con la necesidad de proteger los derechos y libertades de los demás, el derecho a la protección de los datos personales suele interactuar con otros derechos fundamentales. En la sección 1.3 se ofrece un análisis detallado de tales interacciones. En cuanto a los objetivos de interés general, entre ellos se incluyen los objetivos generales de la UE recogidos en el artículo 3 del Tratado de la Unión Europea (TUE), como promover la paz y el bienestar de sus pueblos, la justicia y la protección sociales y la creación de un espacio de libertad, seguridad y justicia en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de prevención y lucha contra la delincuencia, así como otros objetivos e intereses protegidos por disposiciones específicas de los Tratados ([73]). El Reglamento general de protección de datos especifica además el artículo 52, apartado 1, de la Carta en este sentido: el artículo 23, apartado 1, del Reglamento enumera una serie de objetivos de interés general considerados legítimos para limitar los derechos de las personas, siempre que tal limitación respete el contenido esencial del derecho a la protección de los datos personales y sea necesaria y proporcionada. La seguridad y la defensa del Estado, la prevención de la delincuencia, la protección de importantes intereses económicos y financieros de la UE o de los Estados miembros, la salud pública y la seguridad social están entre los intereses públicos recogidos en el Reglamento.

Es importante definir y explicar el objetivo de interés general que persiga la limitación con suficiente grado de detalle, ya que la necesidad de dicha limitación se determinará en virtud de ese contexto. Resulta esencial describir con claridad y detalle el objetivo de la limitación y las medidas propuestas para que se pueda

([73]) Explicaciones sobre la Carta de los Derechos Fundamentales (2007/CE 303/02), DO 2007 n.º C 303, pp. 17-35.

determinar si es necesaria ([74]). El objetivo perseguido va estrechamente ligado a la necesidad y proporcionalidad de la limitación.

Ejemplo: *Schwarz contra Stadt Bochum* ([75]) trataba de las limitaciones del derecho al respeto de la vida privada y del derecho a la protección de los datos personales derivadas de la toma y conservación de impresiones dactilares cuando las autoridades de los Estados miembros expiden pasaportes ([76]). El demandante solicitó un pasaporte al Stadt Bochum, pero se negó a que le tomasen las impresiones dactilares; por esta razón, el Stadt Bochum denegó su solicitud de pasaporte. Entonces interpuso recurso ante un órgano jurisdiccional alemán con objeto de que se le expidiese un pasaporte sin tomar sus impresiones dactilares. El órgano jurisdiccional alemán remitió el asunto al TJUE, preguntando si el artículo 1, apartado 2, del Reglamento 2252/2004 sobre normas para las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje expedidos por los Estados miembros debía considerarse válido.

El TJUE señaló que las impresiones dactilares **están comprendidas en el concepto de datos personales**, ya que contienen objetivamente información única sobre personas físicas que permite su identificación precisa, de modo que la toma y conservación de impresiones dactilares constituye tratamiento de datos personales. Este tratamiento, que se rige por el artículo 1, apartado 2, del Reglamento n.º 2252/2004, constituye una vulneración de los derechos al respeto de la vida privada y a la protección de los datos personales ([77]). Sin embargo, el artículo 52, apartado 1, de la Carta permite limitaciones del ejercicio de dichos derechos, siempre que estén establecidas por la ley, respeten el contenido esencial de esos derechos y, dentro del respeto del principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de los demás.

En el asunto que nos ocupa, el TJUE observó en primer lugar que la limitación derivada de la toma y conservación de impresiones dactilares en el proceso de expedición de pasaportes debía considerarse **establecida por la ley**,

([74]) SEPD (2017), *Herramientas para determinar la necesidad*, Bruselas, 11 de abril de 2017, p. 4.

([75]) TJUE, C-291/12, *Michael Schwarz contra Stadt Bochum*, 17 de octubre de 2013.

([76]) Ibíd., apartados 33-36.

([77]) Ibíd., apartados 27-30.

ya que estas operaciones están recogidas en el artículo 1, apartado 2, del Reglamento n.º 2252/2004. En segundo lugar, este Reglamento se diseñó para prevenir la falsificación de pasaportes y su uso fraudulento. De este modo, el artículo 1, apartado 2, tiene la finalidad de prevenir, entre otras cosas, la entrada ilegal de personas en el territorio de la Unión y, por tanto, persigue un objetivo de interés general reconocido por la Unión. En tercer lugar, de los elementos de que disponía el TJUE no se deducía —ni se había alegado siquiera— que las limitaciones en el caso de autos del ejercicio de estos derechos no respetasen el contenido esencial de dichos derechos. En cuarto lugar, la conservación de impresiones dactilares en un dispositivo de almacenamiento dotado de fuertes medidas de seguridad como el establecido por esa disposición requiere sofisticación técnica. Esta conservación puede reducir el riesgo de falsificación de pasaportes y facilitar la tarea de las autoridades encargadas de examinar su autenticidad en las fronteras de la Unión. El hecho de que el método no sea enteramente fiable no es decisivo. Aunque el método no excluya completamente las admisiones de personas no autorizadas, basta con que reduzca considerablemente el riesgo de tales admisiones. Habida cuenta de las consideraciones anteriores, el TJUE dictaminó que la toma y conservación de impresiones dactilares mencionada en el artículo 1, apartado 2, del Reglamento n.º 2252/2004 era idónea para alcanzar los objetivos perseguidos por dicho Reglamento y, por extensión, el objetivo de impedir la entrada ilegal de personas en el territorio de la Unión ([78]).

Seguidamente, el TJUE valoró si este tratamiento de datos personales es **necesario**, señalando que la acción en cuestión consiste únicamente en captar la impresión dactilar de dos dedos, los cuales están, además, normalmente a la vista de los demás, de modo que no se trata de una operación que revista un carácter íntimo. Tal operación tampoco supone un inconveniente físico o psíquico particular para el interesado, al igual que sucede con la toma de su imagen facial. Por otro lado, es preciso subrayar que la única alternativa real a la toma de las impresiones dactilares que se expuso en el procedimiento ante el Tribunal era la captación de una imagen del iris del ojo. Ninguno de los documentos presentados al TJUE indicaba que este último procedimiento vulnerara en menor medida los derechos reconocidos por los artículos 7 y 8 de la Carta que la toma de impresiones dactilares. Además, en cuanto a la eficacia de estos dos últimos métodos, consta que

([78]) Ibíd., apartados 35-45.

el grado de desarrollo tecnológico del método basado en el reconocimiento del iris es menor que el del método basado en las impresiones dactilares, es en la actualidad sensiblemente más oneroso que el procedimiento de comparación de impresiones dactilares y, por ello, es menos apto para un uso generalizado. En consecuencia, no se había puesto en conocimiento del TJUE la existencia de medidas que contribuyesen, con la suficiente eficacia, al objetivo de proteger los pasaportes contra su uso fraudulento vulnerando de forma menos grave los derechos reconocidos por los artículos 7 y 8 de la Carta que el método basado en las impresiones dactilares ([79]).

El TJUE observó que el artículo 4, apartado 3, del Reglamento n.º 2252/2004 dispone expresamente que las impresiones dactilares solo podrán utilizarse con el único fin de verificar la autenticidad del pasaporte y la identidad de su titular, mientras que el artículo 1, apartado 2, del Reglamento no contempla la conservación de las impresiones dactilares en un medio distinto del propio pasaporte, que pertenece exclusivamente a su titular. Es decir, el Reglamento no ofrece una base jurídica al almacenamiento centralizado de los datos recabados en su virtud o a la utilización de tales datos con fines distintos al de impedir la entrada ilegal de personas en el territorio de la Unión ([80]). En atención a todas las consideraciones anteriores, el TJUE concluyó que el examen de la cuestión prejudicial no había puesto de manifiesto ningún elemento que pudiera afectar a la validez del artículo 1, apartado 2, del Reglamento n.º 2252/2004.

Relación entre la Carta y el CEDH

Pese a que se expresan con diferente texto, las condiciones para la licitud de las limitaciones de los derechos establecidas en el artículo 52, apartado 1, de la Carta recuerdan a las del artículo 8, apartado 2, del CEDH relativo al derecho al respeto de la vida privada. En su jurisprudencia, el TUE y el TEDH se refieren a menudo a las sentencias respectivas, como parte del diálogo constante entre ambos tribunales en busca de una interpretación armonizada de la normativa de protección de datos. El artículo 52, apartado 3, de la Carta establece que «[e]n la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio».

([79]) TJUE, C-291/12, *Michael Schwarz contra Stadt Bochum*, 17 de octubre de 2013, apartados 46-53.

([80]) Ibíd., apartados 56-61.

Sin embargo, el artículo 8 de la Carta no se corresponde directamente con ningún artículo del CEDH ([81]). El artículo 52, apartado 3, de la Carta se refiere al contenido y alcance de los derechos protegidos por cada ordenamiento jurídico, más que a las condiciones para su limitación. Sin embargo, en vista del contexto general de diálogo y cooperación entre ambos tribunales, el TJUE puede tener en cuenta en sus análisis los criterios de licitud de las limitaciones en virtud del artículo 8 del CEDH, según la interpretación del TEDH. También puede darse la situación contraria, por la que el TEDH puede hacer referencia a las condiciones de licitud de las limitaciones recogidas en la Carta. En cualquier caso, también habrá que tener en cuenta que en el CEDH no existe un equivalente perfecto del artículo 8 de la Carta que se refiera a la protección de los datos personales y, en particular, a los derechos del interesado, a los motivos legítimos para el tratamiento de datos personales y al control por parte de una autoridad independiente. Algunos componentes del artículo 8 de la Carta pueden fundamentarse en la jurisprudencia del TEDH sentada en virtud del artículo 8 del CEDH y en relación con el Convenio 108 ([82]). Este vínculo garantiza la existencia de una inspiración mutua entre el TJUE y el TEDH en materias relacionadas con la protección de datos.

1.3. Interacción con otros derechos e intereses legítimos

Puntos clave

- El derecho a la protección de los datos suele interactuar con otros derechos, como la libertad de expresión y el derecho a recibir y comunicar información.
- Esta interacción suele ser ambivalente: aunque hay situaciones en que el derecho a la protección de los datos personales entra en conflicto con un derecho específico, también hay situaciones en que el derecho a la protección de los datos personales garantiza efectivamente el respeto de ese mismo derecho específico. Así ocurre, por ejemplo, en el caso de la libertad de expresión, dado que el secreto profesional es un componente del derecho al respeto de la vida privada.
- La necesidad de proteger los derechos y libertades de los demás es uno de los criterios utilizados para determinar la licitud de la limitación del derecho a la protección de los datos personales.

([81]) SEPD (2017), *Herramientas para determinar la necesidad*, Bruselas, 11 de abril de 2017, p. 6.

([82]) Explicaciones sobre la Carta Europea de Derechos Fundamentales (2007/C 303/02), artículo 8.

- Cuando hay diferentes derechos enfrentados, los órganos jurisdiccionales deben realizar un ejercicio de ponderación para conciliarlos.
- El Reglamento general de protección de datos obliga a los Estados miembros a conciliar el derecho a la protección de los datos personales con la libertad de expresión y de información.
- Los Estados miembros también pueden adoptar normas específicas en su Derecho nacional para conciliar el derecho a la protección de los datos personales con el acceso público a documentos públicos y las obligaciones de secreto profesional.

El derecho a la protección de los datos personales no es un derecho absoluto; las condiciones para la licitud de las limitaciones de este derecho se han detallado anteriormente. Uno de los criterios de licitud de las limitaciones de derechos, reconocidos tanto en el Derecho del CdE como en el Derecho de la UE, es que la injerencia en la protección de datos sea necesaria para la protección de los derechos y libertades de los demás. Cuando la protección de datos interactúa con otros derechos, tanto el TEDH como el TJUE han declarado de forma reiterada que es necesario realizar un ejercicio de ponderación con otros derechos en la aplicación e interpretación del artículo 8 del CEDH y del artículo 8 de la Carta ([83]). Para ilustrar cómo se lleva a cabo esta ponderación con el fin de alcanzar un equilibrio se ofrecen varios ejemplos importantes.

Además del ejercicio de ponderación realizado por estos órganos jurisdiccionales, los Estados pueden adoptar, si es necesario, legislación para conciliar el derecho a la protección de los datos personales con otros derechos. Por esta razón, el Reglamento general de protección de datos contempla una serie de excepciones en el ámbito nacional.

Con respecto a la libertad de expresión, el RGPD obliga a los Estados miembros a conciliar por ley «el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria» ([84]). Los Estados miembros también pueden adoptar leyes para

([83]) TEDH, *Von Hannover contra Alemania (n.º 2)* [GS], números 40660/08 y 60641/08, 7 de febrero de 2012; TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 24 de noviembre de 2011, apartado 48; TJUE, C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU* [GS], 29 de enero de 2008, apartado 68.

([84]) RGPD, artículo 85.

conciliar la protección de datos con el acceso público a documentos oficiales y con las obligaciones de secreto profesional protegidas como una forma del derecho al respeto de la vida privada ([85]).

1.3.1. Libertad de expresión

Uno de los derechos que interactúa de manera más significativa con el derecho a la protección de datos es el derecho a la libertad de expresión.

La libertad de expresión está protegida por el artículo 11 de la Carta («Libertad de expresión y de información»). Este derecho comprende la «libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras». La libertad de información, con arreglo tanto al artículo 11 de la Carta como al artículo 10 del CEDH, protege el derecho no solo de comunicar información sino también de *recibirla*.

Las limitaciones de la libertad de expresión deben cumplir los criterios establecidos en el artículo 52, apartado 1, de la Carta, anteriormente descritos. Además, el artículo 11 se corresponde con el artículo 10 del CEDH. De conformidad con el artículo 52, apartado 3, de la Carta, en la medida en que contenga derechos que correspondan a derechos garantizados por el CEDH, «su sentido y alcance serán iguales a los que les confiere dicho Convenio». Las limitaciones que lícitamente pueden imponerse a este derecho garantizado por el artículo 11 de la Carta no pueden, por lo tanto, sobrepasar las establecidas en el artículo 10, apartado 2, del CEDH, es decir, deben estar establecidas por la ley y ser necesarias en una sociedad democrática «para la protección de la reputación o de los derechos ajenos». Estos derechos comprenden, en particular, el derecho al respeto de la vida privada y el derecho a la protección de los datos personales.

La relación entre la protección de los datos personales y la libertad de expresión está regulada por el artículo 85 del Reglamento general de protección de datos, titulado «Tratamiento y libertad de expresión y de información». En virtud de dicho artículo, los Estados miembros deben conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información. En particular, se establecerán exenciones y excepciones de lo dispuesto en determinados capítulos del Reglamento general de protección de datos para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, en la

([85]) RGPD, artículos 86 y 90.

medida en que sean necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

Ejemplo: En *Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy* [GS] ([86]), se pidió al TJUE que definiese la relación entre la protección de datos y la libertad de prensa ([87]). El Tribunal tuvo que examinar la difusión realizada por una empresa, por medio de un servicio de SMS, de datos fiscales de alrededor de 1,2 millones de personas físicas lícitamente obtenidos de la administración fiscal finlandesa. La autoridad finlandesa encargada de supervisar la protección de datos había adoptado una resolución por la que exigía a la empresa que dejara de difundir estos datos. La empresa impugnó esta resolución ante un órgano jurisdiccional nacional, que solicitó al TJUE una aclaración sobre la interpretación de la Directiva sobre protección de datos. En particular, el TJUE tuvo que verificar si el tratamiento de datos personales, que la administración fiscal puso a disposición de los usuarios de teléfonos móviles para que estos recibieran datos fiscales relativos a otras personas físicas, debe considerarse una actividad realizada con fines exclusivamente periodísticos. Tras determinar que las actividades de la empresa constituían «tratamiento de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva sobre protección de datos, el TJUE analizó el artículo 9 de la Directiva (sobre el tratamiento de datos personales y la libertad de expresión). En primer lugar destacó la importancia que tiene el derecho a la libertad de expresión en toda sociedad democrática y sostuvo que los conceptos relacionados con ella, entre ellos el de periodismo, deben ser interpretados en sentido amplio. Después observó que, para obtener una ponderación equilibrada de los dos derechos fundamentales, las excepciones y restricciones a la protección de los datos deben establecerse dentro de los límites de lo que resulte estrictamente necesario. En dichas circunstancias, el TJUE consideró que las actividades realizadas por las empresas en cuestión relativas a datos procedentes de documentos públicos según la legislación nacional, pueden calificarse de «actividades periodísticas» si su finalidad es

([86]) TJUE, C-73/07, *Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy* [GS], 16 de diciembre de 2008, apartados 56, 61 y 62.

([87]) El asunto trataba de la interpretación del artículo 9 de la Directiva sobre protección de datos — actualmente sustituido por el artículo 85 del Reglamento general de protección de datos—, que decía así: «En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión».

divulgar al público información, opiniones o ideas, por cualquier medio de transmisión. También dictaminó que dichas actividades no están reservadas a las empresas de medios de comunicación y pueden ejercerse con ánimo de lucro. Sin embargo, el TJUE dejó que fuera el órgano jurisdiccional nacional quien apreciara si era este el caso en virtud de los hechos concretos de este asunto.

El mismo asunto fue examinado también por el TEDH, después de que el órgano jurisdiccional nacional decidiese, basándose en las orientaciones del TJUE, que la orden de la autoridad de control de cesar en la publicación de toda la información fiscal era una injerencia justificada en la libertad de expresión de la empresa. El TEDH respaldó este criterio ([88]). Determinó que, si bien había una injerencia en el derecho de las empresas a comunicar información, la injerencia era conforme con la ley, perseguía un fin legítimo y era necesaria en una sociedad democrática.

El Tribunal recordó los criterios de la jurisprudencia por los que deben guiarse las autoridades nacionales, así como el propio TEDH, para obtener una ponderación equilibrada de la libertad de expresión con el derecho al respeto de la vida privada. Cuando está en juego el discurso político o un debate sobre una materia de interés público, existe escaso margen para limitar el derecho a recibir y comunicar información, ya que el público tiene derecho a ser informado «y este es un derecho esencial en una sociedad democrática» ([89]). Sin embargo, no cabe considerar que los artículos de prensa dirigidos exclusivamente a satisfacer la curiosidad de determinados lectores en relación con detalles de la vida privada de una persona contribuyan a un debate de interés público. La excepción de las normas de protección de datos con fines periodísticos tiene por objeto permitir que los periodistas obtengan, recopilen y traten datos para poder realizar su labor periodística. De este modo, existía de hecho un interés público en facilitar el acceso a las grandes cantidades de datos fiscales en juego y permitir que las empresas demandantes los recopilasen y tratasen. Por el contrario, el Tribunal dictaminó que no existía interés público en la difusión de grandes volúmenes de datos sin procesar por parte de los periódicos, en un formato inalterado y sin ningún aporte analítico. La información sobre fiscalidad

([88]) TEDH, *Satakunnan Markkinapörssi Oy y Satamedia Oy contra Finlandia* [GS], n.º 931/13, 27 de junio de 2017.

([89]) Ibíd., apartado 169.

podría haber permitido que los miembros curiosos del público clasificasen a las personas según su situación económica y satisficieran las ansias del público de conocer la vida privada de los demás. No cabía considerar que esto contribuyese a un debate de interés público.

Ejemplo: En *Google Spain* ([90]) el TJUE examinó si Google estaba obligada a eliminar de los resultados de sus búsquedas información anticuada sobre las dificultades financieras del demandante. Cuando se introducía el nombre del demandante en el motor de búsqueda de Google, los resultados contenían enlaces a antiguos artículos de prensa que le relacionaban con un procedimiento de quiebra. El demandante consideró que esto vulneraba sus derechos al respeto de la vida privada y a la protección de los datos personales, ya que ese procedimiento había concluido hacía años, por lo que esas referencias eran irrelevantes.

El TJUE aclaró en primer lugar que los motores de búsqueda en internet y los resultados de las búsquedas que facilitan datos personales pueden facilitar la creación de un perfil detallado de una persona física. Dado que la sociedad está cada vez más digitalizada, el requisito de que los datos personales sean precisos y de que su publicación no vaya más allá de lo estrictamente necesario —es decir, proporcionar información al público— es fundamental para garantizar un alto nivel de protección de datos a las personas físicas. El «responsable del tratamiento, debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicho tratamiento cumple los requisitos» del Derecho de la UE, a fin de que las garantías legales establecidas tengan pleno efecto. Esto significa que el derecho de una persona a que se borren sus datos personales cuando el tratamiento de dichos datos ya no sea necesario o estén anticuados alcanza también a los motores de búsqueda, que se dictaminó que eran los responsables del tratamiento, no meros encargados (véase la sección 2.3.1).

Tras examinar si Google estaba obligada a eliminar los enlaces relacionados con el demandante, el TJUE dictaminó que, en determinadas condiciones, las personas físicas tienen derecho a obtener la eliminación de sus datos personales de los resultados de un motor de búsqueda en internet. Este derecho puede invocarse cuando la información relativa a una persona

([90]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014, apartados 81-83.

física sea inexacta, inadecuada, irrelevante o excesiva para los fines del tratamiento de datos. El TJUE reconoció que este derecho no es absoluto, sino que necesita ponderarse con otros derechos, en particular el interés y el derecho del público en general a obtener acceso a la información. Cada solicitud de eliminación requiere una valoración específica para alcanzar un equilibrio entre los derechos fundamentales a la protección de los datos personales y a la vida privada del interesado, por una parte, y los intereses legítimos de todos los usuarios de internet, por otra. El TJUE ofreció orientaciones sobre los factores que deben tenerse en cuenta durante el ejercicio de ponderación equilibrada. La naturaleza de la información en cuestión es un factor especialmente importante. Si la información es sensible para la vida privada de la persona física y cuando no exista interés público en la disponibilidad de la información, la protección de datos y la privacidad prevalecerían sobre el derecho del público en general a obtener acceso a la información. Por el contrario, si parece que el interesado es una figura pública o que la información es de tal naturaleza que justifica otorgar al público en general acceso a dicha información, entonces se justifica la injerencia en los derechos fundamentales a la protección de datos y a la privacidad.

Tras esta sentencia, el Grupo de Trabajo del Artículo 29 adoptó directrices sobre la aplicación del fallo del TJUE. Estas directrices incluyen una lista de criterios comunes que han de aplicar las autoridades de control para resolver reclamaciones relacionadas con solicitudes de eliminación realizadas por personas físicas y que han de orientarles en esta ponderación del ejercicio de los derechos ([91]).

Respecto de la conciliación del derecho a la protección de datos con el derecho a la libertad de expresión, el TEDH ha dictado varias sentencias históricas.

Ejemplo: En *Axel Springer AG contra Alemania* ([92]), el TEDH determinó que una orden judicial que impedía a la empresa demandante publicar un artículo sobre la detención y condena de un actor famoso vulneraba el artículo 10

([91]) Grupo de Trabajo del Artículo 29 (2014), *Directrices sobre la aplicación de la sentencia del TJUE «Google Spain y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González», C-131/12*, WP 225, Bruselas, 26 de noviembre de 2014.

([92]) TEDH, *Axel Springer AG contra Alemania* [GS], n.º 39954/08, 7 de febrero de 2012, apartados 90 y 91.

del CEDH. El TEDH reiteró los criterios que han de tomarse en consideración para ponderar el derecho a la libertad de expresión y el derecho al respeto de la vida privada, sentados en su jurisprudencia:

- si el hecho del que trataba el artículo publicado en cuestión era de interés general;
- si la persona afectada era una figura pública; y
- el modo en que se obtuvo la información y si esta era fiable.

El TEDH dictaminó que la detención y condena del actor era un hecho judicial público y, por tanto, de interés público; que el actor era suficientemente famoso como para ser considerado una figura pública; y que la información había sido facilitada por la Fiscalía y las partes no ponían en duda su exactitud. Por lo tanto, las limitaciones de publicación impuestas a la empresa no habían sido razonablemente proporcionadas al objetivo legítimo de proteger la vida privada del demandante. El tribunal concluyó que había existido una violación del artículo 10 del CEDH.

Ejemplo: *Couderc y Hachette Filipacchi Associés contra Francia* [GS] ([93]) trataba de la publicación en un semanario francés de una entrevista con la Sra. Coste, que afirmaba que el príncipe Alberto de Mónaco era el padre de su hijo. En la entrevista también se explicaba la relación de la Sra. Coste con el príncipe y la reacción de este ante el nacimiento del bebé, ilustrada con fotos del príncipe con el niño. El príncipe Alberto demandó a la editorial por vulnerar su derecho a la protección de su vida privada. Los órganos jurisdiccionales franceses dictaminaron que la publicación del artículo había causado daños irreversibles al príncipe Alberto y condenó a la editorial a pagar daños y perjuicios y a publicar los pormenores de la sentencia en la portada de la revista.

La editorial llevó el caso al TEDH alegando que la sentencia de los órganos jurisdiccionales franceses constituía una injerencia injustificable en su derecho a la libertad de expresión. El TEDH tuvo que ponderar el derecho del príncipe Alberto a su vida privada con el derecho de la editorial a la libertad de expresión y el derecho del público en general a recibir la información. El

([93]) TEDH, *Couderc y Hachette Filipacchi Associés contra Francia* [GS], n.º 40454/07, 10 de noviembre de 2015.

derecho de la Sra. Coste a compartir su historia con el público y el interés del niño en que se estableciera oficialmente la relación de paternidad fueron otras consideraciones importantes.

El TEDH determinó que la publicación de la entrevista constituía una injerencia en la vida privada del príncipe y pasó a examinar si la injerencia era necesaria. Consideró que la publicación se refería a una figura pública y a una cuestión de interés público, ya que los ciudadanos de Mónaco tenían interés en conocer la existencia de un hijo del príncipe, dado que el futuro de una monarquía hereditaria está «intrínsecamente ligado a la existencia de descendientes» y es por tanto una cuestión de interés para el público ([94]). El Tribunal también observó que el artículo había permitido a la Sra. Coste y a su hijo ejercer su derecho a la libertad de expresión. Los órganos jurisdiccionales nacionales no habían tomado en la debida consideración los principios y criterios desarrollados en la jurisprudencia del TEDH para la ponderación del derecho al respeto de la vida privada y el derecho a la libertad de expresión. Concluyó que Francia había vulnerado el artículo 10 del CEDH sobre la libertad de expresión.

En la jurisprudencia del TEDH, uno de los criterios principales relacionados con la ponderación de estos derechos es si la expresión en cuestión contribuye o no a un debate de interés público general.

Ejemplo: En *Mosley contra Reino Unido* ([95]), un semanario nacional publicó fotografías íntimas del demandante, una figura muy conocida que posteriormente interpuso una demanda civil contra la editorial y obtuvo una resolución favorable con pago de daños y perjuicios. Pese a la indemnización monetaria obtenida, se quejó de que seguía siendo víctima de una vulneración de su derecho a la vida privada, ya que no había tenido la oportunidad de solicitar medidas cautelares previas a la publicación de las fotos en cuestión debido a que no existía ningún requisito legal que obligase al periódico a realizar una notificación previa de la publicación.

([94]) Ibíd., apartados 104-116.

([95]) TEDH, *Mosley contra Reino Unido*, n.º 48009/08, 10 de mayo de 2011, apartados 129 y 130.

El TEDH señaló que, aunque la difusión de dicho material se realizara, por lo general, con fines de entretenimiento más que de educación, sin duda se benefició de la protección del artículo 10 del CEDH, que puede disminuir en virtud de los requisitos del artículo 8 del CEDH cuando la información tenga un carácter privado e íntimo y no exista un interés público en su difusión. Sin embargo, debe tenerse especial cuidado al examinar limitaciones que podrían funcionar como una forma de censura previa a la publicación. En vista del efecto disuasorio que podría acarrear la obligación de notificación previa, de las dudas sobre su eficacia y del amplio margen de apreciación existente en ese ámbito, el TEDH concluyó que el artículo 8 no exigía la existencia de una notificación previa jurídicamente vinculante. De este modo, el Tribunal concluyó que no había existido una violación del artículo 8.

Ejemplo: En *Bohlen contra Alemania* ([96]), el demandante, un famoso cantante y productor artístico, había publicado un libro autobiográfico y posteriormente se había visto obligado a eliminar algunos pasajes a raíz de sentencias judiciales. La historia tuvo amplia cobertura en los medios nacionales y una empresa tabaquera lanzó una campaña publicitaria cómica que hacía referencia a estos hechos, utilizando el nombre de pila del demandante sin su consentimiento. El demandante reclamó daños y perjuicios a la empresa publicitaria sin éxito, alegando que se habían vulnerado sus derechos en virtud del artículo 8 del CEDH. El TEDH reiteró los criterios que guían la ponderación entre el derecho al respeto de la vida privada y el derecho a la libertad de expresión y resolvió que no había existido vulneración del artículo 8. El demandante era una figura pública y el anuncio no aludía a detalles de su vida privada, sino a un hecho público que ya había sido tratado en los medios de comunicación y formado parte de un debate público. Además, el anuncio era de carácter cómico y no incluía contenidos que resultasen degradantes o negativos para el demandante.

Ejemplo: En *Biriuk contra Lituania* ([97]), la demandante argumentó ante el TEDH que Lituania no había cumplido con su obligación de garantizar el respeto de su derecho a la vida privada, porque a pesar de que un periódico importante había cometido una grave violación de su privacidad, los órganos jurisdiccionales nacionales que habían examinado el caso le habían concedido una suma irrisoria en concepto de daños pecuniarios. En su reconocimiento

([96]) TEDH, *Bohlen contra Alemania*, n.º 53495/09, 19 de febrero de 2015, apartados 45-60.

([97]) TEDH, *Biriuk contra Lituania*, n.º 23373/03, 25 de noviembre de 2008.

de los daños no pecuniarios, los órganos jurisdiccionales nacionales habían aplicado las disposiciones de la legislación nacional sobre la comunicación de información al público, que establecía un bajo límite máximo para las indemnizaciones por los daños no pecuniarios causados por la difusión pública ilícita de información acerca de la vida privada de una persona por los medios de comunicación. El caso tenía su origen en la publicación en la portada del mayor diario lituano de un artículo que informaba de que la demandante era seropositiva. El artículo también criticaba la conducta de la demandante y cuestionaba sus valores morales.

El TEDH recordó que la protección de los datos personales, especialmente de los datos médicos, tiene una importancia fundamental para el derecho al respeto de la vida privada con arreglo al CEDH. La confidencialidad de los datos de salud es particularmente importante, ya que la revelación de datos médicos (la condición seropositiva de la demandante en este caso) puede afectar dramáticamente a la vida privada y familiar de una persona, a su situación laboral y a su integración en la sociedad. El Tribunal atribuyó especial importancia al hecho de que, según el reportaje del periódico, el personal médico del hospital había facilitado información sobre la condición seropositiva de la demandante, incumpliendo de forma evidente su obligación de secreto profesional. Por tanto, no había existido una injerencia legítima en el derecho de la demandante a la vida privada.

El artículo había sido publicado en la prensa y la libertad de expresión también es un derecho fundamental con arreglo al CEDH. Sin embargo, al examinar si la existencia de un interés público justificaba la publicación de ese tipo de información acerca de la demandante, el Tribunal dictaminó que la finalidad principal de la publicación era aumentar las ventas del periódico satisfaciendo la curiosidad de sus lectores. No cabía considerar que esta finalidad contribuyese a ningún debate de interés general para la sociedad. Dado que este era un caso de «intolerable abuso de la libertad de prensa» y en vista de las graves limitaciones a la reparación de los daños y de la baja suma por daños no pecuniarios establecida en la legislación nacional, Lituania había incumplido su obligación positiva de proteger el derecho de la demandante a la vida privada. El TEDH resolvió que había existido una violación del artículo 8 del CEDH.

El derecho a la libertad de expresión y el derecho a la protección de los datos personales no siempre están en conflicto. Hay casos en que la protección efectiva de los datos personales garantiza la libertad de expresión.

> Ejemplo: En *Tele2 Sverige*, el TJUE resolvió que la injerencia causada por la Directiva 2006/24 (Directiva sobre conservación de datos) en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta «resulta de gran magnitud y debe considerarse especialmente grave. Además, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante». El TJUE resolvió además que la conservación generalizada de datos de tráfico y localización podría influir en el uso de los medios de comunicación electrónica y «en consecuencia, en el ejercicio por los usuarios de esos medios de su libertad de expresión, garantizada por el artículo 11 de la Carta» ([98]). En ese sentido, al exigir garantías estrictas de que la conservación de datos no se lleve a cabo de manera generalizada, la normativa de protección de datos contribuye en última instancia al ejercicio de la libertad de expresión.

En relación con el derecho a recibir información, que también forma parte de la libertad de expresión, cada vez se tiene mayor conciencia de la importancia de la transparencia gubernativa para el funcionamiento de una sociedad democrática. La transparencia es un objetivo de interés general que, por tanto, podría justificar una injerencia en el derecho a la protección de los datos, siempre que sea necesaria y proporcionada, tal como se explica en la sección 1.2. Por consiguiente, en las dos últimas décadas, el derecho de acceso a los documentos conservados por las autoridades públicas ha sido reconocido como un derecho importante para todos los ciudadanos de la UE, y para toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro.

Según el Derecho del CdE, podrá hacerse referencia a los principios consagrados en la Recomendación relativa al acceso a los documentos públicos, los cuales

([98]) TJUE, asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB contra Post- och telestyrelsen y Secretary of State for the Home Department contra Tom Watson y otros* [GS], 21 de diciembre de 2016, apartado 101; TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros* [GS], 8 de abril de 2014, apartado 28.

inspiraron a los autores del Convenio sobre el Acceso a los Documentos Públicos (Convenio 205) ([99]).

Según el Derecho de la UE, el derecho de acceso a los documentos está garantizado en el Reglamento (CE) n.º 1049/2001 relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (Reglamento de acceso a los documentos) ([100]). El artículo 42 de la Carta y el artículo 15, apartado 3, del TFUE han ampliado este derecho de acceso «a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte».

Este derecho puede entrar en conflicto con el derecho a la protección de datos si el acceso a un documento podría revelar los datos personales de otras personas. El artículo 86 del Reglamento general de protección de datos establece claramente que los datos personales contenidos en documentos oficiales que obren en posesión de autoridades públicas u organismos públicos podrán ser comunicados por dicha autoridad u organismo de conformidad con el Derecho de la Unión ([101]) o de los Estados miembros a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del Reglamento.

Las solicitudes de acceso a los documentos o la información que obren en posesión de las autoridades públicas deberán ponderarse con el derecho a la protección de datos de las personas cuyos datos se incluyan en los documentos solicitados.

Ejemplo: En *Volker und Markus Schecke* ([102]), el TJUE tuvo que valorar la proporcionalidad de la publicación, exigida por la legislación de la UE, del nombre de los beneficiarios de los subsidios agrícolas de la UE y de los importes recibidos. La publicación tenía por objeto aumentar la

([99]) Consejo de Europa, Comité de Ministros (2002), Recomendación Rec(81) 19 y Recomendación Rec(2002) 2 a los Estados miembros sobre el acceso a los documentos públicos, 21 de febrero de 2002; Consejo de Europa, Convenio sobre el Acceso a los Documentos Públicos, STCE n.º 205, 18 de junio de 2009. El Convenio aún no ha entrado en vigor.

([100]) Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, DO 2001 L 145.

([101]) Artículo 42 de la Carta, artículo 15, apartado 3, del TFUE y Reglamento 1049/2009.

([102]) TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 9 de noviembre de 2010, apartados 47-52, 58, 66-67, 75, 86 y 92.

transparencia y contribuir al control público del uso adecuado de los fondos públicos por parte de la administración. Varios beneficiarios impugnaron la proporcionalidad de esta publicación.

El TJUE, teniendo en cuenta que el derecho a la protección de datos no es absoluto, argumentó que la publicación en un sitio web de los datos nominales de los beneficiarios de dos fondos de ayuda agrícola de la UE y de los importes específicos percibidos por ellos constituye una injerencia en su vida privada, en general, y en la protección de sus datos personales, en particular.

El TJUE resolvió que dicha injerencia en los artículos 7 y 8 de la Carta estaba establecida por la ley y cumplía un objetivo de interés general reconocido por la UE, que incluía, en particular, el aumento de la transparencia del uso de los fondos comunitarios. Sin embargo, el TJUE sostuvo que la publicación de los nombres de personas físicas que son beneficiarios de la ayuda agrícola de la UE procedente de estos dos fondos y los importes exactos recibidos constituía una medida desproporcionada y no estaba justificada, con arreglo al artículo 52, apartado 1, de la Carta. Reconoció la importancia que tiene, en una sociedad democrática, mantener a los contribuyentes informados del uso de los fondos públicos. Sin embargo, dado que «no cabe atribuir una primacía automática al objetivo de transparencia sobre el derecho a la protección de los datos de carácter personal» ([103]), las instituciones de la UE estaban obligadas a ponderar el interés de la Unión en la transparencia con la limitación del ejercicio de los derechos a la privacidad y a la protección de los datos personales que sufrieron los beneficiarios a causa de esta publicación.

El TJUE consideró que las instituciones de la UE no habían llevado a cabo este ejercicio de ponderación correctamente, ya que era posible concebir medidas que entrañasen lesiones de menor gravedad a este derecho fundamental de las personas físicas, sin dejar por ello de contribuir eficazmente al objetivo de transparencia que se perseguía con la publicación. Por ejemplo, en lugar de una publicación general que afectase a todos los beneficiarios, indicando su nombre y los importes exactos recibidos por cada uno de ellos, se podría establecer una distinción en función de criterios pertinentes, tales como los periodos durante los cuales dichas personas habían percibido estas ayudas,

([103]) Ibíd., apartado 85.

su frecuencia, tipo y magnitud ([104]). El TJUE declaró entonces parcialmente inválida la legislación de la UE sobre la publicación de información relativa a los beneficiarios de los fondos agrícolas europeos.

Ejemplo: En *Rechnungshof contra Österreichischer Rundfunk y otros* ([105]), el TJUE examinó la compatibilidad de determinada legislación austriaca con el Derecho de la UE sobre protección de datos. La legislación obligaba a un organismo estatal a recoger y comunicar datos sobre ingresos con el fin de publicar los nombres y los ingresos de empleados de varios entes públicos en un informe anual que se ponía a disposición del público en general. Algunas personas se negaron a comunicar sus datos por razones de protección de datos.

En su dictamen, el TJUE tuvo en cuenta la protección de los derechos fundamentales como principio general del Derecho de la UE y el artículo 8 del CEDH, recordando que la Carta no era vinculante en ese momento. Resolvió que la recogida de datos nominales sobre los ingresos profesionales de un individuo y, en particular, su comunicación a terceros, está comprendida en el ámbito de aplicación del derecho al respeto de la vida privada y constituye una vulneración de este derecho. Dicha interferencia podría justificarse si hubiera sido conforme a la ley, respondiera a un fin legítimo y fuera necesaria en una sociedad democrática para conseguir dicho fin. El TJUE observó que la legislación austriaca perseguía un fin legítimo, ya que su objetivo era mantener las retribuciones de los funcionarios públicos dentro de unos límites razonables, una consideración que también está relacionada con el bienestar económico del país. Sin embargo, el interés de Austria en garantizar el mejor uso de los fondos públicos debía ponderarse con la gravedad de la injerencia en el derecho de las personas afectadas al respeto de su vida privada.

Aunque consideró que correspondía al órgano jurisdiccional nacional comprobar si la publicación de los datos sobre los ingresos de las personas afectadas era necesaria y proporcionada para el fin perseguido por la legislación, el TJUE instó a dicho órgano jurisdiccional nacional a determinar si no se podía haber conseguido dicho fin de manera igualmente efectiva

([104]) Ibíd., apartado 89.

([105]) TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/09, *Rechnungshof contra Österreichischer Rundfunk y otros* y *Christa Neukomm y Joseph Lauermann contra Österreichischer Rundfunk*, de 20 de mayo de 2003.

por medios menos invasivos. Un ejemplo sería la comunicación de los datos personales únicamente a los organismos públicos de control y no al público en general.

En asuntos posteriores se puso de manifiesto que la ponderación entre la protección de datos y el acceso a los documentos requiere un análisis detallado caso por caso. Ninguno de estos derechos puede prevalecer automáticamente sobre el otro. El TJUE tuvo la oportunidad de interpretar el derecho de acceso a los documentos que contengan datos personales en dos asuntos.

Ejemplo: En *Comisión Europea contra Bavarian Lager* ([106]), el TJUE definió el ámbito de protección de los datos personales en el contexto del acceso a los documentos de las instituciones de la UE y la relación entre el Reglamento (CE) n.º 1049/2001 (Reglamento de acceso a los documentos) y el Reglamento (CE) n.º 45/2001 (Reglamento de protección de datos de las instituciones de la UE). Bavarian Lager, constituida en 1992, importa cerveza alemana embotellada al Reino Unido, destinada principalmente a los establecimientos de despacho de bebidas alcohólicas. Sin embargo, la empresa se encontró con dificultades porque la legislación británica favorecía de hecho a los productores nacionales. En respuesta a la reclamación de Bavarian Lager, la Comisión Europea decidió incoar el procedimiento por incumplimiento contra el Reino Unido, lo cual llevó a que se modificasen las disposiciones impugnadas y se adaptasen al Derecho de la UE. Bavarian Lager solicitó entonces a la Comisión, entre otros documentos, una copia del acta de la reunión a la que habían asistido los representantes de la Comisión, las autoridades británicas y la *Confédération des Brasseurs du Marché Commun* (CBMC). La Comisión acordó difundir determinados documentos relacionados con la reunión, aunque ocultó cinco nombres que aparecían en el acta, porque dos de esas personas se habían opuesto expresamente a que se revelase su identidad y la Comisión no pudo ponerse en contacto con las otras tres personas. Mediante decisión de 18 de marzo de 2004, la Comisión desestimó una nueva solicitud presentada por Bavarian Lager con objeto de obtener el acta completa de la reunión, citando, en particular, la protección de la vida privada de dichas personas, tal como garantiza el Reglamento de protección de datos de las instituciones de la UE.

([106]) TJUE, C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd.* [GS], 29 de junio de 2010.

Insatisfecha con la decisión, Bavarian Lager interpuso un recurso ante el Tribunal de Primera Instancia. Este órgano jurisdiccional anuló la Decisión de la Comisión mediante sentencia de 8 de noviembre de 2007 (asunto T-194/04, *The Bavarian Lager Co. Ltd contra Comisión de las Comunidades Europeas*), resolviendo que la mera incorporación de los nombres de las personas en cuestión a la lista de asistentes a una reunión en nombre del organismo al que representaban no perjudica la vida privada ni ponía en peligro la vida privada de esas personas.

Tras el recurso de la Comisión, el TJUE anuló la sentencia del Tribunal de Primera Instancia. El TJUE resolvió que el Reglamento de acceso a los documentos establece «un régimen específico y reforzado de protección de la persona cuyos datos personales pudieran, en su caso, divulgarse». En opinión del TJUE, cuando una solicitud para la obtención de documentos que contienen datos personales se basa en el Reglamento de acceso a los documentos, el Reglamento de protección de datos de las instituciones de la UE es aplicable en su totalidad. El TJUE concluyó entonces que la Comisión denegó legítimamente la solicitud de acceso al acta completa de la reunión de octubre de 1996. A falta de consentimiento de los cinco participantes en dicha reunión, la Comisión cumplió de manera suficiente con su deber de apertura difundiendo una versión del documento en cuestión, una vez eliminados sus nombres.

Además, en opinión del TJUE, «al no haber presentado Bavarian Lager ninguna justificación expresa y legítima ni ningún argumento convincente para demostrar la necesidad de la transmisión de dichos datos personales, la Comisión no pudo ponderar los distintos intereses de las partes implicadas. Tampoco podía verificar si existían motivos para suponer que esa transmisión podría perjudicar los intereses legítimos de los interesados», tal como exige el Reglamento de protección de datos de las instituciones de la UE.

Ejemplo: En *ClientEarth y PAN Europe contra EFSA* ([107]), el TJUE examinó si la decisión de la Autoridad Europea de Seguridad Alimentaria (EFSA) de denegar a los demandantes el acceso pleno a los documentos era necesaria para proteger los derechos a la privacidad y a la protección de los datos personales de las personas a las que se referían los documentos. Estos se

([107]) TJUE, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) contra Autoridad Europea de Seguridad Alimentaria (EFSA), Comisión Europea*, 16 de julio de 2015

referían a un proyecto de orientación elaborado por un grupo de trabajo de la EFSA en colaboración con expertos externos acerca de la comercialización de productos fitosanitarios. En principio, la EFSA otorgó un acceso parcial a los demandantes, denegando el acceso a algunas versiones de trabajo del proyecto de orientación. Posteriormente, autorizó el acceso a la versión del proyecto que incluía los comentarios individuales de los expertos externos. Sin embargo, tachó los nombres de los expertos invocando el artículo 4, apartado 1, letra b) del Reglamento n.º 1049/2001 relativo al tratamiento de datos personales por las instituciones y los organismos de la UE y a la necesidad de proteger la privacidad de los expertos externos. En primera instancia, el Tribunal General de la UE respaldó la decisión de la EFSA.

Tras el recurso de los demandantes, el TJUE anuló la sentencia de primera instancia. Concluyó que la transmisión de datos personales en ese caso era necesaria para determinar la imparcialidad de cada uno de los expertos externos en el desempeño de sus funciones como científicos y para garantizar la transparencia del proceso decisorio en la EFSA. Según el TJUE, la EFSA no especificó de qué modo se perjudicarían los intereses legítimos de los expertos externos en revelar los nombres de aquellos que habían realizado comentarios concretos sobre el proyecto de orientación. No basta con argumentar que esta revelación puede perjudicar la vida privada con carácter general si no se aportan pruebas concretas para cada caso.

De conformidad con estas sentencias, la injerencia en el derecho a la protección de los datos personales en el contexto del acceso a los documentos precisa de una razón específica y justificada. El derecho de acceso a los documentos no puede prevalecer automáticamente sobre el derecho a la protección de los datos ([108]).

Este planteamiento es parecido al del TEDH en relación con la privacidad y el acceso a los documentos, como demuestra la sentencia siguiente. En la sentencia *Magyar Helsinki*, el TEDH dictaminó que el artículo 10 no otorgaba a la persona el derecho de acceso a la información que obraba en posesión de una autoridad pública ni obligaba al gobierno a comunicar dicha información a la persona. Sin embargo, tal derecho u obligación podría nacer, en primer lugar, cuando la revelación de la información venga impuesta por un mandato judicial que haya adquirido fuerza legal; en segundo lugar, cuando el acceso a la información sea esencial para que la persona

([108]) Véanse, sin embargo, las deliberaciones pormenorizadas en SEPD (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling*, Bruselas, 24 de marzo de 2011.

ejerza su derecho a la libertad de expresión —en particular la libertad de recibir y comunicar información— y cuando su denegación suponga una injerencia en ese derecho ([109]). Si la denegación del acceso a la información constituye una injerencia en la libertad de expresión de un solicitante, y en qué medida, deberá determinarse en cada caso individual y en vista de las circunstancias concretas como, por ejemplo: i) la finalidad de la solicitud de información; ii) la naturaleza de la información solicitada; iii) la función del solicitante; y iv) si la información ya estaba preparada y disponible.

Ejemplo: En *Magyar Helsinki Bizottság contra Hungría* [GS] ([110]), el solicitante, una ONG de derechos humanos, solicitó a la policía información relativa al trabajo de los abogados de oficio, a fin de completar un estudio sobre el funcionamiento del sistema de defensa de oficio en Hungría. La policía se negó a proporcionar esta información, alegando que constituían datos personales no sujetos a divulgación. Aplicando los criterios anteriores, el TEDH resolvió que había existido una injerencia en un derecho protegido por el artículo 10. Más concretamente, el demandante deseaba ejercer el derecho a comunicar información sobre una materia de interés público, había solicitado acceso a información con ese fin y la información era necesaria para que el demandante ejerciese su derecho a la libertad de expresión. La información sobre el nombramiento de los abogados de oficio era de interés para el público. No había motivo para dudar de que el estudio en cuestión contenía información que el demandante se comprometía a comunicar al público y que el público tenía derecho a recibir. El Tribunal quedó por tanto satisfecho de que el acceso a la información solicitada era necesario para que el demandante llevase a cabo esa tarea. Por último, la información estaba preparada y disponible.

El TEDH concluyó que la denegación del acceso a la información en ese caso había afectado a la misma esencia de la libertad para recibir información. Para llegar a esta conclusión, examinó en particular la finalidad de la información solicitada y su contribución a un importante debate público, la naturaleza de la información solicitada y si tenía interés público, así como la labor realizada en la sociedad por el demandante del caso.

([109]) TEDH, *Magyar Helsinki Bizottság contra Hungría* [GS], n.º 18030/11, 8 de noviembre de 2016, apartado 148.

([110]) Ibíd., apartados 181, 187-200.

En su exposición de motivos, el Tribunal observó que el estudio realizado por la ONG se refería al funcionamiento de la justicia y al derecho de defensa, que era un derecho de importancia fundamental con arreglo al CEDH. Dado que la información solicitada no comprendía datos que no fueran de dominio público, el derecho a la privacidad de los interesados (los abogados de oficio) no se hubiera lesionado si la policía hubiera otorgado al demandante acceso a la información. La información solicitada por el demandante era de naturaleza estadística, relativa al número de veces que se había nombrado un abogado de oficio para que representase a acusados en procesos penales.

Para el Tribunal, dado que el estudio tenía por objeto contribuir a un debate importante sobre una materia de interés general, cualquier restricción a la publicación propuesta por la ONG debía haberse examinado en profundidad. La información en cuestión era de interés público, ya que el interés público comprende «materias que pueden dar lugar a considerable controversia, que se refieren a un problema social importante o que tratan de un problema sobre el que el público tendría en interés en recibir información» ([111]). Por tanto, sin duda comprendería un análisis sobre la actuación de la justicia y los procesos equitativos, que era el objeto del estudio del demandante. Tras ponderar los diferentes derechos enfrentados y aplicar el principio de proporcionalidad, el TEDH resolvió que había existido una violación injustificada de los derechos del demandante en virtud del artículo 10 del CEDH.

1.3.2. Secreto profesional

En el Derecho nacional, determinadas comunicaciones pueden estar sujetas a la obligación de secreto profesional. Cabe entender el secreto profesional como un deber ético especial que incurre en una obligación legal intrínseca a determinadas profesiones y funciones, que están basadas en la lealtad y en la confianza. Las personas e instituciones que desempeñan tales funciones están obligadas a no revelar la información confidencial que reciben en el cumplimiento de sus obligaciones. El secreto profesional se aplica muy en particular a la profesión médica y al privilegio abogado-cliente, mientras que numerosas jurisdicciones reconocen asimismo la obligación de secreto profesional en el sector financiero. El secreto profesional no es un derecho fundamental, pero está protegido como una forma del derecho al respeto de la vida privada. Por ejemplo, el TJUE ha dictaminado que, en determinados

([111]) Ibíd., apartado 156.

casos, «puede resultar necesario, en efecto, prohibir la divulgación de determinada información calificada de confidencial para preservar el derecho fundamental de una empresa al respeto de la vida privada, que está recogido en el artículo 8 del [CEDH] y en el artículo 7 de la Carta» ([112]). El TEDH también ha tenido que resolver si las restricciones del secreto profesional constituyen una vulneración del artículo 8 del CEDH, como se ilustra en los ejemplos resaltados.

Ejemplo: En *Pruteanu contra Rumanía* ([113]), el demandante actuó como abogado de una empresa comercial, a la que se había prohibido realizar transacciones bancarias por estar acusada de fraude. Durante la investigación del caso, los órganos jurisdiccionales rumanos autorizaron a la Fiscalía a intervenir y grabar las conversaciones telefónicas de un socio de la empresa durante un periodo de tiempo determinado. Las grabaciones e intervenciones incluían sus comunicaciones con su abogado.

El Sr. Pruteanu afirmó que esto constituía una injerencia en su derecho al respeto de su vida privada y de su correspondencia. En su sentencia, el TEDH destacó el estatuto y la importancia de la relación de un abogado con su cliente. La intervención de las conversaciones de un abogado con su cliente vulneraba indudablemente el secreto profesional, que era el fundamento de la relación entre esas dos personas. En este caso, el abogado también podía denunciar una injerencia en su derecho al respeto de su vida privada y de su correspondencia. El TJUE sostuvo que había existido una violación del artículo 8 del CEDH.

Ejemplo: En *Brito Ferrinho Bexiga Villa-Nova contra Portugal* ([114]), la demandante, una abogada, se negó a facilitar sus extractos bancarios personales a las autoridades tributarias por razones de confidencialidad profesional y secreto bancario. La Fiscalía abrió una investigación por fraude fiscal y solicitó autorización para que se suspendiera la confidencialidad profesional. Los órganos jurisdiccionales nacionales ordenaron la suspensión de las normas de confidencialidad y secreto profesional, tras determinar que el interés público debía prevalecer sobre los intereses particulares de la demandante.

([112]) TJUE, asunto T-462/12 R, *Pilkington Group Ltd contra Comisión Europea*, Auto del Presidente del Tribunal General, 11 de marzo de 2013, apartado 44.

([113]) TEDH, *Pruteanu contra Rumanía*, n.º 30181/05, 3 de febrero de 2015.

([114]) TEDH, *Brito Ferrinho Bexiga Villa-Nova contra Portugal*, n.º 69436/10, 1 de diciembre de 2015.

Cuando el caso llegó al TEDH, el Tribunal resolvió que el acceso a los extractos bancarios de la demandante constituía una injerencia en su derecho al respeto de la confidencialidad profesional, que se inscribe en el ámbito de la vida privada. Esta injerencia tenía una base jurídica, ya que estaba fundamentada en el Código de enjuiciamiento penal, y perseguía un fin legítimo. Sin embargo, al examinar la necesidad y proporcionalidad de la injerencia, el TEDH señaló el hecho de que el procedimiento de suspensión de la confidencialidad se había llevado a cabo sin la participación o el conocimiento de la demandante. Por tanto, esta última no había podido presentar sus alegaciones. Además, aunque el Derecho nacional establecía que en un proceso de este tipo era preceptiva la consulta con el Colegio de Abogados, no se había realizado dicha consulta. Por último, la demandante no tuvo la opción de impugnar efectivamente la suspensión de la confidencialidad, ni recurso alguno para impugnar la medida. Debido a la falta de garantías procesales y de una tutela judicial efectiva sobre la medida de suspensión del deber de confidencialidad, el TEDH concluyó que había existido una violación del artículo 8 del CEDH.

La interacción entre el secreto profesional y la protección de datos suele ser ambivalente. Por una parte, las normas y garantías de protección de datos establecidas en la legislación contribuyen a garantizar el secreto profesional. Por ejemplo, normas que exigen a los responsables y encargados del tratamiento de datos personales la aplicación de medidas robustas de seguridad de los datos para prevenir, entre otras cosas, la pérdida de confidencialidad de los datos personales protegidos por el secreto profesional. Además, el Reglamento general de protección de datos de la UE permite el tratamiento de datos de salud, que constituyen categorías especiales de datos personales que merecen una protección más sólida, pero lo supedita a la existencia de medidas adecuadas y específicas para proteger los derechos de los interesados, en particular el secreto profesional ([115]).

Por otro lado, las obligaciones de secreto profesional impuestas a los responsables y encargados del tratamiento al respeto de determinados datos personales pueden limitar los derechos de los interesados, concretamente el derecho a recibir información. Aunque el Reglamento general de protección de datos contiene una extensa lista de información que, en principio, debe facilitarse al interesado cuando los datos personales no se hayan obtenido de él o ella, este requisito de revelación no será

([115]) Reglamento general de protección de datos, artículo 9, apartado 2, letra h) y artículo 9, apartado 3.

de aplicación cuando los datos personales deban mantenerse confidenciales debido a una obligación de secreto profesional establecida por el Derecho nacional o por el Derecho de la UE ([116]).

El Reglamento general de protección de datos (RGPD) contempla la posibilidad de que los Estados miembros adopten, en Derecho, normas legales específicas para garantizar las obligaciones de secreto profesional o equivalente y para conciliar el derecho a la protección de los datos personales con la obligación de secreto profesional ([117]).

El RGPD establece que los Estados miembros podrán adoptar normas específicas sobre los poderes de las autoridades de control en relación con los responsables o encargados de tratamiento que estén sujetos a una obligación de secreto profesional. Dichas normas específicas se refieren al poder de obtener acceso a todos los locales del responsable o del encargado del tratamiento, incluidos sus equipos de tratamiento y los datos personales que obren en su poder, cuando hayan recibido tales datos personales en el curso de una actividad sujeta a la obligación de secreto. Por tanto, las autoridades de control encargadas de la protección de los datos deben respetar las obligaciones de secreto profesional que vinculan a los responsables y encargados del tratamiento. Más aún, los miembros de las propias autoridades de control también están sujetos al deber de secreto profesional durante y después de su mandato. Durante el ejercicio de sus funciones, los miembros y el personal de las autoridades de control pueden conocer información confidencial. El artículo 54, apartado 2, del Reglamento establece claramente que están sujetos al deber de secreto profesional en relación con dicha información confidencial.

El RGPD obliga a los Estados miembros a notificar a la Comisión las disposiciones que adopten para conciliar la protección de datos y los principios establecidos en el Reglamento con la obligación de secreto profesional.

1.3.3. Libertad de religión y convicciones

La libertad de religión y convicciones está protegida por el artículo 9 del CEDH (libertad de pensamiento, de conciencia y de religión) y por el artículo 10 de la Carta de los Derechos Fundamentales de la Unión Europea. Los datos personales que revelan convicciones religiosas o filosóficas se consideran «datos sensibles» tanto en el

([116]) Ibíd., artículo 14, apartado 5, letra d).

([117]) Ibíd., considerando 164 y artículo 90.

Derecho de la UE como en el Derecho del CdE y su tratamiento y uso están sujetos a una protección reforzada.

Ejemplo: En *Sinan Işık contra Turquía* ([118]), el demandante era miembro de la comunidad religiosa aleví, cuya confesión está influenciada por el sufismo y por otras creencias preislámicas y algunos pensadores consideran que constituye una religión diferenciada, mientras que para otros forma parte del Islam. El demandante denunció que, en contra de sus deseos, su carné de identidad contenía una rúbrica dedicada a la religión en la que figuraba la mención «Islam», en lugar de «aleví». Los órganos jurisdiccionales nacionales rechazaron su petición de modificar su carné de identidad con la mención «aleví» alegando que ese término designaba a un subgrupo del Islam y no una religión independiente. Entonces el demandante recurrió ante el TEDH alegando que se había visto obligado a revelar su confesión religiosa en razón de la mención obligatoria de la religión en el carné de identidad, sin su consentimiento, y que esto lesionaba su derecho a la libertad de religión y de conciencia, sobre todo considerando que la mención «Islam» en su carné de identidad era incorrecta.

El TEDH reiteró que la libertad religiosa de una persona conlleva la libertad de manifestar su religión de manera colectiva, en público y en el círculo de personas con quienes comparte su fe, pero también individualmente y en privado. La legislación nacional vigente en ese momento obligaba a las personas físicas a llevar un carné de identidad, un documento que debían mostrar a petición de cualquier autoridad pública o de empresas privadas, en el que se indicaba su religión. Esta obligación no reconocía que el derecho a manifestar la propia religión también implica lo contrario, es decir, el derecho a no verse obligado a revelar las propias creencias. Aunque el Gobierno alegó que se había modificado la legislación nacional para que las personas físicas pudieran solicitar que la casilla reservada a la religión se dejase vacía, en opinión del Tribunal, el mero hecho de que una persona tenga que solicitar que se suprima la religión podría constituir la divulgación de una información relativa a su actitud hacia la religión. Además, cuando el carné de identidad incluye una casilla consagrada a la religión, el hecho de dejarla vacía tiene una connotación especial, ya que el titular de un carné de

([118]) TEDH, *Sinan Işık contra Turquía*, n.º 21924/05, 2 de febrero de 2010.

identidad que no contenga el dato de la religión se distinguirá de aquellas personas cuyo carné de identidad sí lo contenga. El TEDH concluyó que la legislación nacional vulneraba el artículo 9 del CEDH.

Sin embargo, el funcionamiento de iglesias y asociaciones o comunidades religiosas puede hacer necesario el tratamiento de los datos personales de sus miembros a fin de facilitar las comunicaciones y la organización de actividades en la congregación. Por tanto, las iglesias y asociaciones religiosas suelen aplicar normas relativas al tratamiento de datos personales. En virtud del artículo 91 del Reglamento general de protección de datos, cuando dichas normas sean generales podrán mantener su validez siempre que sean conformes con el Reglamento. Las iglesias y asociaciones religiosas que establezcan tales normas deberán someterse a la supervisión de una autoridad de control independiente, que podrá ser específica, siempre que cumplan los requisitos del Reglamento general de protección de datos para tales autoridades ([119]).

Las organizaciones religiosas podrán llevar a cabo el tratamiento de datos personales por varias razones: por ejemplo, para mantener el contacto con sus feligreses o para difundir información sobre la organización de eventos, actos religiosos y festividades, actos benéficos, etc. En algunos Estados, las iglesias deben llevar registros de sus miembros por razones tributarias, ya que la pertenencia a establecimientos religiosos puede influir en los impuestos que deben pagar las personas físicas. En cualquier caso, en virtud del Derecho de la UE, los datos que revelan creencias religiosas son datos sensibles y las iglesias deben rendir cuentas de su gestión y tratamiento de tales datos, sobre todo porque la información que manejan las organizaciones religiosas suele referirse a menores de edad, personas mayores u otros miembros vulnerables de la sociedad.

1.3.4. Libertad de las artes y de las ciencias

Otro derecho que debe ponderarse con el derecho al respeto a la vida privada y el derecho a la protección de datos es la libertad de las artes y de las ciencias, que está expresamente protegido por el artículo 13 de la Carta de los Derechos Fundamentales de la Unión Europea. Este derecho se infiere en primer lugar de las libertades de pensamiento y expresión y debe ejercerse respetando el artículo 1 de la Carta (dignidad humana). El TEDH considera que la libertad de las artes está protegida por

([119]) Reglamento general de protección de datos, artículo 91, apartado 2.

el artículo 10 del CEDH ([120]). El derecho garantizado por el artículo 13 de la Carta también puede estar sujeto a limitaciones de conformidad con el artículo 52, apartado 1, de la Carta, que también puede interpretarse bajo el prisma del artículo 10, apartado 2, del CEDH ([121]).

Ejemplo: En *Vereinigung bildender Künstler contra Austria* ([122]), los tribunales austriacos prohibieron a la asociación demandante que continuara exhibiendo una pintura que incluía fotos de las cabezas de diversas figuras públicas en posturas sexuales. Un parlamentario austriaco, cuya foto había sido utilizada en la pintura, ejerció una acción contra la asociación demandante, solicitando una orden judicial que prohibiera exhibir la pintura. El órgano jurisdiccional nacional dictó dicha orden. El TEDH reiteró que el artículo 10 del CEDH se extiende a la comunicación de ideas que ofendan, sorprendan o perturben al Estado o a una parte de la población. Quienes crean, realizan, distribuyen o exhiben obras de arte contribuyen al intercambio de ideas y opiniones y el Estado tiene la obligación de no limitar indebidamente su libertad de expresión. Teniendo en cuenta que la pintura era un *collage* y que utilizaba fotografías únicamente de las cabezas de las personas, y que sus cuerpos estaban pintados de una forma poco real y exagerada, con lo que evidentemente no se perseguía reflejar la realidad ni tan siquiera insinuarla, el TEDH declaró asimismo que «difícilmente podría entenderse que la pintura aborda detalles de la vida privada [de la persona representada] sino que más bien está relacionada con su posición pública como político» y que «en dicha calidad [la persona representada] debería mostrar una mayor tolerancia ante las críticas». Tras ponderar los distintos intereses enfrentados, el TEDH consideró que la prohibición ilimitada contra una exhibición posterior de la pintura resultaba desproporcionada. El Tribunal concluyó que había existido una violación del artículo 10 del CEDH.

La legislación europea sobre protección de datos también reconoce el especial valor que tiene la ciencia para la sociedad. El Reglamento general de protección de datos y el Convenio 108 modernizado permiten la conservación de datos durante periodos de tiempo prolongados siempre que los datos personales sean objeto de

([120]) TEDH, *Müller y otros contra Suiza*, n.º 10737/84, de 24 de mayo de 1988.

([121]) Explicaciones sobre la Carta de los Derechos Fundamentales, DO 2007 C 303.

([122]) TEDH, *Vereinigung bildender Künstler contra Austria*, n.º 68345/01, de 25 de enero de 2007, apartados 26 y 34.

tratamiento exclusivamente con fines de investigación científica o histórica. Además, y con independencia del fin originario de una determinada actividad de tratamiento de datos, el uso posterior de datos personales para la investigación científica no se considerará un fin incompatible ([123]). Al mismo tiempo, deben establecerse garantías adecuadas para llevar a cabo dicho tratamiento, con el fin de proteger los derechos y libertades de los interesados. El Derecho de la Unión o de los Estados miembros puede contemplar excepciones a los derechos de los interesados como, por ejemplo, el derecho de acceso, rectificación y restricción del tratamiento, y de oposición al tratamiento de sus datos personales con fines de investigación científica, histórica o estadística (véase también la sección 6.1 y la sección 9.4).

1.3.5. Protección de la propiedad intelectual

El derecho a la protección de la propiedad está consagrado tanto en el artículo 1 del Protocolo n.º 1 del CEDH como en el artículo 17, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea. Un aspecto importante del derecho de propiedad que es particularmente pertinente para la protección de datos es la protección de la propiedad intelectual, que se menciona expresamente en el artículo 17, apartado 2, de la Carta. Varias Directivas del ordenamiento jurídico de la UE tienen por objeto proteger de manera efectiva la propiedad intelectual, en particular los derechos de autor. La propiedad intelectual comprende no solo la propiedad literaria y artística sino también las patentes, las marcas y los derechos conexos.

Tal como ha dejado claro la jurisprudencia del TJUE, la protección del derecho fundamental a la propiedad debe ponderarse equilibradamente con la protección de otros derechos fundamentales, en particular, con el derecho a la protección de datos ([124]). Ha habido casos en los que las instituciones dedicadas a la protección de los derechos de autor exigieron a los proveedores de acceso a internet que revelaran la identidad de los usuarios de las plataformas de intercambio de archivos en internet. Dichas plataformas con frecuencia ofrecen a los usuarios de internet la posibilidad de descargar de forma gratuita títulos musicales, aunque estén protegidos por derechos de autor.

([123]) Reglamento general de protección de datos, artículo 5, apartado 1, letra b).

([124]) TJUE, C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU* [GS], 29 de enero de 2008, apartados 62-68.

Ejemplo: *Promusicae contra Telefónica de España* ([125]) trataba de la negativa de un proveedor español de acceso a internet, Telefónica, a comunicar a Promusicae, una organización sin ánimo de lucro de productores musicales y editores de grabaciones musicales y audiovisuales, los datos personales de determinadas personas a las que Telefónica prestaba un servicio de acceso a internet. Promusicae solicitó que le fuera facilitada la información referida para poder ejercitar acciones civiles contra los interesados, que según ella utilizaban un programa de intercambio de ficheros que permitía el acceso a fonogramas cuyos derechos patrimoniales de explotación correspondían a los asociados de Promusicae.

El órgano jurisdiccional español remitió la cuestión al TJUE para que aclarase si debían comunicarse dichos datos personales, de conformidad con el Derecho comunitario, en el contexto de un procedimiento civil para garantizar la protección efectiva de los derechos de autor. Hizo mención de las Directivas 2000/31, 2001/29 y 2004/48, interpretadas asimismo a la luz de los artículos 17 y 47 de la Carta. El TJUE concluyó que estas tres Directivas, así como la Directiva sobre la privacidad en las comunicaciones electrónicas (Directiva 2002/58), no prohíben a los Estados miembros que impongan el deber de comunicar datos personales en el contexto de un procedimiento civil, para garantizar la protección efectiva de los derechos de autor.

El TJUE destacó que el asunto, por tanto, planteaba la cuestión de la necesaria conciliación de las exigencias relacionadas con la protección de distintos derechos fundamentales, a saber, el derecho al respeto de la vida privada con los derechos a la protección de la propiedad y a un recurso efectivo.

Concluyó que «corresponde a los Estados miembros, a la hora de adaptar su ordenamiento jurídico a las Directivas citadas, procurar basarse en una interpretación de estas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico a estas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con dichas Directivas, sino también procurar

([125]) Ibíd., apartados 54 y 60.

que la interpretación de estas que tomen como base no entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad» ([126]).

Ejemplo: *Bonnier Audio AB y otros contra Perfect Communication Sweden AB* ([127]) trataba del equilibrio entre los derechos a la propiedad intelectual y la protección de datos personales. Los demandantes —cinco sociedades editoras propietarias de los derechos de autor de 27 audiolibros— iniciaron un procedimiento ante el órgano jurisdiccional sueco, alegando que estos derechos de autor se vulneraban por medio de un servidor FTP (un protocolo de transferencia de archivos que permite compartir archivos y transferir datos a través de internet). Los demandantes solicitaron que el proveedor de servicios de internet (ISP) revelase el nombre y domicilio de la persona que utilizaba la dirección IP desde la cual se enviaban los archivos. El ISP, ePhone, se opuso a la demanda, alegando que vulneraba la Directiva 2006/24 (la Directiva de conservación de datos invalidada en 2014).

El órgano jurisdiccional sueco remitió la cuestión al TJUE para que aclarase si la Directiva 2006/24 se oponía a la aplicación de una disposición nacional basada en el artículo 8 de la Directiva 2004/48 (Directiva relativa al respeto de los derechos de propiedad intelectual), que permitía que se requiriese judicialmente a un ISP para que comunicarse al titular de un derecho de autor la identidad de los abonados cuyas direcciones IP hubieran servido supuestamente para la vulneración de dicho derecho. La pregunta se basaba en la premisa de que el demandante había aportado pruebas claras de la vulneración de un derecho de autor concreto y de que la medida era proporcionada.

El TJUE señaló que la Directiva 2006/24 regulaba exclusivamente el tratamiento y la conservación de datos generados por proveedores de servicios de comunicaciones electrónicas con fines de investigación, detección y enjuiciamiento de delitos graves, así como su transmisión a las autoridades nacionales competentes. Por tanto, una disposición nacional

([126]) Ibíd., apartados 65 y 68; véase también TJUE, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) contra Netlog NV*, 16 de febrero de 2012.

([127]) TJUE, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB / Perfect Communication Sweden AB*, 19 de abril de 2012.

de transposición de la Directiva de respeto a los derechos de propiedad intelectual está fuera del ámbito de aplicación de la Directiva 2006/24 y, por tanto, no está prohibida por dicha Directiva ([128]).

En lo que respecta a la comunicación del nombre y domicilio en cuestión, que solicitaban los demandantes, el TJUE resolvió que dicha acción constituía un tratamiento de datos personales y se encontraba comprendida en el ámbito de aplicación de la Directiva 2002/58 (Directiva sobre la privacidad y las comunicaciones electrónicas). También señaló que la comunicación de tales datos se requería, en el marco de un procedimiento civil, en interés del titular de un derecho de autor con el fin de garantizar la efectiva protección de tales derechos y, por tanto también pertenece, por razón de su objeto, al ámbito de aplicación de la Directiva 2004/48 ([129]).

El TJUE concluyó que debía interpretarse que las Directivas 2002/58 y 2004/48 no se oponían a la aplicación de una normativa nacional como la examinada en el procedimiento principal, en la medida en que dicha normativa permita al órgano jurisdiccional nacional que conozca de una acción por la que se solicite un requerimiento judicial de comunicación de datos de carácter personal ponderar, en función de las circunstancias de cada caso y con la debida observancia de las exigencias derivadas del principio de proporcionalidad, los intereses contrapuestos existentes.

1.3.6. Protección de datos e intereses económicos

En la era digital o la era de los macrodatos, se ha dicho que los datos son «el nuevo petróleo» de la economía para impulsar la innovación y la creatividad ([130]). Muchas empresas han desarrollado sólidos modelos de negocio en torno al tratamiento de datos, una actividad que a menudo conlleva tratar datos de carácter personal. Es posible que algunas empresas crean que determinadas normas aplicables a la protección de los datos personales pueden acarrear obligaciones excesivamente onerosas que pueden afectar a sus intereses económicos. De este modo, se plantea la cuestión de si los intereses económicos de los responsables y encargados del

([128]) Ibíd., apartado 40-41.

([129]) Ibíd., apartados 52-54. Véase también TJUE, C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU* [GS], 29 de enero de 2008, apartado 58.

([130]) Véase, por ejemplo, *Financial Times* (2016), «Data is the new oil... who's going to own it?», 16 de noviembre de 2016.

tratamiento o del público en general podrían justificar la limitación del derecho a la protección de los datos.

Ejemplo: En *Google Spain* ([131]), el TJUE resolvió que, en determinadas circunstancias, las personas físicas tienen derecho a solicitar a los motores de búsqueda que eliminen ciertos resultados de su índice de búsqueda. En su exposición de motivos, el TJUE apuntó el hecho de que el uso de motores de búsqueda y los resultados de las búsquedas pueden servir para crear un perfil detallado de la persona. Esta información puede afectar a multitud de aspectos de su vida privada que, sin dicho motor, no se habrían encontrado o interconectado fácilmente. Por tanto, constituía una injerencia potencialmente grave en los derechos fundamentales de los interesados al respeto de la vida privada y a la protección de los datos personales.

A continuación, el TJUE examinó si la injerencia podía estar justificada. Con respecto al interés económico de la empresa propietaria del motor de búsqueda en el tratamiento de los datos, el TJUE manifestó que «es obligado declarar que el mero interés económico del gestor de tal motor en este tratamiento no [...] justifica [la injerencia]» y que «en principio» los derechos fundamentales recogidos en los artículos 7 y 8 de la Carta prevalecen sobre dicho interés económico y el interés del público en general en encontrar esa información al realizar una búsqueda relativa al nombre del interesado ([132]).

Una de las consideraciones esenciales de la legislación europea sobre protección de datos es que las personas físicas tengan mayor control sobre sus datos personales. Especialmente en la era digital, existe un desequilibrio entre el poder de las entidades empresariales que llevan a cabo el tratamiento y tienen acceso a ingentes cantidades de datos de carácter personal y el poder de control sobre dichos datos de las personas a quienes pertenecen. El TJUE realiza un análisis caso por caso cuando se trata de ponderar la protección de datos y los intereses económicos, como los intereses de terceros en relación con sociedades anónimas y sociedades de responsabilidad limitada, como se ilustra en la sentencia *Manni*.

([131]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014.

([132]) Ibíd., apartados 81 y 97.

Ejemplo: El asunto *Manni* ([133]) trataba de la inscripción de los datos personales de una persona física en un registro mercantil público. El Sr. Manni había solicitado a la Cámara de Comercio de Lecce que eliminase sus datos personales de ese registro, tras descubrir que sus clientes potenciales podían acceder a él y ver que había sido administrador de una sociedad que se había declarado en quiebra hacía más de una década. Esta información influía negativamente en sus clientes potenciales y podía tener consecuencias perjudiciales para sus intereses comerciales.

Se solicitó al TJUE que determinase si el Derecho de la UE reconocía el derecho a la supresión de datos en ese caso. Para alcanzar su conclusión, el Tribunal ponderó la normativa de protección de datos de la UE y el interés comercial del Sr. Manni en que se eliminase la información relativa a la quiebra de su anterior empresa con el interés público del acceso a la información. Tomó debida nota del hecho de que la publicidad de los datos en el registro público de sociedades estaba establecida por la ley, y en particular por una Directiva de la UE que tenía por objeto facilitar el acceso de terceros a la información de las sociedades. Esta publicidad era importante para proteger los intereses de terceros que podrían tener intención de hacer negocios con una empresa concreta, dado que la única garantía que ofrecen las sociedades anónimas y las sociedades de responsabilidad limitada ante terceros es su patrimonio. Por tanto, «la publicidad debe permitir a los terceros conocer los actos esenciales de la sociedad y ciertas indicaciones relativas a ella, en particular la identidad de las personas que tienen el poder de obligarla» ([134]).

En vista de la importancia del fin legítimo perseguido por el registro, el TJUE resolvió que el Sr. Manni no tenía derecho a obtener la supresión de sus datos personales, ya que la necesidad de proteger los intereses de terceros en relación con las sociedades anónimas y las sociedades de responsabilidad limitada, así como de garantizar la seguridad jurídica, la lealtad de las transacciones comerciales y, de este modo, el buen funcionamiento del mercado interior, prevalecía sobre sus derechos en virtud de la normativa de protección de datos. Esto se justificaba especialmente en vista del hecho de que las personas que deciden participar en los intercambios económicos

([133]) TJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 9 de marzo de 2017.

([134]) Ibíd., apartado 49.

mediante una sociedad anónima o una sociedad de responsabilidad limitada son conscientes de que están obligadas a hacer públicos los datos relativos a su identidad y a sus funciones.

Pese a concluir que no había motivos para obtener la supresión de los datos en este caso, el TJUE reconoció la existencia del derecho de oposición al tratamiento de los datos, expresándose en los siguientes términos: «no es posible excluir que puedan existir situaciones particulares en las que razones preponderantes y legítimas propias de la situación concreta del interesado justifiquen excepcionalmente que el acceso a los datos personales que les conciernen, inscritos en el registro, se limite, al expirar un plazo suficientemente largo [...] a los terceros que justifiquen un interés específico en su consulta» ([135]).

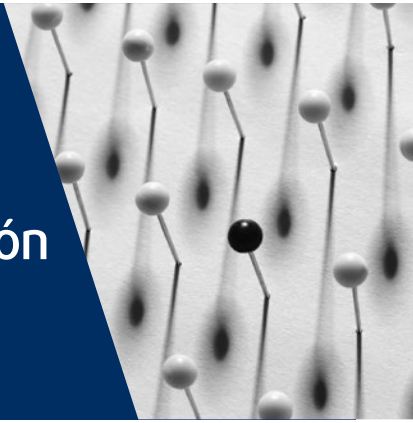
El TJUE declaró que corresponde a los órganos jurisdiccionales nacionales apreciar en cada caso, a la luz del conjunto de circunstancias pertinentes del interesado, la existencia o ausencia de razones preponderantes y legítimas que puedan justificar excepcionalmente la limitación del acceso de terceros a los datos personales contenidos en los registros de sociedades. Sin embargo, aclaró que, en el caso del Sr. Manni, el mero hecho de que la publicidad de sus datos personales en el registro supuestamente afectase a su clientela no podía considerarse una razón preponderante y legítima. Los clientes potenciales del Sr. Manni tienen un interés legítimo en la información relativa a la quiebra de su anterior empresa.

La injerencia en los derechos fundamentales del Sr. Manni y de otras personas incluidas en el registro al respeto de su vida privada y a la protección de sus datos personales, garantizados por los artículos 7 y 8 de la Carta, servía a un objetivo de interés general y era necesaria y proporcionada.

En *Manni*, por tanto, el TJUE resolvió que los derechos a la protección de los datos y a la vida privada no prevalecían sobre el interés de terceros en obtener acceso a la información contenida en el registro de sociedades en relación con las sociedades anónimas y sociedades de responsabilidad limitada.

([135]) Ibíd., apartado 60.

2 Terminología de protección de datos



UE	Materias tratadas	CdE
Datos personales		
Reglamento general de protección de datos, artículo 4, apartado 1 Reglamento general de protección de datos, artículo 4, apartado 5 y artículo 5, apartado 1, letra e). Reglamento general de protección de datos, artículo 9 TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 2010 TJUE, C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU* [GS], 2008 TJUE, C-70/10, *Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 TJUE, C-582/14, *Patrick Breyer contra Bundesrepublik Deutschland*, 2016 TJUE, asuntos acumulados C-141/12 y C-372/12, *YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel contra M y S*, 2014	Definición legal de protección de datos	Convenio 108 modernizado, artículo 2, letra a) TEDH, *Bernh Larsen Holding AS y otros contra Noruega*, n.º 24117/08, 2013 TEDH, *Uzun contra Alemania*, n.º 35623/05, 2010. TEDH, *Amann contra Suiza* [GS], n.º 27798/95, 2000

UE	Materias tratadas	CdE
TJUE, C-101/01, *Procedimiento penal entablado contra Bodil Lindqvist*, 2003	**Categorías especiales de datos personales (datos sensibles)**	Convenio 108 modernizado, artículo 6, apartado 1
TJUE, C-434/16, *Peter Nowak contra Data Protection Commissioner*, 2017	**Datos personales anonimizados y seudo-nimizados**	Convenio 108 modernizado, artículo 5, apartado 4, letra e) Informe explicativo del Convenio 108 modernizado, párrafo 50.
Tratamiento de datos		
Reglamento general de protección de datos, artículo 4, apartado 2 TJUE, C-212/13, *František Ryneš contra Úřad pro ochranu osobních údajů*, 2014 TJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 2017 TJUE, C-101/01, *Procedimiento penal entablado contra Bodil Lindqvist*, 2003 TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 2014	**Definiciones**	Convenio 108 modernizado, artículo 2, letras b) y c)
Usuarios de los datos		
Reglamento general de protección de datos, artículo 4, apartado 7 TJUE, C-212/13, *František Ryneš contra Úřad pro ochranu osobních údajů*, 2014 CJEU, C-1318/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 2014	**Responsable del tratamiento**	Convenio 108 modernizado, artículo 2, letra d) Recomendación sobre la creación de perfiles, artículo 1, letra g)*
Reglamento general de protección de datos, artículo 4, apartado 8	**Encargado del tratamiento**	Convenio 108 modernizado, artículo 2, letra f). Recomendación sobre la creación de perfiles, artículo 1, letra h)

UE	Materias tratadas	CdE
Reglamento general de protección de datos, artículo 4, apartado 9	**Destinatario**	Convenio 108 modernizado, artículo 2, letra e).
Reglamento general de protección de datos, artículo 4, apartado 10	**Tercero**	
Consentimiento		
Reglamento general de protección de datos, artículo 4, apartado 11, y artículo 7 TJUE, C-543/09, *Deutsche Telekom AG contra Bundesrepublik Deutschland*, 2011 TJUE, C-536/15, *Tele2 (Netherlands) BV y otros contra Autoriteit Consument en Markt (ACM)*, 2017	**Definición y requisitos para el consentimiento válido**	Convenio 108 modernizado, artículo 5, apartado 2 Recomendación sobre datos médicos, artículo 6, y diversas recomendaciones posteriores TEDH, *Elberte contra Letonia*, n.º 61243/08, 2015

*Nota: * Consejo de Europa, Comité de Ministros (2010), Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles (Recomendación sobre creación de perfiles), 23 de noviembre de 2010.*

2.1. Datos personales

Puntos clave

- Los datos son de carácter personal si están relacionados con una persona identificada o identificable: el «interesado».
- Para determinar si una persona física es identificable, el responsable del tratamiento u otra persona deberá tener en cuenta todos los medios razonables que puedan utilizarse —como la singularización— para identificar de forma directa o indirecta a la persona física.
- La autenticación implica demostrar que una determinada persona posee una determinada identidad y/o está autorizada a realizar determinadas actividades.
- Existen categorías especiales de datos, los denominados datos sensibles, recogidos en el Convenio 108 y en la legislación de la UE en materia de protección de datos, que exigen una protección reforzada y que, por lo tanto, están sujetos a un régimen jurídico especial.

- Los datos son anonimizados si ya no se refieren a una persona identificada o identificable.
- La seudonimización es una medida por la que no se pueden atribuir datos personales al interesado sin información adicional, que se conserva por separado. La «clave» que permite reidentificar a los titulares de los datos debe conservarse por separado y de manera segura. Los datos sometidos a un proceso de seudonimización siguen siendo datos personales. En el Derecho de la UE no existe el concepto de «datos seudonimizados».
- Los principios y normas de la protección de datos no se aplican a la información anonimizada. Sin embargo, sí se aplican a los datos seudonimizados.

2.1.1. Principales aspectos del concepto de datos personales

En el Derecho de la UE, así como **en el Derecho del CdE**, la definición de «datos personales» comprende toda información sobre una persona física identificada o identificable ([136]). Se refiere a información acerca de una persona cuya identidad sea manifiestamente clara o se pueda determinar a partir de información adicional. Para determinar si una persona es identificable, el responsable del tratamiento u otra persona deberá tener en cuenta todos los medios razonables que puedan utilizarse para identificar de manera directa o indirecta a la persona física, como por ejemplo la singularización, que permite tratar a una persona de forma diferente a otra ([137]).

Si se tratan datos de dicha persona, esta persona se denominará el «interesado».

El interesado

En el Derecho de la UE, las personas físicas son las únicas beneficiarias de las normas de protección de datos ([138]) y únicamente los seres vivos están protegidos por la legislación europea sobre protección de datos ([139]). El Reglamento general de protección de datos (RGPD) define los datos personales como toda información sobre una persona física identificada o identificable.

([136]) Reglamento general de protección de datos, artículo 4, apartado 1; Convenio 108 modernizado, artículo 2, letra a).

([137]) Reglamento general de protección de datos, considerando 26.

([138]) Ibíd., artículo 1.

([139]) Ibíd., considerando 27. Véase también Grupo de Trabajo del Artículo 29 (2007), *Dictamen 4/2007 sobre el concepto de datos personales*, WP 136, 20 de junio de 2007, p. 22.

El Derecho del CdE, en particular el Convenio 108 modernizado, también se refiere a la protección de las personas físicas en relación con el tratamiento de sus datos personales. También ahí se entiende por datos personales toda información sobre una persona física identificada o identificable. Esta persona física es conocida en la legislación sobre protección de datos como «el interesado».

Las personas jurídicas también gozan de cierta protección. Existe jurisprudencia del TEDH en relación con demandas de personas jurídicas que alegan la violación de su derecho a la protección contra el uso de sus datos, de conformidad con el artículo 8 del CEDH. El artículo 8 del CEDH comprende el derecho al respeto de la vida privada y familiar y también del domicilio y la correspondencia. Por tanto, el Tribunal puede examinar casos en virtud de este último derecho, en lugar del derecho a la vida privada.

Ejemplo: *Bernh Larsen Holding AS y otros contra Noruega* ([140]) trataba de una demanda presentada por tres empresas noruegas contra una resolución de la administración fiscal, que les ordenaba facilitar a los auditores fiscales una copia de todos los datos almacenados en un servidor que todas ellas utilizaban conjuntamente.

El TEDH determinó que dicha obligación de las empresas demandantes constituía una injerencia en sus derechos al respeto al «domicilio» y la «correspondencia», en virtud de lo dispuesto en el artículo 8 del CEDH. No obstante, el Tribunal dictaminó que las autoridades fiscales contaban con garantías efectivas y adecuadas contra los abusos: las empresas demandantes habían sido notificadas con bastante antelación; estuvieron presentes y pudieron realizar aportaciones durante la intervención *in situ*; y el material debía destruirse una vez finalizada la inspección fiscal. En esas circunstancias, se había logrado un equilibrio justo entre el derecho al respeto del «domicilio» y la «correspondencia» de las empresas demandantes y su interés en proteger la privacidad de las personas que trabajaban para ellas, por un lado, y el interés público de garantizar una inspección eficaz a efectos de la declaración de impuestos, por otro lado. El Tribunal resolvió que no había existido una violación del artículo 8.

([140]) TEDH, *Bernh Larsen Holding AS y otros contra Noruega*, n.º 24117/08, 14 de marzo de 2013. Véase asimismo, en cambio, TEDH, *Liberty y otros contra Reino Unido*, n.º 58243/00, 1 de julio de 2008.

De acuerdo con el Convenio 108 modernizado, la protección de datos tiene que ver fundamentalmente con la protección de las personas físicas, si bien las Partes Contratantes pueden extender dicha protección a personas jurídicas como empresas y asociaciones en su Derecho nacional. El Informe explicativo del Convenio modernizado establece que el Derecho nacional puede proteger los intereses legítimos de las personas jurídicas extendiendo el ámbito de aplicación del Convenio a estos agentes ([141]). La **legislación de la UE sobre protección de datos** no cubre el tratamiento de datos que conciernan a personas jurídicas, y en particular no afecta a las empresas establecidas como personas jurídicas, incluidos el nombre y la forma de la persona jurídica, así como sus datos de contacto ([142]) No obstante, la Directiva sobre la privacidad y las comunicaciones electrónicas sí protege la confidencialidad de las comunicaciones y los intereses legítimos de las personas jurídicas en relación con el incremento de la capacidad de almacenamiento y tratamiento automatizado de datos relativos a abonados y usuarios ([143]). Del mismo modo, el proyecto de Reglamento sobre la privacidad y las comunicaciones electrónicas extiende la protección a las personas jurídicas.

Ejemplo: En *Volker und Markus Schecke* ([144]), el TJUE, en relación con la publicación de los datos personales de los beneficiarios de ayudas agrícolas, sostuvo que «las personas jurídicas solo pueden acogerse a la protección de los artículos 7 y 8 de la Carta frente a dicha identificación en la medida en que en la razón social de la persona jurídica se identifique a una o varias personas físicas. [...E]l respeto del derecho a la vida privada en lo que respecta al tratamiento de los datos de carácter personal, reconocido por los artículos 7 y 8 de la Carta, se aplica a toda información sobre una persona física identificada o identificable [...]» ([145]).

Ponderando el interés de la UE de garantizar la transparencia en la concesión de las ayudas, por una parte, y los derechos fundamentales a la privacidad y la protección de los datos de las personas beneficiarias de dichas ayudas, por otra, el TJUE consideró que la injerencia en estos derechos fundamentales era

([141]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 30.

([142]) Reglamento general de protección de datos, considerando 14.

([143]) Directiva sobre la privacidad y las comunicaciones electrónicas, considerando 7 y artículo 1, apartado 2.

([144]) TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 9 de noviembre de 2010, apartado 53.

([145]) Ibíd., apartados 52-53.

desproporcionada. Consideró que el objetivo de transparencia se podría haber logrado de manera efectiva con medidas menos invasivas para los derechos de las personas afectadas. Sin embargo, al examinar la proporcionalidad de la publicación de información relativa a personas jurídicas receptoras de ayudas, el TJUE alcanzó una conclusión diferente y resolvió que dicha publicación no sobrepasaba los límites del principio de proporcionalidad. Declaró que «para las personas jurídicas, la gravedad de la lesión del derecho a la protección de sus datos de carácter personal se presenta de forma diferente que para las personas físicas» ([146]). Las personas jurídicas estaban sujetas a obligaciones más onerosas en relación con la publicación de información sobre ellas. El TJUE consideró que supondría una carga administrativa desmesurada para las autoridades nacionales competentes obligarlas a examinar si los datos de cada persona jurídica identifican a alguna persona jurídica beneficiaria de ayudas, antes de publicar tales datos. Por lo tanto, la legislación que exigía una publicación generalizada de los datos relativos a personas jurídicas respetaba un justo equilibrio entre los intereses enfrentados.

Naturaleza de los datos

Cualquier tipo de información puede ser considerada datos personales siempre que estos hagan referencia a una persona identificada o identificable.

Ejemplo: La evaluación del desempeño laboral de un empleado por parte de un superior, conservada en el expediente laboral del empleado, son datos personales acerca del empleado. Esto es así aunque puedan reflejar únicamente, en todo o en parte, la opinión personal del superior, como por ejemplo: «el empleado no muestra dedicación por su trabajo»; en lugar de hechos concretos, como sería: «el empleado se ha ausentado del trabajo durante cinco semanas en los últimos seis meses».

Los datos personales comprenden información relativa a la vida privada de una persona, que también incluye sus actividades profesionales, así como información sobre su vida pública.

([146]) Ibíd., apartado 87.

En *Amann* ([147]), el TEDH interpretó que el término «datos personales» no se limitaba a las cuestiones del ámbito privado de una persona física. Este significado del término «datos personales» también es relevante para el RGPD.

Ejemplo: En *Volker und Markus Schecke* ([148]), el TJUE declaró que «[a] este respecto es irrelevante el hecho de que los datos publicados se refieran a actividades profesionales [...]. El Tribunal Europeo de Derechos Humanos ha declarado a este respecto, en referencia a la interpretación del artículo 8 del Convenio 108, que los términos "vida privada" no debían interpretarse restrictivamente y que "ninguna razón de principio permite excluir las actividades profesionales [...] del concepto de "vida privada"».

Ejemplo: En los asuntos acumulados *YS contra Minister voor Immigratie, Integratie en Asiel* y *Minister voor Immigratie, Integratie en Asiel contra M y S* ([149]), el TJUE declaró que el análisis jurídico incluido en un proyecto de resolución del servicio de inmigración y naturalización relativo a las solicitudes de permisos de residencia no constituye en sí mismo un dato personal, aunque puede incluir datos personales.

La jurisprudencia del TEDH relativa al artículo 8 del CEDH confirma que puede resultar difícil separar completamente los aspectos de la vida privada y de la vida profesional ([150]).

Ejemplo: En *Bărbulescu contra Rumanía* ([151]), el demandante había sido despedido por utilizar la internet de su empleador en horario laboral vulnerando el reglamento interno. Su empleador había vigilado sus comunicaciones y presentó las grabaciones, que recogían mensajes de carácter puramente privado, durante el procedimiento nacional. El TEDH resolvió que el artículo 8 era de aplicación y dejó abierta la cuestión de si el restrictivo reglamento del empleador dejaba al demandante una

([147]) Véase TEDH, *Amann contra Suiza* [GS], n.º 27798/95, 16 de febrero de 2000, apartado 65.

([148]) TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 9 de noviembre de 2010, apartado 59.

([149]) TJUE, asuntos acumulados C-141/12 y C-372/12, *YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel contra M y S*, 17 de julio de 2014, apartado 39.

([150]) Véase, por ejemplo, TEDH, *Rotaru contra Rumanía* [GS], n.º 28341/95, 4 de mayo de 2000, apartado 43; TEDH, *Niemietz contra Alemania*, n.º 13710/88, 16 de diciembre de 1992, apartado 29.

([151]) TEDH, *Bărbulescu contra Rumanía* [GS], n.º 61496/08, 5 de septiembre de 2017, apartado 121.

expectativa razonable de privacidad, pero en cualquier caso determinó que las instrucciones del empleador no podían reducir a cero la vida social privada en el lugar de trabajo. En lo que respecta al fondo del asunto, se debía otorgar a los Estados Contratantes un amplio margen de apreciación para determinar la necesidad de establecer un marco jurídico que reglamentase las condiciones en las que un empleador podía regular las comunicaciones no profesionales de sus empleados —por medios electrónicos u otros— en el lugar de trabajo. No obstante, las autoridades nacionales debían asegurarse de que la introducción por parte de un empleador de medidas de vigilancia de la correspondencia y otras comunicaciones, al margen del alcance y duración de tales medidas, fuera acompañada de garantías adecuadas y suficientes contra los abusos. Era esencial respetar la proporcionalidad y disponer de garantías procesales contra la arbitrariedad y el TEDH señaló una serie de factores pertinentes en las circunstancias en cuestión. Estos factores incluían, por ejemplo, el alcance de la vigilancia de los empleados por parte del empleador y el grado de invasión de la privacidad del empleado, las consecuencias para este último y si se habían establecido garantías adecuadas. Además, las autoridades nacionales debían garantizar que un empleado cuyas comunicaciones hubieran sido objeto de vigilancia dispusiera de un recurso ante un órgano judicial con jurisdicción para determinar, al menos en el fondo, cómo se habían respetado los criterios establecidos y si las medidas impugnadas eran lícitas. En este caso, el TEDH resolvió que existía una violación del artículo 8 porque las autoridades nacionales no habían protegido adecuadamente el derecho del demandante al respeto de su vida privada y su correspondencia y, en consecuencia, no habían alcanzado un equilibrio justo entre los intereses enfrentados.

Tanto en el **Derecho de la Unión Europea** como en el **Derecho del CdE**, la información contiene datos sobre una persona si:

- la persona es identificada o identificable con esta información; o
- en dicha información se singulariza a la persona, aunque no se identifique, de manera que fuera posible averiguar quién es el interesado si se llevara a cabo una mayor investigación.

Ambos tipos de información están protegidos del mismo modo por la legislación europea en materia de protección de datos. La identificabilidad directa o indirecta

de las personas físicas requiere una apreciación continua, «teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos» ([152]). El TEDH ha declarado en repetidas ocasiones que el concepto de «datos personales» con arreglo al CEDH es el mismo que el que se contempla en el Convenio 108, en especial por lo que respecta a la condición de que se refieran a personas identificadas o identificables ([153]).

El RGPD establece que una persona física es identificable cuando su «identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» ([154]). Por lo tanto, la identificación requiere elementos que describan a una persona de un modo que permita distinguirla de todas las demás y reconocerla de forma individual. El nombre de una persona es un ejemplo excelente de tales elementos descriptivos y puede identificar directamente a una persona. En algunos casos, otros atributos pueden tener efectos similares a los del nombre y hacer que una persona sea identificable directamente. El número de teléfono, el número de la seguridad social o el número de matrícula de un vehículo son ejemplos de datos que pueden hacer que una persona sea identificable. También es posible utilizar atributos —como archivos informáticos, *cookies* y herramientas de control de tráfico web— para singularizar a las personas físicas identificando su comportamiento y sus hábitos. Como se explica en un dictamen del Grupo de Trabajo del Artículo 29, «[s]in ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos, o de otro tipo, y atribuirle determinadas decisiones, puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto» ([155]). La definición de datos personales, tanto en el Derecho de la UE como en el Derecho del CdE, es suficientemente amplia para abarcar todas las posibilidades de identificación (y, por tanto, todos los grados de identificabilidad).

([152]) Reglamento general de protección de datos, considerando 26.

([153]) Véase TEDH, *Amann contra Suiza* [GS], n.º 27798/95, 16 de febrero de 2000, apdo. 65.

([154]) Reglamento general de protección de datos, artículo 4, apartado 1.

([155]) Grupo de Trabajo del Artículo 29, *Dictamen 4/2007 sobre el concepto de datos personales*, WP 136, 20 de junio de 2007, p. 15.

Ejemplo: En *Promusicae contra Telefónica de España* ([156]), el TJUE declaró que «[t]ampoco se discute que la comunicación de los nombres y direcciones de determinados usuarios de [una determinada plataforma de intercambio de archivos por internet] implique la comunicación de datos personales, es decir, de información sobre las personas físicas identificadas o identificables, conforme a la definición que figura en el artículo 2, letra a), de la Directiva 95/46 [actualmente el artículo 4, apartado 1, del RGPD]. Esta comunicación de datos que, según Promusicae, almacena Telefónica —cuestión que ésta no niega—, constituye un tratamiento de datos personales» ([157]).

Ejemplo: *Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* ([158]) trataba de la negativa del proveedor de servicios de internet de instalar un sistema de filtrado de las comunicaciones electrónicas que utilizan los programas de intercambio de archivos para evitar que se compartan archivos vulnerando los derechos de autor protegidos por SABAM, una empresa de gestión que representa a autores, compositores y editores. El TJUE resolvió que las direcciones IP de los usuarios «son datos protegidos de carácter personal, ya que permiten identificar concretamente a tales usuarios».

Dado que muchos nombres no son únicos, es posible que para establecer la identidad de una persona sean necesarios otros atributos que garanticen que no se confunda a una persona con otra. A veces, puede ser necesario combinar atributos directos e indirectos para identificar a la persona a la que se refiere la información. Con frecuencia se utiliza la fecha y el lugar de nacimiento. Además, en algunos países se han introducido números personalizados para distinguir mejor a los ciudadanos. Los datos fiscales transferidos ([159]), los datos relativos al solicitante de un documento de residencia incluido en un documento administrativo ([160]) y los documentos

([156]) TJUE, C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU* [GS], 29 de enero de 2008, apartado 45.

([157]) Antigua Directiva 95/46, artículo 2, letra b), actual Reglamento general de protección de datos, artículo 4, apartado 2.

([158]) TJUE, C-70/10, *Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 de noviembre de 2011, apartado 51.

([159]) TJUE, C-201/14, *Smaranda Bara y otros contra Casa Națională de Asigurări de Sănătate y otros*, 1 de octubre de 2015.

([160]) TJUE, asuntos acumulados C-141/12 y C-372/12, *YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel contra M y S*, 17 de julio de 2014.

relativos a relaciones bancarias y fiduciarias ([161]) pueden ser datos personales. Los datos biométricos, como las impresiones dactilares, fotografías digitales o imágenes del iris, los datos de localización y los atributos en línea se utilizan cada vez más para identificar a las personas en la era tecnológica.

En lo que atañe a la aplicabilidad de la legislación europea en materia de protección de datos, sin embargo, no es necesaria la propia identificación del interesado, sino que basta que la persona en cuestión sea identificable. Se considera que una persona es identificable si se dispone de elementos suficientes para identificar a la persona de forma directa o indirecta ([162]). De conformidad con el considerando 26 del RGPD, el criterio de referencia es si puede ser que los usuarios previsibles de la información tengan a su disposición y administren medios razonables de identificación, entre los que se incluye la información que obre en poder de los terceros destinatarios (véase la sección 2.3.2).

Ejemplo: Una autoridad local decide recopilar datos de los automóviles que circulan por las calles de su localidad. Para ello, toma fotografías de los automóviles, grabando automáticamente la hora y la ubicación, para pasar dichos datos a la autoridad competente, de forma que esta pueda imponer multas a quienes han infringido los límites de velocidad. Un interesado presenta una reclamación, alegando que la autoridad local carece de base jurídica para recopilar esos datos con arreglo a la legislación en materia de protección de datos. La autoridad local mantiene que no recopila datos personales. Las matrículas, afirma, son anónimas. La autoridad local no está legalmente autorizada a acceder al registro general de vehículos a fin de descubrir la identidad del propietario o del conductor del automóvil.

Este razonamiento no es conforme con el considerando 26 del RGPD. Dado que la finalidad de la recopilación de datos es claramente identificar y sancionar a los conductores que circulan a una velocidad excesiva, es previsible que se intente su identificación. Aunque las autoridades locales no disponen directamente de medios de identificación, transmiten los datos a la autoridad competente, la policía, que sí dispone de esos medios. En el considerando 26 también se menciona de manera expresa una situación en la que es previsible que otros destinatarios de los datos, distintos del usuario inmediato de estos, puedan intentar identificar a la persona física. En vista

([161]) TEDH, *M.N. y otros contra San Marino*, n.º 28005/12, 7 de julio de 2015.

([162]) Reglamento general de protección de datos, artículo 4, apartado 1.

de lo dispuesto en el considerando 26, la actuación de la autoridad local equivale a recopilar datos sobre personas identificables y, por tanto, exige la existencia de una base jurídica con arreglo a la legislación en materia de protección de datos.

Para «determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos» ([163]).

Ejemplo: En *Breyer contra Bundesrepublik Deutschland* ([164]), el TJUE examinó el concepto de la identificabilidad indirecta de los interesados. El asunto trataba de las direcciones IP dinámicas, que cambian cada vez que se establece una nueva conexión a internet. Los sitios web gestionados por las instituciones federales alemanas registraban y almacenaban las direcciones IP dinámicas para evitar ataques cibernéticos y para ejercitar acciones penales en caso necesario. Solo el proveedor de servicios de internet que utilizaba Mr. Breyer disponía de la información adicional necesaria para identificarle.

El TJUE consideró que una dirección IP dinámica, que un proveedor de servicios de medios en línea registra cuando una persona accede a un sitio web que dicho proveedor hace accesible al público, constituye datos personales cuando solo un tercero —el proveedor de servicios de internet en este caso— tiene los datos adicionales necesarios para identificar a esa persona ([165]). Sostuvo que «no es necesario que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona» para que la información sea constitutiva de datos personales. Los usuarios de una dirección IP dinámica registrada por un proveedor de servicios de internet pueden ser identificados en determinadas situaciones, por ejemplo en el marco de un proceso penal en caso de ataques cibernéticos,

([163]) Ibíd., considerando 26.

([164]) TJUE, C-582/14, *Patrick Breyer contra Bundesrepublik Deutschland*, 19 de octubre de 2016, apartado 43.

([165]) Antigua 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, artículo 2, letra a).

con la ayuda de otras personas ([166]). Según el TJUE, cuando el proveedor «disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a internet de dicha persona», esto constituiría «un medio que pueda ser razonablemente utilizado para identificar al interesado». Por tanto, estos datos se consideran datos de carácter personal.

Según el Derecho del CdE, la identificabilidad debe entenderse de un modo similar. El Informe explicativo del Convenio 108 modernizado incluye una descripción similar: el concepto de «identificable» no solo se refiere a la identidad civil o jurídica de la persona física como tal, sino también a lo que puede permitir que una persona sea «individualizada» o singularizada respecto de los demás y, en consecuencia, que pueda recibir un trato diferente. Esta «individualización» podría efectuarse, por ejemplo, haciendo referencia a esa persona en concreto, o a un dispositivo o conjunto de dispositivos (ordenador, teléfono móvil, cámara, dispositivos de juegos, etc.) vinculado a un número de identificación, un seudónimo, datos biométricos o genéticos, datos de localización, una dirección IP u otro identificador ([167]). Una persona física no se considera «identificable» si su identificación requiere dedicar tiempo, esfuerzo o recursos más allá de lo razonable. Este es el caso, por ejemplo, cuando para identificar al interesado serían necesarias operaciones excesivamente complejas, prolongadas en el tiempo y costosas. La apreciación de si el tiempo, el esfuerzo o los recursos dedicados van más allá de lo razonable o no es algo que debe determinarse caso por caso teniendo en cuenta factores como la finalidad del tratamiento, los costes y beneficios de la identificación, el tipo de responsable del tratamiento y la tecnología utilizada ([168]).

En cuanto a la forma de conservación o uso de los datos personales, es importante señalar que no es relevante para la aplicabilidad de la legislación sobre protección de datos. Las comunicaciones escritas o habladas pueden incluir datos personales

([166]) TJUE, C-70/10, *Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 de noviembre de 2011, apartados 47-48.

([167]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 18.

([168]) Ibíd., apartado 16.

y también imágenes ([169]), en particular las filmaciones ([170]) o el sonido ([171]) de un sistema de circuito cerrado de televisión (CCTV). La información grabada por medios electrónicos y la información en papel también pueden ser datos de carácter personal. Incluso las muestras de tejido humano —que contienen el ADN de una persona— pueden ser fuentes de datos biométricos ([172]), en la medida en que estos datos están relacionados con las características genéticas heredadas o adquiridas de una persona física, proporcionan información única acerca de su salud o fisiología y se obtienen del análisis de una muestra biológica de esa persona ([173]).

Anonimización

En virtud del principio de limitación de la conservación incluido tanto en el RGPD como en el Convenio 108 modernizado (que se aborda con más detalle en el capítulo 3), los datos deben mantenerse «de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales» ([174]). En consecuencia, los datos deberán eliminarse o anonimizarse en el caso de que un responsable del tratamiento desee almacenarlos una vez que dejen de ser necesarios y de servir para su propósito inicial.

El proceso de anonimización de los datos consiste en eliminar todos los elementos identificativos de un conjunto de datos personales para que ya no sea posible identificar al interesado ([175]). En su dictamen 05/2014, el Grupo de Trabajo del Artículo 29 analiza la eficacia y los límites de las diferentes técnicas de anonimización ([176]). Reconoce la utilidad potencial de este tipo de técnicas, pero destaca que algunas de ellas

([169]) TEDH, *Von Hannover contra Alemania*, n.º 59320/00, 24 de junio de 2004; TEDH, *Sciacca contra Italia*, n.º 50774/99, 11 de enero de 2005; TJUE, C-212/13, *František Ryneš contra Úřad pro ochranu osobních údajů*, 11 de diciembre de 2014.

([170]) TEDH, *Peck contra Reino Unido*, n.º 44647/98, 28 de enero de 2003; TEDH, *Köpke contra Alemania* (dic.), n.º 420/07, 5 de octubre de 2010; SEPD (2010), *Directrices de videovigilancia del SEPD*, 17 de marzo de 2010.

([171]) TEDH, *P.G. y J.H. contra Reino Unido*, n.º 44787/98, 25 de septiembre de 2001, apartados 59-60; TEDH, *Wisse contra Francia*, n.º 71611/01, 20 de diciembre de 2005 (versión en francés).

([172]) Véase Grupo de Trabajo del Artículo 29 (2007), *Dictamen 4/2007 sobre el concepto de datos personales*, WP136, 20 de junio de 2007, p. 9; Consejo de Europa, Recomendación Rec(2006) 4 del Comité de Ministros a los Estados miembros sobre la investigación con materiales biológicos de origen humano, 15 de marzo de 2006.

([173]) Reglamento general de protección de datos, artículo 4, apartado 13.

([174]) Ibíd., artículo 5, apartado 1, letra e); Convenio 108 modernizado, artículo 5, apartado 2, letra e).

([175]) Reglamento general de protección de datos, considerando 26.

([176]) Grupo de Trabajo del Artículo 29 (2014), *Dictamen 5/2014 sobre técnicas de anonimización*, WP 216, 10 de abril de 2014.

no funcionan necesariamente en todos los casos. Para hallar la solución óptima en una situación concreta, deberá decidirse el proceso de anonimización adecuado en cada caso. Sea cual sea la técnica utilizada, la identificación debe hacerse imposible de manera irreversible. Esto significa que, para que los datos sean anonimizados, no puede quedar en la información ningún elemento que pueda servir para reidentificar a los interesados haciendo un esfuerzo razonable ([177]). El riesgo de reidentificación se puede determinar teniendo en cuenta «el tiempo, el esfuerzo o los recursos necesarios en vista del carácter de los datos, el contexto de su uso, las tecnologías de reidentificación disponibles y los costes correspondientes» ([178]).

Cuando los datos han sido adecuadamente anonimizados, dejan de ser datos personales y la legislación en materia de protección de datos ya no es de aplicación.

El RGPD establece que no se puede obligar a la persona u organización responsable del tratamiento de los datos personales a mantener, adquirir o tratar información adicional para identificar al interesado con la única finalidad de cumplir con lo dispuesto en el Reglamento. Sin embargo, esta norma tiene una exención importante: cuando el interesado, con el fin de ejercer sus derechos de acceso, rectificación, supresión, limitación del tratamiento y portabilidad de los datos, facilite información adicional al responsable del tratamiento que permita su identificación, entonces los datos que se hubieran anonimizado anteriormente volverán a tener la consideración de datos de carácter personal ([179]).

Seudonimización

Los datos de carácter personal contienen atributos como el nombre, la fecha de nacimiento, el sexo, el domicilio u otros elementos que pueden hacer posible la identificación. El proceso de seudonimización de los datos personales implica que estos atributos se sustituyen por un seudónimo.

El Derecho de la UE define la «seudonimización» como «el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que

([177]) Reglamento general de protección de datos, considerando 26.

([178]) Consejo de Europa (2007), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, 23 de enero de 2017, apartado 6.2.

([179]) Reglamento general de protección de datos, artículo 11.

los datos personales no se atribuyan a una persona física identificada o identificable» ([180]). Al contrario que los datos anonimizados, los datos seudonimizados siguen siendo datos personales y, por tanto, sujetos a la legislación en materia de protección de datos. Aunque la seudonimización puede reducir los riesgos para la seguridad de los interesados, no está exenta del ámbito de aplicación del RGPD.

El RGPD reconoce varios usos de la seudonimización como medida técnica adecuada para reforzar la protección de los datos y se menciona en particular para el diseño y la seguridad de su tratamiento ([181]). Constituye asimismo una salvaguardia adecuada que se podría utilizar para tratar datos personales con fines distintos de aquellos para los que se recabaron inicialmente los datos ([182]).

La seudonimización no se menciona expresamente en la definición legal del Convenio 108 modernizado del **CdE**. Sin embargo, el Informe explicativo del Convenio 108 modernizado establece claramente que «el uso de un seudónimo o de cualquier identificador/identidad digital no acarrea la anonimización de los datos ya que todavía es posible identificar o individualizar al interesado» ([183]). Una manera de seudonimizar los datos es el cifrado. Una vez seudonimizados los datos, el vínculo con la identidad existe en forma del seudónimo más una clave de descifrado. Sin esa clave, es difícil identificar los datos seudonimizados. Sin embargo, las personas autorizadas a utilizar la clave de descifrado pueden efectuar la reidentificación fácilmente. El uso de las claves de cifrado por parte de personas no autorizadas deberá estar especialmente protegido. Por tanto, «[l]os datos seudonimizados deben [...] considerarse datos personales [...]» regulados por el Convenio 108 modernizado ([184]).

Autenticación

Se trata de un procedimiento mediante el cual una persona es capaz de demostrar que posee una determinada identidad o que está autorizada para realizar determinadas tareas, como acceder a una zona de seguridad o retirar dinero de una cuenta bancaria. La autenticación se puede llevar a cabo comparando datos biométricos, como una foto o las impresiones dactilares de un pasaporte, con los datos de

([180]) Ibíd., art. 4 (5).

([181]) Ibíd., artículo 25, apartado 1.

([182]) Ibíd., artículo 6, apartado 4.

([183]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 17.

([184]) Ibíd.

la persona que se presenta, por ejemplo, en un control de inmigración ([185]); o bien solicitando información que solo pudiera conocer la persona que tuviera una determinada identidad o autorización, como un número de identificación personal (PIN) o una contraseña; o bien exigiendo la presentación de un dispositivo determinado, que debe estar exclusivamente en posesión de la persona que tiene una determinada identidad o autorización, como una tarjeta con un chip especial o una llave de una caja de seguridad bancaria. Aparte de las contraseñas o de las tarjetas con chip —a veces unidas a un PIN—, la firma electrónica es un instrumento capaz de identificar y autenticar a una persona en las comunicaciones electrónicas.

2.1.2. Categorías especiales de datos personales

Tanto **en el Derecho de la UE** como **en el Derecho del CdE**, existen categorías especiales de datos personales que, por su carácter, pueden suponer un riesgo para los interesados cuando son objeto de tratamiento y necesitan una protección reforzada. Estos datos están sujetos a un principio de prohibición y existe un número limitado de condiciones en las que dicho tratamiento es lícito.

En el marco del Convenio 108 modernizado (artículo 6) y del RGPD (artículo 9), las siguientes categorías se consideran datos sensibles:

- datos personales que revelan el origen racial o étnico;
- datos personales que revelan opiniones políticas, creencias religiosas y otras creencias, incluidas las filosóficas;
- datos personales que revelan la pertenencia a un sindicato;
- datos genéticos y datos biométricos tratados con el fin de identificar a una persona;
- datos personales relativos a la salud, la vida sexual o la orientación sexual.

([185]) Ibíd., apartados 56-57.

Ejemplo: *Bodil Lindqvist* ([186]) trataba de la mención de diferentes personas por su nombre o por otros medios, como su número de teléfono o información sobre sus aficiones, en una página de internet. El TJUE declaró que «la indicación de que una persona se haya lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud» ([187]).

Datos personales relativos a delitos y condenas penales

El Convenio 108 modernizado incluye datos personales relativos a delitos, procesos y condenas penales, y las medidas de seguridad relacionadas, en la lista de categorías especiales de datos personales ([188]). En el marco del RGPD, los datos personales relativos a condenas y delitos penales o medidas de seguridad conexas no aparecen mencionados como tal en la lista de categorías especiales de datos, pero se abordan en un artículo específico. El artículo 10 del RGPD establece que el tratamiento de estos datos solo podrá llevarse a cabo «bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados». Por otra parte, solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas ([189]). En la UE, el tratamiento de datos personales en el contexto de los cuerpos de seguridad se rige por un instrumento jurídico específico: la Directiva 2016/680/UE ([190]). Esta Directiva contiene disposiciones específicas sobre protección de datos, que son vinculantes para las autoridades competentes en el tratamiento de datos personales con los fines específicos de prevención, investigación, detección y enjuiciamiento de infracciones penales (véase la sección 8.2.1).

([186]) TJUE, C-101/01, *Procedimiento penal entablado contra Bodil Lindqvist*, 6 de noviembre de 2003, apartado 51.

([187]) Antigua Directiva 95/46/CE, artículo 8, apartado 1, actual Reglamento general de protección de datos, artículo 9, apartado 1.

([188]) Convenio 108 modernizado, artículo 6, apartado 1.

([189]) Reglamento general de protección de datos, artículo 10.

([190]) 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 2016 L 119.

2.2. Tratamiento de datos

Puntos clave

- Por «tratamiento de datos» se entiende cualquier operación realizada con datos personales.
- El término «tratamiento» comprende el tratamiento automatizado y no automatizado.
- En el Derecho de la UE, el «tratamiento» se refiere, además, al tratamiento manual en ficheros estructurados.
- En el Derecho del CdE, el significado de «tratamiento» puede ser ampliado por el Derecho nacional a fin de incluir el tratamiento manual.

2.2.1. El concepto de tratamiento de datos

El concepto de tratamiento de datos personales es muy amplio **tanto en el Derecho de la UE como en el Derecho del CdE**: «"tratamiento" [...] cualquier operación [...] como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación supresión o destrucción» ([191]) de datos personales. El Convenio 108 modernizado añade la preservación de los datos personales a la definición ([192]).

Ejemplo: En *František Ryneš* ([193]), el Sr. Ryneš captó la imagen de dos personas que rompieron ventanas de su vivienda por medio del sistema doméstico de vigilancia por CCTV que había instalado para proteger su propiedad. El TJUE determinó que la grabación y conservación de datos personales por medio del sistema de videovigilancia constituye un tratamiento de datos automatizado que está comprendido en el ámbito de aplicación de la legislación de la UE en materia de protección de datos.

([191]) Reglamento general de protección de datos, artículo 4, apartado 2. Véase asimismo Convenio 108 modernizado, artículo 2, letra b).

([192]) Convenio 108 modernizado, artículo 2, letra b).

([193]) TJUE, C-212/13, *František Ryneš contra Úřad pro ochranu osobních údajů*, 11 de diciembre de 2014, apartado 25.

Ejemplo: En *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni* ([194]), el Sr. Manni solicitó que se eliminasen sus datos personales del registro de una empresa de calificación crediticia que le vinculaba a la liquidación de una empresa inmobiliaria, con menoscabo de su reputación. El TJUE resolvió que «al transcribir y conservar esta información en el registro y al comunicarla, en su caso, a terceros previa petición, la autoridad encargada de éste lleva a cabo un "tratamiento de datos personales" del que es "responsable"».

Ejemplo: Los empresarios recopilan y tratan datos acerca de sus empleados, incluida la información relativa a sus salarios. Sus contratos de trabajo establecen los fundamentos jurídicos para poder hacerlo de manera legítima.

Los empresarios deben remitir los datos relativos a los salarios de su personal a la administración fiscal. Esta transmisión de datos también se considerará «tratamiento» en el sentido que dicho término posee en el Convenio 108 y en el RGPD. Pero el fundamento jurídico de esta revelación no está en el contrato de trabajo. Debe existir una base jurídica adicional para las operaciones de tratamiento que tengan como resultado la transmisión de los datos relativos al salario por parte de los empresarios a la administración fiscal. Dicha base jurídica suele encontrarse en las disposiciones de las legislaciones fiscales nacionales. Sin estas disposiciones —y en ausencia de otros motivos legítimos para el tratamiento—, esta transmisión de datos personales sería un tratamiento ilícito.

2.2.2. Tratamiento de datos automatizado

La protección de datos en virtud del Convenio 108 modernizado y el RGPD se aplica plenamente al tratamiento de datos automatizado.

En el **Derecho de la UE**, el tratamiento de datos automatizado consiste en operaciones de «tratamiento total o parcialmente automatizado de datos personales» ([195]). El

([194]) TJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 9 de marzo de 2017, apartado 35.

([195]) Reglamento general de protección de datos, artículo 2, apartado 1, y artículo 4, apartado 2.

Convenio 108 modernizado incluye una definición parecida ([196]). En la práctica, esto significa que cualquier tratamiento de datos personales realizado por medios automatizados con ayuda, por ejemplo, de un ordenador personal, un dispositivo móvil o un enrutador, está sujeto a las normas de protección de datos de la UE y del CdE.

Ejemplo: *Bodil Lindqvist* ([197]) trataba de la mención de diferentes personas por su nombre o por otros medios, como su número de teléfono o información sobre sus aficiones, en una página de internet. El TJUE resolvió que «la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46» ([198]).

Ejemplo: En *Google Spain SL, Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González* ([199]), el Sr. González solicitó que se eliminase o modificase un enlace entre su nombre en el motor de búsqueda de Google y dos páginas que anunciaban una subasta de inmuebles para cobrar deudas con la seguridad social. El TJUE declaró que «al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda "recoge" tales datos que "extrae", "registra" y "organiza" posteriormente en el marco de sus programas de indexación, "conserva" en sus servidores y, en su caso, "comunica" y "facilita el acceso" a sus usuarios en forma de listas de resultados de sus búsquedas» ([200]). El TJUE concluye que estas acciones constituyen «tratamiento», «sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales».

([196]) Convenio 108 modernizado, artículo 2, letras b) y c); Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 21.

([197]) TJUE, C-101/01, *Procedimiento penal entablado contra Bodil Lindqvist*, 6 de noviembre de 2003, apartado 27.

([198]) Reglamento general de protección de datos, artículo 2, apartado 1.

([199]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014.

([200]) Ibíd., apartado 28.

2.2.3. Tratamiento de datos no automatizado

El tratamiento de datos manual también requiere protección.

La protección de datos **en el Derecho de la UE** no se limita en modo alguno al tratamiento de datos automatizado. En consecuencia, con arreglo a la legislación de la UE, la protección de datos se aplica al tratamiento de datos personales en un fichero manual, es decir, en un fichero en papel especialmente estructurado ([201]). Un fichero estructurado es aquel que clasifica un conjunto de datos personales, de modo que sean accesibles en virtud de determinados criterios. Por ejemplo, si una empresa mantiene un expediente titulado «bajas de empleados», que contiene todos los datos de las bajas que han tenido los empleados durante el último año y que está clasificado por orden alfabético, este expediente constituirá un fichero manual sujeto a las normas de protección de datos de la UE. El motivo de esta ampliación de la protección de datos es que:

- los ficheros en papel pueden estructurarse de modo que faciliten y agilicen la búsqueda de información;

- el almacenamiento de datos personales en ficheros en papel estructurados hace que sea más sencillo eludir las limitaciones establecidas legalmente para el tratamiento de datos automatizado ([202]).

Con arreglo al **Derecho del CdE**, la definición de tratamiento automatizado reconoce que en algunas fases del uso manual de los datos personales puede ser necesario realizar operaciones automatizadas ([203]). El artículo 2, letra c) del Convenio 108 modernizado establece que «(c)uando no se utilice el tratamiento automatizado, se entenderá por tratamiento de datos un conjunto de operaciones realizadas con datos personales dentro de un conjunto estructurado de tales datos que sean accesibles o recuperables en virtud de determinados criterios».

([201]) Reglamento general de protección de datos, artículo 2, apartado 1.

([202]) Reglamento general de protección de datos, considerando 15.

([203]) Convenio 108 modernizado, artículo 2, letras b) y c).

2.3. Usuarios de datos personales

Puntos clave

- La persona a quien corresponde determinar los medios y fines del tratamiento de los datos personales de otras personas es el «responsable del tratamiento» conforme a la legislación en materia de protección de datos; si varias personas toman esta decisión conjuntamente, podrán ser «corresponsables del tratamiento».
- Un «encargado del tratamiento» es una persona física o jurídica que trata datos personales por cuenta del responsable del tratamiento.
- El encargado del tratamiento pasa a ser el responsable del tratamiento si es él mismo quien determina los medios y fines del tratamiento de los datos.
- Cualquier persona a quien se comunican datos personales es un «destinatario».
- Un «tercero» es una persona física o jurídica distinta del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.
- El consentimiento como base jurídica para el tratamiento de datos personales debe ser otorgado de manera libre, específica, informada e inequívoca por medio de una clara acción afirmativa que signifique aceptación del tratamiento.
- El tratamiento de categorías especiales de datos sobre la base del consentimiento exige que este sea un consentimiento explícito.

2.3.1. Responsables del tratamiento y encargados del tratamiento

La consecuencia más importante de ser un responsable del tratamiento o un encargado del tratamiento es la responsabilidad jurídica de cumplir con las obligaciones respectivas, de conformidad con la legislación en materia de protección de datos. En el sector privado, estas suelen ser personas físicas o jurídicas, mientras que en el sector público normalmente se trata de una autoridad. Existe una diferencia importante entre el responsable del tratamiento y el encargado del tratamiento: el primero es la persona física o jurídica que determina los fines y medios del tratamiento, mientras que la segunda es la persona física o jurídica que trata los datos por cuenta del responsable, siguiendo instrucciones estrictas. En principio, es el responsable quien debe controlar el tratamiento y quien asume la responsabilidad por ello, incluida la responsabilidad jurídica. Sin embargo, con la reforma de las normas

sobre protección de datos, los encargados del tratamiento tienen ahora la obligación de cumplir muchos de los requisitos que se aplican a los responsables. Por ejemplo, en virtud del RGPD, los encargados del tratamiento deben llevar un registro de todas las categorías de actividades de tratamiento para demostrar que cumplen con sus obligaciones conforme al Reglamento ([204]). Los encargados también están obligados a aplicar medidas técnicas y organizativas que garanticen la seguridad del tratamiento ([205]), a nombrar un delegado de protección de datos en determinadas circunstancias ([206]) y a notificar las violaciones de la seguridad de los datos personales al encargado del tratamiento ([207]).

Para determinar si una persona tiene la capacidad de decidir y determinar los fines y medios del tratamiento será necesario examinar los elementos objetivos o circunstancias del caso. El responsable del tratamiento, de acuerdo con la definición recogida en el RGPD, puede ser una persona física, una persona jurídica o cualquier otro organismo. Sin embargo, el Grupo de Trabajo del Artículo 29 ha puesto de relieve que para que las personas físicas dispongan de una entidad más estable para ejercitar sus derechos, «debería darse preferencia a la consideración de que el responsable del tratamiento sea la empresa o el organismo como tal, en lugar de una persona específica perteneciente a esa empresa o ese organismo» ([208]). Por ejemplo, una empresa que venda suministros sanitarios a profesionales es la responsable de elaborar y mantener la lista de distribución de todos los profesionales sanitarios de una determinada zona y no el director de ventas que efectivamente utiliza y mantiene la lista.

Ejemplo: Cuando el departamento de marketing de la empresa Sunshine pretende tratar datos para un estudio de mercado, el responsable del tratamiento será la empresa y no los empleados del departamento de marketing. El departamento de marketing no puede ser el responsable del tratamiento, ya que no posee una identidad jurídica independiente.

Las personas físicas pueden ser responsables del tratamiento con arreglo al Derecho de la UE y al Derecho del CdE. Sin embargo, cuando tratan datos acerca de otras

([204]) Reglamento general de protección de datos, artículo 30, apartado 2.

([205]) Ibíd., artículo 32.

([206]) Ibíd., artículo 37.

([207]) Ibíd., artículo 33, apartado 2.

([208]) Grupo de Trabajo del Artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, Bruselas, 16 de febrero de 2010.

personas en relación con una actividad puramente personal o doméstica, los particulares no están sujetos a las normas del RGPD y del Convenio 108 modernizado y no tienen la consideración de responsables del tratamiento ([209]). Un individuo que conserva su correspondencia, un diario personal en el que describe incidentes con amigos y compañeros y el historial médico de miembros de su familia, puede estar exento de las normas de protección de datos, ya que estas actividades podrían ser puramente personales o meramente domésticas. El RGPD especifica además que las actividades personales o domésticas también podrían incluir la actividad en redes sociales y la actividad en línea realizada en el contexto de las citadas actividades ([210]). Por el contrario, las normas de protección de datos se aplican íntegramente a los responsables y encargados del tratamiento que proporcionan los medios para tratar datos personales relacionados con actividades personales o domésticas (por ejemplo, plataformas de redes sociales) ([211]).

El acceso de los ciudadanos a internet y la posibilidad de utilizar plataformas de comercio electrónico, redes sociales y blogs para compartir información personal acerca de sí mismos y de otras personas hace que sea cada vez más difícil distinguir el tratamiento de datos para actividades personales del tratamiento de datos para actividades no personales ([212]). La consideración de las actividades como puramente personales o domésticas depende de las circunstancias ([213]) Las actividades que tienen aspectos profesionales o comerciales no pueden beneficiarse de la exención destinada a actividades domésticas ([214]). Por tanto, cuando la magnitud y la frecuencia del tratamiento de datos indique que se trata de una actividad profesional o a tiempo completo, un ciudadano particular podrá tener la consideración de responsable del tratamiento. Además del carácter profesional o comercial de la actividad de tratamiento, otro factor que hay que tener en cuenta es si se ponen datos personales a disposición de un elevado número de personas, evidentemente externas

([209]) Reglamento general de protección de datos, considerando 18 y artículo 2, apartado 2, letra c); Convenio 108 modernizado, artículo 3, apartado 2.

([210]) Reglamento general de protección de datos, considerando 18.

([211]) Ibíd., considerando 18; Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 29.

([212]) Véase la declaración del Grupo de Trabajo del Artículo 29 sobre las negociaciones relativas al paquete de reforma de la protección de datos (2013), *Anexo 2: Propuestas y modificaciones relativas a la exención para actividades personales o domésticas*, 27 de febrero de 2013.

([213]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 28.

([214]) Véase Reglamento general de protección de datos, considerando 18; y Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 27.

al ámbito privado de la persona. La jurisprudencia sentada en virtud de la Directiva sobre protección de datos establece que la legislación en materia de protección de datos será de aplicación cuando un ciudadano particular, utilizando internet, publique datos acerca de otras personas en un sitio web público. El TJUE todavía no ha resuelto sobre hechos similares con arreglo al RGPD, que contiene más directrices sobre los temas que podrían considerarse ajenos al ámbito de aplicación de la legislación sobre protección de datos en virtud de la «excepción doméstica», como el uso de las redes sociales con fines personales.

Ejemplo: *Bodil Lindqvist* ([215]) trataba de la mención de diferentes personas por su nombre o por otros medios, como su número de teléfono o información sobre sus aficiones, en una página de internet. El TJUE mantuvo que «la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios [...] constituye un "tratamiento total o parcialmente automatizado de datos personales"» en el sentido del artículo 3, apartado 1, de la Directiva sobre protección de datos ([216]).

Dicho tratamiento de datos personales no está comprendido en el ámbito de aplicación de las actividades exclusivamente personales o domésticas, que quedan fuera del ámbito de aplicación de las normas de protección de datos de la UE, ya que esta excepción «debe [...] interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es este el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas» ([217]).

Según el TJUE, la legislación de la EU en materia de protección de datos también puede aplicarse a las grabaciones visuales realizadas por una cámara de seguridad de instalación privada en determinadas circunstancias.

([215]) TJUE, C-101/01, Procedimiento penal entablado contra Bodil Lindqvist, 6 de noviembre de 2003.

([216]) Ibíd., apartado 27; antigua Directiva 95/46/CE, artículo 3, apartado 1, actual Reglamento general de protección de datos, artículo 2, apartado 1.

([217]) TJUE, C-101/01, *Procedimiento penal entablado contra Bodil Lindqvist*, 6 de noviembre de 2003, apartado 47.

Ejemplo: En *František Ryneš* ([218]), el Sr. Ryneš captó la imagen de dos personas que rompieron ventanas de su vivienda por medio del sistema doméstico de vigilancia por CCTV que había instalado para proteger su propiedad. La grabación se entregó posteriormente a la policía y se utilizó en el proceso penal.

El TJUE declaró que «[e]n la medida en que una vigilancia por videocámara [...] se extiende, aunque sea en parte, al espacio público, abarcando por ello una zona ajena a la esfera privada de la persona que procede al tratamiento de datos valiéndose de ese medio, tal vigilancia por videocámara no puede considerarse una actividad exclusivamente "personal o doméstica" [...]» ([219]).

Responsable del tratamiento

En el Derecho de la UE, se define al responsable del tratamiento como aquella persona que «solo o junto con otros, determine los fines y los medios del tratamiento» ([220]). La decisión del responsable del tratamiento establecerá el motivo y el modo en que se tratarán los datos.

En el Derecho del CdE, el Convenio 108 modernizado define al «responsable de tratamiento» como «la persona física o jurídica, autoridad pública, servicio, agencia o cualquier otro organismo que, por sí solo o junto con otros, tenga la facultad de tomar decisiones con respecto al tratamiento de datos personales» ([221]). Esta facultad de decisión afecta a los fines y medios del tratamiento, así como a las categorías de datos sujetos a tratamiento y al acceso a los datos ([222]). Si esta facultad se deriva de una designación legal o de circunstancias factuales deberá decidirse en cada caso ([223]).

([218]) TJUE, C-212/13, *František Ryneš contra Úřad pro ochranu osobních údajů*, 11 de diciembre de 2014, apartado 33.

([219]) Antigua Directiva 95/46/CE, artículo 3, apartado 2, segundo guion, actual Reglamento general de protección de datos, artículo 2, apartado 2, letra c).

([220]) Reglamento general de protección de datos, artículo 4, apartado 7.

([221]) Convenio 108 modernizado, artículo 2, letra d).

([222]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 22.

([223]) Ibíd.

Ejemplo: *Google Spain* ([224]) fue un asunto planteado por un ciudadano español que quería que un antiguo artículo de un periódico relativo a sus antecedentes financieros fuera eliminado de Google.

Se preguntó al TJUE si Google, como gestor del motor de búsqueda, era el «responsable del tratamiento» de los datos en el sentido del artículo 2, letra d) de la Directiva sobre protección de datos ([225]). El Tribunal consideró una definición amplia del concepto de «responsable» para garantizar «una protección eficaz y completa de los interesados» ([226]) El TJUE resolvió que el gestor del motor de búsqueda determinaba los fines y medios de la actividad y que hacía posible que los datos cargados en las páginas de internet por los editores de los sitios web fueran accesibles a cualquier usuario de internet que realizase una búsqueda con el nombre del interesado ([227]). Por tanto, el TJUE determinó que se podía considerar a Google «responsable del tratamiento» ([228]).

Cuando el responsable o encargado del tratamiento está radicado fuera de la UE, esa empresa debe designar, por escrito, a un representante en el territorio de la UE ([229]). El RGPD hace hincapié en que el representante debe estar establecido «en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado» ([230]). Si no se designa ningún representante, seguirá siendo posible entablar acciones legales contra el responsable o el encargado del tratamiento ([231]).

([224]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014.

([225]) Reglamento general de protección de datos, artículo 4, apartado 7; TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014, apartado 21.

([226]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014, apartado 34.

([227]) Ibíd., apartados 35-40.

([228]) Ibíd., apartado 41.

([229]) Reglamento general de protección de datos, artículo 27, apartado 1.

([230]) Ibíd., art. 27 apartado 3.

([231]) Ibíd., art. 27 apartado 5.

Corresponsabilidad del tratamiento

El RGPD establece que, si dos o más responsables del tratamiento determinan conjuntamente los fines y medios del tratamiento, se consideran corresponsables del tratamiento. Esto significa que deciden juntos tratar los datos para un fin común ([232]). El Informe explicativo del Convenio 108 modernizado señala que también pueden existir varios responsables o corresponsables del tratamiento **en el marco del CdE** ([233]).

El Grupo de Trabajo del Artículo 29 señala que la corresponsabilidad del tratamiento puede tomar diferentes formas y que la participación de los distintos responsables en las actividades de control puede ser desigual ([234]). Esta flexibilidad permite dar respuesta a realidades cada vez más complejas en el ámbito del tratamiento de datos ([235]). Los corresponsables del tratamiento deben por tanto determinar sus respectivas responsabilidades por el cumplimiento de las obligaciones conforme al Reglamento en un acuerdo específico ([236]).

La corresponsabilidad del tratamiento conlleva la responsabilidad conjunta de una actividad de tratamiento de datos personales ([237]). En el marco del **Derecho de la UE**, esto significa que cada responsable o encargado del tratamiento puede ser declarado plenamente responsable de la totalidad de los daños causados por el tratamiento sujeto a corresponsabilidad, con el fin de garantizar que el interesado reciba una compensación ([238]).

Ejemplo: Una base de datos gestionada conjuntamente por varias entidades de crédito sobre sus clientes morosos es un ejemplo común de corresponsabilidad del tratamiento. Cuando una persona solicita una línea de

([232]) Ibíd., artículo 4, apartado 7 y artículo 26.

([233]) Convenio 108 modernizado, artículo 2, letra d); Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal , apartado 22.

([234]) Grupo de Trabajo del Artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, Bruselas, 16 de febrero de 2010, p. 19.

([235]) Ibíd.

([236]) Reglamento general de protección de datos, considerando 79.

([237]) Ibíd., apartado 21.

([238]) Ibíd., artículo 82, apartado 4.

crédito a un banco que es uno de los corresponsables del tratamiento de los datos, la entidad bancaria consulta la base de datos como ayuda para tomar decisiones sobre la solvencia del solicitante con conocimiento de causa.

La normativa no establece de forma explícita si la corresponsabilidad del tratamiento exige que el fin común sea el mismo para cada uno de los responsables del tratamiento ni si es suficiente que sus fines solo coincidan en parte. Hasta la fecha, no existe jurisprudencia pertinente en el ámbito europeo. En su Dictamen de 2010 sobre responsables y encargados del tratamiento, el Grupo de Trabajo del Artículo 29 establece que los corresponsables pueden compartir todos los fines y medios del tratamiento o solo algunos fines o medios o parte de los mismos ([239]). Considerando que lo primero implicaría la existencia de una relación muy estrecha entre los distintos actores, lo segundo indicaría una relación más independiente.

El Grupo de Trabajo del Artículo 29 defiende una interpretación más amplia del concepto de corresponsabilidad del tratamiento con el fin de permitir cierta flexibilidad que tenga en cuenta la creciente complejidad de la realidad actual del tratamiento de datos personales ([240]). Un asunto en el que estuvo implicada la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) ilustra la posición del Grupo de Trabajo.

Ejemplo: En el denominado caso SWIFT, las entidades bancarias europeas utilizaban SWIFT, a quien en un inicio se consideró la encargada del tratamiento, para realizar transferencias de datos durante las transacciones bancarias. SWIFT comunicó dichos datos sobre transacciones bancarias, almacenados en un centro de servicio informático de los Estados Unidos, al Departamento del Tesoro estadounidense, sin que las entidades bancarias europeas que utilizaban sus servicios le hubieran ordenado expresamente que lo hiciera. El Grupo de Trabajo del Artículo 29, al evaluar la licitud de dicha situación, llegó a la conclusión de que las entidades bancarias que utilizan

([239]) Grupo de Trabajo del Artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, Bruselas, 16 de febrero de 2010, p. 19.

([240]) Ibíd.

SWIFT, así como la propia SWIFT, debían ser consideradas corresponsables del tratamiento de los datos ante los clientes europeos en lo que atañe a la difusión de sus datos a las autoridades estadounidenses ([241]).

Encargado del tratamiento

En el Derecho de la UE, el encargado del tratamiento se define como la persona que lleva a cabo el tratamiento de datos personales por cuenta del responsable del tratamiento ([242]). Las actividades que le son atribuidas al encargado pueden limitarse a una tarea o contexto específico o pueden ser bastante generales e integrales.

En el Derecho del CdE, el significado de encargado del tratamiento coincide con el establecido en el Derecho de la UE ([243]).

Los encargados del tratamiento, además de tratar datos para otras personas, también serán responsables por derecho propio del tratamiento de datos que realicen para sus propios fines, como la administración de sus propios empleados, ventas y cuentas.

Ejemplo: La empresa Everready está especializada en el tratamiento de datos destinado a la administración de los datos de recursos humanos de otras empresas. En esta función, Everready es un encargado del tratamiento. En los casos en que Everready trata los datos de sus propios empleados, en cambio, es la responsable de las operaciones de tratamiento de datos destinadas a cumplir sus obligaciones como empleadora.

Relación entre el responsable del tratamiento y el encargado del tratamiento

Como se ha visto, el responsable es la persona que determina los fines y los medios del tratamiento. El RGPD establece claramente que el encargado solo podrá tratar datos personales siguiendo las instrucciones del responsable, a menos que venga

([241]) Grupo de Trabajo del Artículo 29 (2006), *Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT)*, WP 128, Bruselas, 22 de noviembre de 2006.

([242]) Reglamento general de protección de datos, artículo 4, apartado 8.

([243]) Convenio 108 modernizado, artículo 2, letra f).

obligada a ello por la legislación de la UE o del Estado miembro ([244]). El contrato entre el responsable y el encargado es un elemento esencial de su relación y un requisito legal ([245]).

Ejemplo: El director de la empresa Sunshine decide que la empresa Cloudy —especializada en almacenamiento de datos en la nube— gestione los datos de los clientes de Sunshine. Sunshine es la responsable del tratamiento y Cloudy es tan solo una encargada, ya que, según el contrato, Cloudy solo puede utilizar los datos de los clientes de Sunshine para los fines que esta última determine.

Si la facultad de determinar los medios de tratamiento se delega en el encargado, el responsable deberá, no obstante, ejercer un grado apropiado de control sobre las decisiones del encargado en relación con los medios del tratamiento. La responsabilidad general sigue recayendo en el responsable del tratamiento, quien deberá supervisar a los encargados para velar por que sus decisiones cumplan la legislación en materia de protección de datos y sus propias instrucciones.

Asimismo, si el encargado no respeta las condiciones de tratamiento de los datos establecidas por el responsable, el encargado pasará a convertirse en el responsable, al menos en la medida en que haya incumplido las instrucciones del responsable. Lo más probable es que esto suponga que el encargado pase a ser un responsable que actúa de manera ilícita. A su vez, el responsable inicial deberá explicar cómo ha sido posible que el encargado incumpliese su mandato ([246]). De hecho, el Grupo de Trabajo del Artículo 29 tiende a presuponer que en estos casos existe corresponsabilidad del tratamiento, ya que es la mejor manera de proteger los intereses de los interesados ([247]).

También pueden plantearse cuestiones relativas al reparto de la responsabilidad cuando el responsable es una pequeña empresa y el encargado es una gran

([244]) Reglamento general de protección de datos, artículo 29.

([245]) Ibíd., artículo 28, apartado 3.

([246]) Ibíd., artículo 82, apartado 2.

([247]) Grupo de Trabajo del Artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, Bruselas, 16 de febrero de 2010, p. 25; Grupo de Trabajo del Artículo 29 (2006), *Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT)*, WP 128, Bruselas, 22 de noviembre de 2006.

empresa corporativa que tiene fuerza para dictar las condiciones de sus servicios. En dichas circunstancias, sin embargo, el Grupo de Trabajo del Artículo 29 mantiene que el nivel de responsabilidad no debería disminuir por razón del desequilibrio económico y que debería mantenerse el significado del concepto de responsable del tratamiento ([248]).

En aras de la claridad y la transparencia, los detalles de la relación entre el responsable y el encargado deberán consignarse por escrito en un contrato ([249]). El contacto debe incluir, en particular, el tema, la naturaleza, la finalidad y la duración del tratamiento, el tipo de datos personales y las categorías de interesados. También deberán establecerse los derechos y obligaciones del responsable y del encargado, como los requisitos en materia de confidencialidad y seguridad. La ausencia de un contrato de este tipo constituye un incumplimiento de la obligación del responsable del tratamiento de documentar por escrito las responsabilidades mutuas y puede acarrear sanciones. Cuando se ocasionen daños y perjuicios por actuar al margen o en contra de las instrucciones lícitas del responsable, no solamente será este último quien deba responder, sino también el encargado ([250]). El encargado del tratamiento debe llevar un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable ([251]). Este registro deberá ponerse a disposición de la autoridad de control que lo solicite, ya que el responsable y el encargado deben colaborar con dicha autoridad en el desempeño de sus funciones ([252]). Los responsables y los encargados también tienen la posibilidad de adherirse a un código de conducta aprobado o a un mecanismo de certificación aprobado para demostrar que cumplen los requisitos del RGPD ([253]).

Es posible que los encargados deseen delegar determinadas tareas en otros encargados (subencargados). Esto está permitido por la ley siempre que se establezcan cláusulas contractuales adecuadas entre el responsable y el encargado, en las que se indique si la autorización del responsable es necesaria en cada caso o si basta con informar de ello. El RGPD establece que el encargado inicial sigue siendo plenamente

([248]) Grupo de Trabajo del Artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, Bruselas, 16 de febrero de 2010, p. 19.

([249]) Reglamento general de protección de datos, artículo 28, apartados 3 y 9.

([250]) Ibíd., artículo 82, apartado 2.

([251]) Ibíd., artículo 30, apartado 2.

([252]) Ibíd., artículo 30, apartado 4, y artículo 31.

([253]) Ibíd., artículo 28, apartado 5, y artículo 42, apartado 4.

responsable ante el responsable del tratamiento en el caso de que un subencargado incumpla sus obligaciones de protección de datos ([254]).

En el Derecho del CdE se aplica íntegramente la interpretación de los conceptos de responsable y encargado aquí expuesta ([255]).

2.3.2. Destinatarios y terceros

La diferencia entre estas dos categorías de personas o entidades, que se introdujeron en la Directiva sobre protección de datos, radica principalmente en su relación con respecto al responsable del tratamiento y, en consecuencia, en su autorización para acceder a los datos personales que dicho responsable conserva.

Un «tercero» es una persona diferente del responsable y del encargado del tratamiento. En virtud del artículo 4, apartado 10, del RGPD, un tercero es una «persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado». Esto significa que las personas que trabajen para una organización diferente del responsable del tratamiento —aunque pertenezca al mismo grupo o sociedad matriz— será (o pertenecerá a) un «tercero». Por otra parte, las sucursales de un banco que traten cuentas de clientes bajo la autoridad directa de su oficina central no serán «terceros» ([256]).

El «destinatario» es un término más amplio que «tercero». En el sentido del artículo 4, apartado 9, del RGPD, un destinatario es «la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero». Este destinatario podrá ser, bien una persona externa al responsable o al encargado (en este último caso, estaríamos ante un tercero) o bien una persona perteneciente a la organización del responsable o del encargado, como un empleado u otro departamento de la misma empresa o autoridad.

La distinción entre destinatarios y terceros solo es importante respecto de las condiciones de lícita difusión de los datos. Los empleados del responsable o del

([254]) Ibíd., artículo 28, apartado 4.

([255]) Véase, por ejemplo, Convenio 108 modernizado, artículo 2, letras b) y f); Recomendación sobre creación de perfiles, artículo 1.

([256]) Grupo de Trabajo del Artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, Bruselas, 16 de febrero de 2010, p. 31.

encargado pueden ser destinatarios de datos personales, sin que sean necesarios otros requisitos legales, si participan en las operaciones de tratamiento del responsable o del encargado. En cambio, un tercero, al ser independiente del responsable o del encargado, no está autorizado a utilizar los datos personales tratados por el responsable, salvo por causas jurídicas específicas en un caso concreto.

Ejemplo: Un empleado de un responsable del tratamiento que utilice datos personales para realizar las tareas que le han sido atribuidas por el empleador será destinatario de los datos, pero no un tercero, ya que utiliza los datos por cuenta del responsable del tratamiento y conforme a sus instrucciones. Por ejemplo, si el empleador comunica datos personales de sus empleados a su departamento de recursos humanos con miras a próximas evaluaciones de desempeño, el equipo de recursos humanos será destinatario de dichos datos personales, ya que le habrán sido comunicados en el curso del tratamiento para el responsable.

Sin embargo, si la organización facilita datos de sus empleados a una empresa de formación que los vaya a utilizar con el fin de adaptar un programa de formación para los empleados, la empresa de formación es un tercero. El motivo es que la empresa de formación no tiene legitimidad ni autorización específica (que en el caso de los «recursos humanos» se origina en la relación de empleo con el responsable del tratamiento) para tratar estos datos personales. En otras palabras, no ha recibido la información en el curso de su relación laboral con el responsable del tratamiento.

2.4. Consentimiento

Puntos clave

- El consentimiento como base jurídica para el tratamiento de datos personales debe ser otorgado de manera libre, específica, informada e inequívoca por medio de una clara acción afirmativa que signifique aceptación del tratamiento.
- El tratamiento de categorías especiales de datos exige un consentimiento explícito.

Como se verá con detalle en el capítulo 4, el consentimiento es uno de los seis motivos legítimos para tratar datos personales. El consentimiento es «toda manifestación de voluntad libre, específica, informada e inequívoca» ([257]).

El **Derecho de la UE** establece tres elementos para que el consentimiento sea válido, que tienen por objeto garantizar que los interesados realmente accedieron a que sus datos fueran utilizados ([258]):

- El consentimiento debe otorgarse por medio de un claro acto afirmativo con que el interesado efectúe una manifestación de voluntad libre, específica, informada e inequívoca de aceptación del tratamiento de sus datos personales. Este acto puede ser una acción o una declaración.

- El interesado debe tener derecho a retirar su consentimiento en cualquier momento.

- En el contexto de una declaración escrita que también comprenda otros conceptos, como «condiciones de servicio», las solicitudes de consentimiento deben realizarse en lenguaje claro y sencillo y con una formulación inteligible y de fácil acceso, que distinga claramente el consentimiento de otras cuestiones; si parte de esta declaración viola el RGPD no será vinculante.

El consentimiento solo será válido en el contexto de la legislación sobre protección de datos si se cumplen todos estos requisitos. Corresponde al responsable del tratamiento demostrar que el interesado ha consentido el tratamiento de sus datos ([259]). Los elementos del consentimiento válido se analizarán con más detalle en la sección 4.1.1 sobre razones lícitas para el tratamiento de datos personales.

El Convenio 108 no incluye una definición de consentimiento, sino que esta es una cuestión que se remite a la legislación nacional. Sin embargo, **en el Derecho del CdE**, los elementos del consentimiento válido se corresponden con los explicados anteriormente ([260]).

([257]) Reglamento general de protección de datos, artículo 4, apartado 11. Véase asimismo el Convenio 108 modernizado, artículo 5, apartado 2.

([258]) Reglamento general de protección de datos, artículo 7.

([259]) Ibíd., artículo 7, apartado 1.

([260]) Convenio 108 modernizado, artículo 5, apartado 2; Comité Ad hoc sobre Protección de Datos (CAHDATA), Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartados 40-43.

Naturalmente, los requisitos adicionales contemplados en el Derecho civil para que el consentimiento sea válido, como la capacidad jurídica, también son de aplicación en el contexto de la protección de datos, puesto que son requisitos legales previos fundamentales. El consentimiento inválido de las personas que no posean capacidad jurídica tendrá como consecuencia la falta de base legal para el tratamiento de datos de dichas personas. En lo que respecta a la capacidad jurídica de los menores para formalizar contratos, el RGPD establece que sus normas sobre la edad mínima de obtención del consentimiento válido no afectan a las disposiciones generales del Derecho contractual de los Estados miembros ([261]).

El consentimiento debe otorgarse de manera clara, de modo que no quede rastro de duda acerca de las intenciones del interesado ([262]). El consentimiento ha de ser explícito cuando concierna al tratamiento de datos sensibles, y se puede otorgar oralmente o por escrito ([263]). En este último caso puede otorgarse por medios electrónicos ([264]). En el marco del **Derecho de la UE** y del **Derecho del CdE**, la aceptación del tratamiento de los datos personales propios debe efectuarse por medio de una declaración o una clara acción afirmativa ([265]). Por tanto, el silencio, las casillas previamente marcadas, los formularios previamente cumplimentados o la inacción no pueden constituir consentimiento ([266]).

([261]) Reglamento general de protección de datos, artículo 8, apartado 3.

([262]) Ibíd., artículo 6, apartado 1 y artículo 9, apartado 2, letra a).

([263]) Ibíd., considerando 32.

([264]) Ibíd.

([265]) Ibíd., artículo 4, apartado 11; Comité Ad hoc sobre Protección de Datos (CAHDATA), Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 40.

([266]) Reglamento general de protección de datos, considerando 32; Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 40.

3

Principios fundamentales de la legislación europea en materia de protección de datos

UE	Materias tratadas	CdE
Reglamento general de protección de datos, artículo 5, apartado 1, letra a)	El principio de licitud	Convenio 108 modernizado, artículo 5, apartado 3
Reglamento general de protección de datos, artículo 5, apartado 1, letra a)	El principio de lealtad	Convenio 108 modernizado, artículo 5, apartado 4, letra a) TEDH, *K.H. y otros contra Eslovaquia*, n.º 32881/04, 2009
Reglamento general de protección de datos, artículo 5, apartado 1, letra a) TJUE, C-201/14, *Smaranda Bara y otros contra Casa Națională de Asigurări de Sănătate y otros*, 2015	El principio de transparencia	Convenio 108 modernizado, artículo 5, apartado 4, letra a) y artículo 8. TEDH, *Haralambie contra Rumanía*, n.º 21737/03, 2009
Reglamento general de protección de datos, artículo 5, apartado 1, letra b)	El principio de limitación de la finalidad	Convenio 108 modernizado, artículo 5, apartado 4, letra b)
Reglamento general de protección de datos, artículo 5, apartado 1, letra c) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Kärntner Landesregierung y otros* [GS], 2014	El principio de minimización de datos	Convenio 108 modernizado, artículo 5, apartado 4, letra c)

UE	Materias tratadas	CdE
Reglamento general de protección de datos, artículo 5, apartado 1, letra d) TJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam contra M. E. E. Rijkeboer*, 2009.	**El principio de exactitud de los datos**	Convenio 108 modernizado, artículo 5, apartado 4, letra d)
Reglamento general de protección de datos, artículo 5, apartado 1, letra e) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland* y *Kärntner Landesregierung y otros* [GS], 2014	**El principio de limitación del plazo de conservación**	Convenio 108 modernizado, artículo 5, apartado 4, letra e) TEDH, *S. y Marper contra Reino Unido* [GS], números 30562/04 y 30566/04, 2008
Reglamento general de protección de datos, artículo 5, apartado 1, letra f), y artículo 32	**Principio de seguridad de los datos (integridad y confidencialidad)**	Convenio 108 modernizado, artículo 7
Reglamento general de protección de datos, artículo 5, apartado 2	**El principio de responsabilidad proactiva**	Convenio 108 modernizado, artículo 10, apartado 1

El artículo 5 del Reglamento general de protección de datos establece los principios por los que se rige el tratamiento de datos personales. Estos principios son:

- licitud, lealtad y transparencia;
- limitación de la finalidad;
- minimización de los datos;
- exactitud de los datos;
- limitación del plazo de conservación;
- integridad y confidencialidad.

Estos principios son el punto de partida de otras disposiciones más detalladas en artículos posteriores del Reglamento. También aparecen en los artículos 5, 7, 8 y 10 del Convenio 108 modernizado. Toda la legislación posterior en materia de protección de datos tanto en el ámbito de la Unión Europea como del Consejo de Europa

debe respetar estos principios, que deberán tenerse en cuenta a la hora de interpretar dicha legislación. En el Derecho de la UE, solo se permiten limitaciones a los principios de tratamiento en la medida en que se correspondan con los derechos y obligaciones estipulados en los artículos 12 a 22 y deben respetar el contenido esencial de los derechos y libertades fundamentales. Cualquier exención y limitación de estos principios fundamentales debe establecerse en el ámbito de la UE o en el ámbito nacional ([267]), debe establecerse por ley, servir a un fin legítimo y ser una medida necesaria y proporcionada en una sociedad democrática ([268]). Deben cumplirse las tres condiciones.

3.1. Los principios de licitud, lealtad y transparencia del tratamiento

Puntos clave

- Los principios de licitud, lealtad y transparencia se aplican a todo tipo de tratamiento de datos personales.
- En el RGPD, la licitud requiere que se cumpla al menos una de las siguientes condiciones:
  - consentimiento del interesado;
  - necesidad de ejecutar un contrato;
  - una obligación legal;
  - necesidad de proteger los intereses vitales del interesado o de otra persona física;
  - necesidad de cumplir una misión realizada en interés público;
  - necesidad de satisfacer los intereses legítimos del responsable del tratamiento o de un tercero, siempre que sobre los mismos no prevalezcan los intereses y derechos del interesado.
- El tratamiento de datos personales debe efectuarse de manera leal.
  - El interesado deberá ser informado del riesgo para garantizar que el tratamiento no tenga efectos negativos imprevisibles.

([267]) Convenio 108 modernizado, artículo 11, apartado 1; Reglamento general de protección de datos, artículo 23, apartado 1.

([268]) Reglamento general de protección de datos, artículo 23, apartado 1.

- El tratamiento de datos personales debe efectuarse de manera transparente.
  - Los responsables del tratamiento deberán comunicar a los interesados, antes de proceder al tratamiento de sus datos, la finalidad del tratamiento y su propia identidad y dirección, entre otros detalles.
  - La información sobre las operaciones del tratamiento deberá comunicarse con un lenguaje claro y sencillo, para que los interesados puedan entender fácilmente las normas, los riesgos, las salvaguardias y los derechos que les conciernen.
  - Los interesados tendrán derecho a acceder a sus datos cuando estos estén siendo objeto de tratamiento.

3.1.1. Licitud del tratamiento de datos

La normativa de protección de datos de la UE y del CdE requiere que el tratamiento de datos personales sea lícito ([269]). Para que el tratamiento sea lícito se requiere el consentimiento del interesado u otra razón legítima contemplada en la legislación sobre protección de datos ([270]). El artículo 6, apartado 1, del RGPD incluye cinco razones lícitas para el tratamiento, además del consentimiento, a saber, cuando sea necesario en el contexto de la ejecución de un contrato, en el cumplimiento de una misión realizada en el ejercicio de poderes públicos, en el cumplimiento de una obligación, con el fin de satisfacer los intereses legítimos del responsable del tratamiento o de terceros o para proteger los intereses vitales del interesado. Esto se analizará con más detalle en la sección 4.1.

3.1.2. Lealtad del tratamiento

Además de ser lícito, el tratamiento de datos debe efectuarse de manera leal, según la normativa de protección de datos de la UE y del CdE ([271]). El principio de lealtad del tratamiento rige primordialmente la relación entre el responsable del tratamiento y el interesado.

([269]) Convenio 108 modernizado, artículo 5, apartado 3; Reglamento general de protección de datos, artículo 5, apartado 1, letra a).

([270]) Carta de los Derechos Fundamentales de la Unión Europea, artículo 8, apartado 2; Reglamento general de protección de datos, considerando 40 y artículos 6-9; Convenio 108 modernizado, artículo 5, apartado 2; Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 41.

([271]) Reglamento general de protección de datos, artículo 5, apartado 1, letra a); Convenio 108 modernizado, artículo 5, apartado 4, letra a).

Los responsables del tratamiento deben notificar a los interesados y al público en general que tratarán los datos de manera lícita y transparente y deben ser capaces de demostrar que las operaciones de tratamiento cumplen las disposiciones del RGPD. Las operaciones de tratamiento no deben realizarse en secreto y los interesados deben ser conocedores de los riesgos potenciales. Además, los responsables del tratamiento, en la medida de lo posible, deberán actuar de manera que se cumplan los deseos del interesado sin dilaciones, en especial cuando su consentimiento constituya la base jurídica del tratamiento de datos.

Ejemplo: En *K.H. y otros contra Eslovaquia* ([272]), las demandantes eran ocho mujeres de origen étnico romaní que habían sido tratadas en dos hospitales en el este de Eslovaquia durante sus embarazos y partos. Posteriormente, ninguna de ellas pudo volver a concebir hijos después de repetidos intentos. Los órganos jurisdiccionales nacionales ordenaron a los hospitales que permitiesen que las demandantes y sus representantes consultaran sus historias clínicas y realizasen copias manuscritas de algunos pasajes, pero denegaron sus peticiones de fotocopiar los documentos, supuestamente para evitar un posible abuso. Las obligaciones positivas de los Estados con arreglo al artículo 8 del CEDH incluyen necesariamente la obligación de poner a disposición de los interesados copias de sus ficheros de datos. Era el Estado quien debía determinar el procedimiento de copia de los ficheros de datos personales o, en su caso, demostrar motivos fundados para su denegación. En el caso de las demandantes, los órganos jurisdiccionales nacionales justificaron la prohibición de hacer copias de sus historias clínicas, principalmente por la necesidad de proteger la información pertinente frente a abusos. Sin embargo, el TEDH no entendió cómo las demandantes, a quienes se les había concedido, en todo caso, acceso a toda su historia clínica, podrían haber abusado de la información que les concernía. Además, podría haberse evitado el riesgo de abuso de otra forma que no fuera negar las copias de los ficheros a las demandantes, como por ejemplo limitando el grupo de personas autorizadas a acceder a ellos. El Estado no logró demostrar la existencia de motivos lo suficientemente fundados para denegar a las demandantes el acceso efectivo a la información relacionada con su salud. El Tribunal concluyó que había existido una violación del artículo 8.

([272]) TEDH, *K.H. y otros contra Eslovaquia*, n.º 32881/04, 28 de abril de 2009.

En lo que respecta a los servicios de internet, las características de los sistemas de tratamiento de datos deben hacer posible que los interesados entiendan realmente lo que ocurre con sus datos. En cualquier caso, el principio de lealtad va más allá de las obligaciones de transparencia y podría vincularse además a la ética en el tratamiento de los datos personales.

Ejemplo: El departamento de investigación de una universidad realiza un experimento para analizar los cambios de estado de ánimo de 50 sujetos, que deben registrar sus pensamientos en un fichero electrónico cada hora, en un momento concreto. Las 50 personas dieron su consentimiento para este proyecto concreto y para este uso concreto de los datos por la universidad. El departamento de investigación pronto descubrió que el registro electrónico de pensamientos sería muy útil en otro proyecto orientado a la salud mental, coordinado por otro equipo. Aunque la universidad, como responsable del tratamiento, podría haber utilizado los mismos datos en el trabajo de otro equipo sin hacer nada más para garantizar la licitud del tratamiento de esos datos, puesto que las finalidades son compatibles, la universidad informó a los sujetos y les pidió un nuevo consentimiento, en aplicación de su código ético de investigación y del principio de lealtad del tratamiento.

3.1.3. Transparencia del tratamiento

La normativa de protección de datos de la UE y del CdE exige que el tratamiento de los datos personales se efectúe «de manera transparente en relación con el interesado» ([273]).

Este principio establece la obligación de que el responsable del tratamiento adopte las medidas que sean apropiadas para mantener a los interesados —que pueden ser usuarios o clientes— informados acerca de cómo se utilizan sus datos ([274]). La transparencia puede referirse a la información proporcionada a la persona antes de comenzar el tratamiento de los datos ([275]), a la información que debe estar a disposi-

([273]) Reglamento general de protección de datos, artículo 5, apartado 1, letra a); Convenio 108 modernizado, artículo 5, apartado 4, letra a) y artículo 8.

([274]) Reglamento general de protección de datos, artículo 12.

([275]) Ibíd., artículos 13 y 14.

ción de los interesados durante el tratamiento ([276]), o a la información proporcionada a los interesados cuando estos hayan solicitado acceso a sus propios datos ([277]).

> Ejemplo: En el caso de *Haralambie contra Rumanía* ([278]), el demandante no obtuvo acceso a la información relativa a su persona que obraba en poder del servicio secreto hasta cinco años después de su solicitud. El TEDH reiteró que los particulares que eran objeto de un expediente personal conservado por las autoridades públicas tenían un interés vital en poder acceder al mismo. Las autoridades tenían el deber de establecer un procedimiento eficaz de acceso a dicha información. El TEDH consideró que ni la cantidad de expedientes transferidos ni las carencias del sistema de archivo justificaban un retraso de cinco años para conceder la petición del demandante de acceso a su expediente. Las autoridades no habían proporcionado al demandante un procedimiento eficaz y accesible que le permitiera obtener acceso a su expediente personal en un tiempo razonable. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

Las operaciones de tratamiento deben explicarse a los interesados de un modo fácilmente accesible que garantice que estos entienden lo que ocurrirá con sus datos. Esto significa que el interesado debe conocer la finalidad concreta del tratamiento de sus datos personales en el momento de su recogida ([279]). La transparencia del tratamiento exige que se utilice lenguaje claro y sencillo ([280]). Los interesados deben tener claro cuáles son los riesgos, las normas, las salvaguardias y los derechos que conciernen al tratamiento de sus datos personales ([281]).

El Derecho del CdE también especifica que el responsable del tratamiento está obligado a facilitar cierta información esencial a los interesados de manera proactiva. La información sobre el nombre y dirección del responsable (o corresponsables) del tratamiento, la base jurídica y las finalidades del tratamiento, las categorías de datos tratados y sus destinatarios, así como los medios para ejercer los derechos, se pueden facilitar en cualquier formato apropiado (a través de un sitio web, con

([276]) Grupo de Trabajo del Artículo 29, *Dictamen 2/2017 sobre el tratamiento de datos en el trabajo*, p. 23.

([277]) Reglamento general de protección de datos, artículo 15.

([278]) TEDH, *Haralambie contra Rumanía*, n.º 21737/03, 27 de octubre de 2009.

([279]) Reglamento general de protección de datos, considerando 39.

([280]) Ibíd.

([281]) Ibíd.

herramientas tecnológicas en dispositivos personales, etc.), siempre que la información se presente de manera leal y efectiva al interesado. La información presentada deberá ser fácilmente accesible, legible, comprensible y adaptada a los interesados de que se trate (en un lenguaje apto para niños si fuera necesario, por ejemplo). También deberá facilitarse cualquier información adicional que sea necesaria para garantizar un tratamiento leal de los datos o que sea útil para ese fin, como el periodo de conservación, el conocimiento de las razones que justifican el tratamiento de los datos o información sobre la transmisión de datos a un destinatario de otra Parte o no Parte (indicando si esa no Parte en concreto ofrece un nivel apropiado de protección o las medidas adoptadas por el responsable del tratamiento para garantizar dicho nivel apropiado de protección de datos) ([282]).

De conformidad con el derecho de acceso ([283]), el interesado tiene derecho a que el responsable del tratamiento le informe, cuando lo solicite, si sus datos son objeto de tratamiento y, en tal caso, qué datos son objeto de dicho tratamiento ([284]). Además, de conformidad con el derecho a la información ([285]), las personas cuyos datos son objeto de tratamiento deberán ser informadas por los responsables o encargados del tratamiento de manera proactiva acerca de la finalidad, la duración y los medios de tratamiento, entre otros detalles, en principio antes de que comience la actividad de tratamiento.

Ejemplo: El asunto *Smaranda Bara y otros contra Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)* ([286]) trataba de la transmisión de datos fiscales relativos a los ingresos de trabajadores por cuenta propia por parte de la Agencia Nacional de Administración Tributaria al Fondo nacional del seguro de enfermedad de Rumanía, en función de los cuales debían pagarse atrasos de cotizaciones al seguro de enfermedad. Se pidió al TJUE que determinase si se debía haber facilitado información previa al interesado en relación con la identidad del responsable del tratamiento y la finalidad de la transmisión de los datos, antes de que dichos datos fueran tratados por el Fondo nacional del seguro de enfermedad. El TJUE resolvió que cuando una administración pública de

([282]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 68.

([283]) Reglamento general de protección de datos, artículo 15.

([284]) Convenio 108 modernizado, artículo 8 y artículo 9, apartado 1, letra b).

([285]) Reglamento general de protección de datos, artículos 13 y 14.

([286]) TJUE, C-201/14, *Smaranda Bara y otros contra Casa Naţională de Asigurări de Sănătate y otros*, 1 de octubre de 2015, apartados 28-46.

un Estado miembro transmite datos personales a otra administración pública que realiza un tratamiento ulterior de esos datos, los interesados deben ser informados acerca de esa transmisión o tratamiento.

En determinadas situaciones, se admiten excepciones a la obligación de informar a los interesados acerca del tratamiento de datos personales, que se analizarán con más detalle en la sección 6.1 sobre los derechos del interesado.

3.2. El principio de limitación de la finalidad

Puntos clave

- La finalidad del tratamiento de datos deberá definirse antes de que comience el tratamiento.
- No puede realizarse un tratamiento ulterior de los datos de manera que sea incompatible con la finalidad original, aunque el Reglamento general de protección de datos prevé excepciones a esta norma con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.
- En esencia, el principio de limitación de la finalidad significa que cualquier tratamiento de datos personales debe realizarse con un fin perfectamente definido y solo con fines adicionales especificados que sean compatibles con el original.

El principio de limitación de la finalidad es uno de los principios fundamentales de la legislación europea sobre protección de datos. Está estrechamente relacionado con la transparencia, la previsibilidad y el control del usuario: si la finalidad del tratamiento es suficientemente específica y clara, las personas saben qué esperar y se refuerza la transparencia y la seguridad jurídica. Al mismo tiempo, es importante definir claramente la finalidad para que los interesados puedan ejercer sus derechos de manera efectiva, como el derecho de oposición al tratamiento ([287]).

Este principio exige que cualquier tratamiento de datos personales se realice con un fin perfectamente definido y solo con fines adicionales que sean compatibles con el fin original ([288]). El tratamiento de datos personales con fines indefinidos o ilimi-

([287]) Grupo de Trabajo del Artículo 29 (2013), *Dictamen 3/2013 sobre la limitación a una finalidad específica*, WP 203, 2 de abril de 2013.

([288]) Reglamento general de protección de datos, artículo 5, apartado 1, letra b).

tados es, por tanto, ilícito. Tampoco es lícito el tratamiento de datos personales sin una finalidad concreta, únicamente basado en la consideración de que puede ser útil en algún momento del futuro. La legitimidad del tratamiento de datos personales dependerá de la finalidad del mismo, que debe ser explícita, especificada y legítima.

Cada nueva finalidad del tratamiento de datos que no sea compatible con la original deberá tener su propio fundamento jurídico y no podrá basarse en el hecho de que los datos fueran inicialmente obtenidos o tratados para otra finalidad legítima. A su vez, el tratamiento legítimo se limita a la finalidad inicialmente especificada y cualquier finalidad nueva exigirá otro fundamento jurídico distinto. Por ejemplo, la difusión de datos personales a terceros con una nueva finalidad deberá someterse a una atenta consideración, ya que es probable que esa difusión necesite otro fundamento jurídico, distinto del utilizado para recopilar los datos.

Ejemplo: Una compañía aérea obtiene datos de sus pasajeros para hacer reservas con el fin de operar el vuelo de manera adecuada. La compañía aérea necesitará datos sobre los números de asiento de los pasajeros, limitaciones físicas especiales (como la necesidad de una silla de ruedas) y requisitos alimentarios específicos (como la comida kosher o halal). Si se solicita a las compañías aéreas que transmitan estos datos, que están incluidos en el registro de nombres de los pasajeros (PNR), a las autoridades de inmigración del puerto de desembarque, estos datos se estarán utilizando entonces con fines de control de la inmigración, que son distintos de la finalidad inicial de obtención de los datos. La transmisión de estos datos a la autoridad de inmigración exigirá, por lo tanto, otro fundamento jurídico distinto.

Al considerar el ámbito de aplicación y los límites de una finalidad concreta, el Convenio 108 y el Reglamento general de protección de datos se basan en el concepto de compatibilidad: se admite el uso de los datos para fines compatibles por razones del fundamento jurídico inicial. Por tanto, no se puede realizar un tratamiento ulterior de los datos de una manera inesperada, inapropiada o inaceptable para el interesado ([289]). Para determinar si el tratamiento ulterior ha de considerarse compatible, el responsable del tratamiento deberá tener en cuenta lo siguiente (entre otros elementos):

([289]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 49.

- «cualquier relación entre estos fines y los fines del tratamiento ulterior previsto;
- el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior;
- la naturaleza de los datos personales;
- las consecuencias para los interesados del tratamiento ulterior previsto; y
- la existencia de garantías adecuadas tanto en la operación de tratamiento original con en la operación de tratamiento ulterior prevista» ([290]). Esto se puede hacer, por ejemplo, mediante el cifrado o la seudonimización.

Ejemplo: La empresa Sunshine adquiere datos de clientes en el curso de su actividad de gestión de las relaciones con los clientes (GRC). A continuación transmite estos datos a Moonlight, una empresa de *marketing* directo que quiere utilizarlos para colaborar en las campañas de marketing de terceros. La transmisión de datos realizada por Sunshine a otras empresas con fines de marketing constituye un uso ulterior de los datos para una nueva finalidad, que es incompatible con la GRC, que era la finalidad inicial de Sunshine para recopilar los datos de clientes. Por lo tanto, la transmisión de los datos a la empresa Moonlight precisa contar con un fundamento jurídico propio.

Por el contrario, el uso de los datos de GRC por parte de la empresa Sunshine para sus propios fines de marketing, es decir, el envío de mensajes de marketing a sus propios clientes en relación con sus propios productos, en general puede considerarse una finalidad compatible.

El Reglamento general de protección de datos y el Convenio 108 modernizado declaran que «el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos»

([290]) Reglamento general de protección de datos, considerando 50 y artículo 6, apartado 4; Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 49.

se considerará *a priori* compatible con los fines iniciales ([291]). Sin embargo, para realizar un tratamiento ulterior de datos personales deberán establecerse salvaguardias adecuadas como la anonimización, el cifrado o la seudonimización de los datos, así como la limitación del acceso a estos ([292]). El Reglamento general de protección de datos añade que «[s]i el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines» ([293]). Por lo tanto, cuando se realice un tratamiento ulterior de los datos, el interesado deberá ser informado de los fines, así como de sus derechos, incluido el derecho de oposición ([294]).

Ejemplo: La empresa Sunshine ha recopilado y almacenado datos de sus clientes en su actividad de gestión de relaciones con los clientes (GRC). El uso ulterior de estos datos por parte de la empresa Sunshine para realizar un análisis estadístico del comportamiento de compra de sus clientes es admisible, ya que los fines estadísticos son compatibles. No será necesario otro fundamento jurídico, como el consentimiento de los interesados. Sin embargo, para el tratamiento ulterior de los datos personales con fines estadísticos, la empresa Sunshine debe establecer salvaguardias adecuadas de los derechos y libertades del interesado. Las medidas técnicas y organizativas que Sunshine debe aplicar pueden incluir la seudonimización.

3.3. El principio de minimización de datos

Puntos clave

- El tratamiento de datos debe limitarse a lo necesario para cumplir un fin legítimo.

([291]) Reglamento general de protección de datos, artículo 5, apartado 1, letra b); Convenio 108 modernizado, artículo 5, apartado 4, letra b). Un ejemplo de dichas disposiciones nacionales es la Ley austriaca de protección de datos *(Datenschutzgesetz)*, Boletín Oficial Federal I n.º 165/1999, apdo. 46.

([292]) Reglamento general de protección de datos, artículo 6, apartado 4; Convenio 108 modernizado, artículo 5, apartado 4, letra b); Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 50.

([293]) Reglamento general de protección de datos, considerando 50.

([294]) Ibíd.

- El tratamiento de datos personales solo debe llevarse a cabo cuando la finalidad de dicho tratamiento no se pueda cumplir razonablemente por otros medios.
- El tratamiento de datos no puede constituir una injerencia desproporcionada en los intereses, derechos y libertades que se ponen en juego.

Únicamente se tratarán los datos que sean «adecuados, pertinentes y no excesivos en relación con el fin para el que se obtienen o tratan» ([295]). Las categorías de datos seleccionados para su tratamiento deben ser necesarias para lograr el objetivo declarado de las operaciones tratamiento, y el responsable del tratamiento deberá limitar estrictamente la recogida de datos a aquella información que esté directamente relacionada con el fin específico que persiga el tratamiento.

Ejemplo: En el asunto *Digital Rights Ireland* ([296]), el TJUE examinó la validez de la Directiva sobre conservación de datos, que tenía por objeto armonizar las disposiciones nacionales relativas a la conservación de datos personales generados o tratados por medio de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones para su posible transmisión a las autoridades competentes en la lucha contra los delitos graves, como el crimen organizado y el terrorismo. Sin perjuicio de que se consideró que esta finalidad respondía efectivamente a un objetivo de interés general, el hecho de que la Directiva abarcase de manera generalizada «a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves» se consideró problemático ([297]).

Además, mediante el uso de tecnología especial para reforzar la privacidad, a veces es posible evitar todo uso de datos personales o aplicar medidas que reduzcan la capacidad para atribuir datos a un interesado (por ejemplo, la seudonimización), de modo que se obtenga una solución compatible con la privacidad. Esto es especialmente adecuado en sistemas de tratamiento más amplios.

([295]) Convenio 108 modernizado, artículo 5, apartado 4, letra c); Reglamento general de protección de datos, artículo 5, apartado 1, letra c).

([296]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros* y *Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.

([297]) Ibíd., apartados 44 y 57.

Ejemplo: Un ayuntamiento ofrece una tarjeta con chip a los usuarios habituales del sistema de transporte público municipal previo pago de una determinada tasa. La tarjeta lleva el nombre del usuario escrito en la superficie de la misma, así como de forma electrónica en el chip. Cuando se utiliza un autobús o un tranvía, debe pasarse la tarjeta con chip frente a los dispositivos de lectura instalados, por ejemplo, en los autobuses y en los tranvías. Los datos que lee el dispositivo se cotejan por medios electrónicos con una base de datos que incluye los nombres de las personas que han comprado la tarjeta de transporte.

Este sistema no es plenamente conforme con el principio de minimización de los datos, puesto que se podría comprobar si una persona física está autorizada a utilizar los medios de transporte sin tener que cotejar los datos personales que contiene el chip de la tarjeta con una base de datos. Bastaría, por ejemplo, con que el chip de la tarjeta incluyera una imagen electrónica especial (como un código de barras) que, al pasar frente al dispositivo de lectura, confirmase si la tarjeta es válida o no. Un sistema de este tipo no registraría quién ha utilizado cada medio de transporte en cada momento. Esta sería la solución óptima en el sentido del principio de minimización, ya que este principio deriva en la obligación de reducir al mínimo la recopilación de datos.

El artículo 5, apartado 1 del Convenio 108 modernizado contiene un requisito de proporcionalidad en el tratamiento de datos personales en relación con el fin legítimo perseguido. Debe existir un equilibrio justo entre todos los intereses enfrentados en todas las etapas del tratamiento. Esto significa que «[l]os datos personales que sean adecuados y pertinentes pero constituyan una injerencia desproporcionada en los derechos y libertades fundamentales en juego deberán considerarse excesivos» ([298]).

([298]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 52; Reglamento general de protección de datos artículo 5, apartado 1, letra c).

3.4. El principio de exactitud de los datos

Puntos clave

- El responsable del tratamiento deberá aplicar el principio de exactitud de los datos en todas las operaciones de tratamiento.
- Los datos inexactos deberán ser suprimidos o rectificados sin dilación.
- Puede que sea necesario verificar periódicamente y mantener actualizados los datos a fin de garantizar su exactitud.

El responsable del tratamiento que disponga de información personal no utilizará dicha información sin adoptar medidas que garanticen, con una certeza razonable, que los datos son exactos y están actualizados ([299]).

La obligación de garantizar la exactitud de los datos debe considerarse en el contexto de la finalidad del tratamiento.

Ejemplo: En el asunto *Rijkeboer* ([300]), el TJUE examinó la petición de información realizada por un nacional neerlandés a la administración local de la ciudad de Ámsterdam sobre la identidad de las personas a quienes se habían comunicado, durante los dos años anteriores, los datos que le concernían que obraban en poder de la autoridad local, así como sobre el contenido de los datos comunicados. El TJUE declaró que el «derecho a la privacidad conlleva que la persona de que se trata pueda cerciorarse de la exactitud y la licitud del tratamiento de sus datos personales, esto es, en particular, de que los datos personales son exactos, y de que son comunicados a los destinatarios autorizados». El TJUE se refería después al cuadragésimo primer considerando de la Directiva sobre protección de datos, que establecía que los interesados deben disfrutar del derecho de acceso a los datos que les conciernan para poder comprobar que son correctos ([301]).

([299]) Reglamento general de protección de datos, artículo 5, apartado 1, letra d); Convenio 108 modernizado, artículo 5, apartado 4, letra d).

([300]) TJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer*, 7 de mayo de 2009.

([301]) Antiguo considerando 41 de la Directiva 95/46/CE.

También puede haber casos en que esté legalmente prohibido actualizar los datos conservados, puesto que la finalidad de dicha conservación es principalmente documentar los acontecimientos, a modo de «instantánea» histórica.

Ejemplo: La historia médica de una operación no debe ser modificada, es decir, «actualizada», ni aunque las conclusiones incluidas en dicha historia resulten ser erróneas. En estas circunstancias, únicamente podrán hacerse añadidos a las observaciones de la historia si queda claramente indicado que son aportaciones realizadas en un momento posterior.

Por otro lado, hay situaciones en las que resulta absolutamente necesario comprobar e incluso actualizar periódicamente la exactitud de los datos debido al daño que podría ocasionarse al interesado si los datos siguieran siendo inexactos.

Ejemplo: Si una persona desea celebrar un contrato de crédito con una entidad bancaria, esta normalmente comprobará la solvencia del posible cliente. Con este fin, existen bases de datos específicas que incluyen datos sobre el historial de crédito de los particulares. Si la base de datos contiene datos incorrectos u obsoletos sobre una persona física, esta persona puede tener graves problemas. Por tanto, los responsables del tratamiento de dichas bases de datos deberán hacer un especial esfuerzo por cumplir con el principio de exactitud.

3.5. El principio de limitación del plazo de conservación

Puntos clave

- El principio de limitación del plazo de conservación obliga a suprimir o anonimizar los datos personales en el momento en que dejen de ser necesarios para los fines para los que fueron recabados.

El artículo 5, apartado 1, letra e) del RGPD y, del mismo modo, el artículo 5, apartado 4, letra e) del Convenio 108 modernizado establecen que los datos personales

deben ser «mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos». Por lo tanto, los datos deberán ser suprimidos o anonimizados cuando se hayan cumplido dichos fines. Con este fin, «el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica», a fin de asegurarse de que no se conserven los datos durante más tiempo del necesario ([302]).

En *S. y Marper*, el TEDH concluyó que los principios esenciales de los instrumentos pertinentes del Consejo de Europa, y la legislación y la práctica de las otras Partes Contratantes, exigían que la conservación de los datos fuera proporcionada respecto de la finalidad de la recopilación y limitada en el tiempo, especialmente en el sector policial ([303]).

Ejemplo: En *S. y Marper* ([304]) el TEDH resolvió que la conservación por tiempo indefinido de las impresiones dactilares, muestras celulares y perfiles de ADN de los dos demandantes era desproporcionada e innecesaria en una sociedad democrática, considerando que el proceso penal contra ambos demandantes había finalizado en una absolución y en la retirada de la acusación, respectivamente.

La limitación del plazo de conservación de los datos personales se aplica únicamente a los datos mantenidos de forma que se permita la identificación de los interesados. Por tanto, una forma lícita de conservar datos que hayan dejado de ser necesarios podría ser la anonimización de los datos.

Los datos archivados con fines de interés público, fines de investigación científica o histórica o fines estadísticos podrán conservarse durante periodos más largos siempre que se utilicen exclusivamente con estos fines ([305]). Deberán adoptarse medidas técnicas y organizativas adecuadas para el almacenamiento y uso permanentes de datos personales, con el fin de salvaguardar los derechos y libertades del interesado.

([302]) Reglamento general de protección de datos, considerando 39.

([303]) TEDH, *S. y Marper contra Reino Unido* [GS], n.os 30562/04 y 30566/04, 4 de diciembre de 2008; véase también, por ejemplo: TEDH, *M.M. contra Reino Unido*, n.º 24029/07, 13 de noviembre de 2012.

([304]) TEDH, *S. y Marper contra Reino Unido* [GS], números 30562/04 y 30566/04, 4 de diciembre de 2008.

([305]) Reglamento general de protección de datos, artículo 5, apartado 1, letra e); Convenio 108 modernizado, artículo 5, apartado 3, letra b) y artículo 9, apartado 2.

El Convenio 108 modernizado también permite excepciones al principio de limitación del plazo de conservación, a condición de que estén establecidas por la ley, respeten el contenido esencial de los derechos y libertades fundamentales y que sean necesarias y proporcionadas para perseguir un número limitado de fines legítimos ([306]). Entre estos fines se encuentran la protección de la seguridad nacional, la investigación y enjuiciamiento de delitos penales, la ejecución de sanciones penales, la protección del interesado y la protección de los derechos y libertades fundamentales de otras personas.

Ejemplo: En el asunto *Digital Rights Ireland* ([307]), el TJUE examinó la validez de la Directiva sobre conservación de datos, que tenía por objeto armonizar las disposiciones nacionales relativas a la conservación de datos personales generados o tratados por medio de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones con el fin de combatir los delitos graves, como el crimen organizado y el terrorismo. La Directiva sobre conservación de datos establecía un periodo de conservación «mínimo de seis meses sin que se establezca ninguna distinción entre las categorías de datos previstas en el artículo 5 de la Directiva en función de su posible utilidad para el objetivo perseguido o de las personas afectadas» ([308]). El TJUE también planteó la cuestión de la ausencia de criterios objetivos en la Directiva sobre conservación de datos, en virtud de los cuales debiera determinarse el periodo exacto de conservación —que podía variar entre un mínimo de seis meses y un máximo de veinticuatro meses— con el fin de asegurar que dicho periodo se limite a lo estrictamente necesario ([309]).

([306]) Convenio 108 modernizado, artículo 9, apartado 1; Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartados 91-98.

([307]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros* y *Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.

([308]) Ibíd., apartado 63.

([309]) Ibíd., apartado 64.

3.6. El principio de seguridad de los datos

Puntos clave

- La seguridad y la confidencialidad de los datos personales son esenciales para evitar que el interesado sufra efectos negativos.
- Las medidas de seguridad pueden ser de carácter técnico u organizativo.
- La seudonimización es un proceso que puede proteger los datos personales.
- La idoneidad de las medidas de seguridad debe determinarse en cada caso y examinarse periódicamente.

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito ([310]). El RGPD establece que el responsable y el encargado del tratamiento deben tener en cuenta «el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como fines riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas» en la aplicación de tales medidas ([311]). En función de las circunstancias concretas del caso, medidas técnicas y organizativas apropiadas pueden ser, por ejemplo, la seudonimización y el cifrado de datos personales o un proceso de verificación y evaluación periódicas de la eficacia de las medidas para garantizar la seguridad del tratamiento ([312]).

Como se ha explicado en la sección 2.1.1, la seudonimización de los datos consiste en sustituir los atributos que contienen los datos personales —que hacen posible la identificación del interesado— por un seudónimo, y mantener dichos atributos separados aplicando medidas técnicas u organizativas. El proceso de seudonimización no debe confundirse con el de anonimización, en el que se eliminan todos los vínculos que identifican a la persona.

([310]) Reglamento general de protección de datos, considerando 39 y artículo 5, apartado 1, letra f); Convenio 108 modernizado, artículo 7.

([311]) Reglamento general de protección de datos, artículo 32, apartado 1.

([312]) Ibíd.

Ejemplo: La frase «Charles Spencer, nacido el 3 de abril de 1967, es padre de cuatro hijos, dos niños y dos niñas» puede seudonimizarse de la siguiente manera:

«C.S. (1967) es padre de cuatro hijos, dos niños y dos niñas»; o bien

«El sujeto 324 es padre de cuatro hijos, dos niños y dos niñas»; o bien

«YESz320l es padre de cuatro hijos, dos niños y dos niñas».

Normalmente, los usuarios que tengan a estos datos seudonimizados no podrán identificar a «Charles Spencer, nacido el 3 de abril de 1967» a partir de «el sujeto 324» o «YESz3201». Por lo tanto, es más probable que los datos seudonimizados estén a salvo de usos indebidos.

No obstante, el primer ejemplo es menos seguro. Si la frase «C.S. (1967) es padre de cuatro hijos, dos niños y dos niñas» se utiliza en la pequeña ciudad en que vive Charles Spencer, este será fácilmente reconocible. El método de seudonimización puede afectar a la eficacia de la protección de datos.

Los datos personales con atributos cifrados o conservados por separado se utilizan en numerosos contextos como forma de mantener en secreto las identidades personales. Esto es especialmente útil cuando los responsables del tratamiento necesitan asegurarse de que están hablando de los mismos interesados, pero no necesitan o no deberían conocer las identidades reales de los interesados. Este es el caso, por ejemplo, cuando un investigador estudia la evolución de una enfermedad en pacientes cuya identidad es conocida únicamente por el hospital en que están siendo tratados y del cual obtiene el investigador las historias clínicas seudonimizadas. La seudonimización es, por tanto, un sólido componente del conjunto de tecnologías de protección de la privacidad. Puede ser un elemento importante en la aplicación de la privacidad desde el diseño. Esto significa integrar la protección de datos en la misma estructura de los sistemas de tratamiento de datos personales.

El artículo 25 del RGPD, que trata de la protección de datos desde el diseño, menciona expresamente la seudonimización como ejemplo de medida técnica y organizativa apropiada que deben aplicar los responsables del tratamiento para aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias. De este modo, los responsables del tratamiento cumplirán los requisitos del

Reglamento y protegerán los derechos de los interesados en el tratamiento de sus datos personales.

La adhesión a un código de conducta aprobado o a un mecanismo de certificación aprobado puede ayudar a demostrar que se cumple el requisito de seguridad del tratamiento ([313]). En su Dictamen sobre las implicaciones para la protección de datos del tratamiento de los registros de nombres de pasajeros, el Consejo de Europa proporciona otros ejemplos de medidas de seguridad adecuadas para la protección de datos personales en los sistemas de registro de nombres de pasajeros, como la conservación de los datos en un entorno físico seguro, la limitación del control de acceso mediante sistemas de inicio de sesión que consten de varios niveles y la protección de la comunicación de los datos con métodos criptográficos robustos ([314])

Ejemplo: Las plataformas de redes sociales y los proveedores de correo electrónico permiten a los usuarios agregar un nivel adicional de seguridad de los datos a los servicios que prestan mediante la autenticación de dos niveles. Además de introducir una contraseña personal, los usuarios deben completar un segundo paso de inicio de sesión para acceder a su cuenta personal. Este segundo paso podría ser, por ejemplo, la introducción de un código de seguridad enviado al teléfono móvil vinculado a la cuenta personal. De este modo, la verificación en dos pasos ofrece una mayor protección de los datos personales contra el acceso no autorizado a cuentas personales mediante acciones de piratería.

El Informe explicativo del Convenio 108 modernizado ofrece ejemplos adicionales de garantías adecuadas, como la imposición de una obligación de secreto profesional o la adopción de medidas cualificadas de seguridad técnica, como el cifrado de los datos ([315]). Cuando se adopten medidas específicas de seguridad, el responsable del tratamiento (o, cuando proceda, el encargado del tratamiento) deberán tener en cuenta diversos elementos, como la naturaleza y el volumen de los datos personales tratados, las posibles consecuencias adversas para los interesados y la necesidad

([313]) Ibíd., artículo 32, apartado 3.

([314]) Comité Consultivo del Consejo del Convenio 108, *Dictamen sobre las implicaciones para la protección de datos del tratamiento de los registros de nombres de pasajeros*, T-PD(2016)18rev, 19 de agosto de 2016, p. 9.

([315]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 56.

de que el acceso a los datos sea restringido ([316]). A la hora de aplicar medidas de seguridad apropiadas debe tenerse en cuenta el estado actual de la técnica de los procedimientos de seguridad aplicados al tratamiento de los datos. El coste de estas medidas debe ser proporcionado a la gravedad y la probabilidad de los riesgos potenciales. Es preciso revisar periódicamente las medidas de seguridad con el fin de actualizarlas si es necesario ([317]).

En caso de violación de la seguridad de los datos personales, tanto el Convenio 108 modernizado como el RGPD obligan al responsable del tratamiento a notificar dicha violación a la autoridad de control competente junto con los riesgos para los derechos y libertades de los interesados sin dilaciones indebidas ([318]). Existe una obligación similar de comunicación al interesado cuando sea probable que la vulneración de sus datos personales pueda entrañar un grave riesgo para sus derechos y libertades ([319]). La comunicación de tales violaciones a los interesados debe efectuarse en lenguaje claro y sencillo ([320]). Si el encargado del tratamiento es conocedor de una violación de la seguridad de los datos personales, deberá notificarla al responsable del tratamiento de forma inmediata ([321]). En determinadas situaciones pueden aplicarse excepciones a la obligación de notificación. Por ejemplo, el responsable del tratamiento no estará obligado a notificar a la autoridad de control cuando «sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas» ([322]). Tampoco será necesario notificar al interesado cuando la aplicación de medidas de seguridad hagan ininteligibles los datos personales para personas no autorizadas o cuando medidas ulteriores garanticen que ya no existe la probabilidad de que se materialice el grave riesgo ([323]). Si la comunicación de una violación de los datos personales de los interesados supone un esfuerzo desproporcionado por cuenta del responsable del tratamiento, se optará en su lugar por una comunicación pública o una medida semejante por la que «se informe de manera igualmente efectiva a los interesados» ([324]).

([316]) Ibíd., apartado 62.

([317]) Ibíd., apartado 63.

([318]) Convenio 108 modernizado, artículo 7, apartado 2; Reglamento general de protección de datos, artículo 33, apartado 1.

([319]) Convenio 108 modernizado, artículo 7, apartado 2; Reglamento general de protección de datos, artículo 34, apartado 1.

([320]) Reglamento general de protección de datos, artículo 34, apartado 2.

([321]) Ibíd., artículo. 33 apartado 1.

([322]) Ibíd.

([323]) Ibíd., artículo 34, apartado 3, letras a) y b).

([324]) Ibíd., artículo 34, apartado 3, letra c).

3.7. El principio de responsabilidad proactiva

Puntos clave

- La responsabilidad proactiva obliga a los responsables y encargados del tratamiento a aplicar medidas de manera activa y continuada para promover y garantizar la protección de los datos en sus actividades de tratamiento.
- Los responsables y encargados del tratamiento tienen la responsabilidad de que sus operaciones de tratamiento de datos cumplan con la legislación en materia de protección de datos y sus obligaciones respectivas.
- Los responsables del tratamiento deben ser capaces de demostrar el cumplimiento de las disposiciones sobre protección de datos ante los interesados, el público en general y las autoridades de control en cualquier momento. Los encargados del tratamiento también deben cumplir determinadas obligaciones estrictamente relacionadas con la responsabilidad proactiva (como por ejemplo llevar un registro de las operaciones de tratamiento y designar un delegado de protección de datos).

El RGPD y el Convenio 108 modernizado establecen que el responsable del tratamiento será responsable del cumplimiento de los principios del tratamiento de datos personales descritos en este capítulo ([325]). A tal efecto, el responsable del tratamiento deberá aplicar medidas técnicas y organizativas adecuadas ([326]). Aunque el principio de responsabilidad proactiva recogido en el artículo 5, apartado 2, del RGPD está dirigido únicamente a los responsables del tratamiento, también cabe esperar que los encargados del tratamiento rindan cuentas, dado que tienen que cumplir varias obligaciones y que están estrechamente relacionados con la responsabilidad proactiva.

La legislación de la UE y del CdE en materia de protección de datos también determinan que el responsable del tratamiento es el responsable del cumplimiento de los principios de protección de datos descritos en las secciones 3.1 a 3.6 y debe ser capaz de demostrarlo ([327]). El Grupo de Trabajo del Artículo 29 señala que «el tipo de procedimientos y mecanismos variará en función de los riesgos del tratamiento y la naturaleza de los datos» ([328]).

([325]) Ibíd., artículo 5, apartado 2; Convenio 108 modernizado, artículo 10, apartado 1.

([326]) Reglamento general de protección de datos, artículo 24.

([327]) Ibíd., artículo 5, apartado 2; Convenio 108 modernizado, artículo 10, apartado 1.

([328]) Grupo de Trabajo del Artículo 29, *Dictamen 3/2010 sobre el principio de responsabilidad proactiva*, WP 173, Bruselas, 13 de julio de 2010, apartado 12.

Los responsables del tratamiento pueden facilitar el cumplimiento de este requisito de varias maneras, entre las que cabe mencionar:

- registrar las actividades de tratamiento y ponerlas a disposición de la autoridad de control cuando esta lo solicite ([329]);
- en determinadas situaciones, designar un delegado de protección de datos que se encargue de todas las cuestiones relacionadas con la protección de los datos personales ([330]);
- realizar evaluaciones de impacto relativas a la protección de datos con respecto a tipos de tratamiento que puedan entrañar un riesgo elevado para los derechos y libertades de las personas físicas ([331]);
- velar por la protección de los datos desde el diseño y por defecto ([332]);
- implantar modalidades y procedimientos para el ejercicio de los derechos de los interesados ([333]);
- adherirse a códigos de conducta o mecanismos de certificación aprobados ([334]).

Aunque el principio de responsabilidad proactiva recogido en el artículo 5, apartado 2, del RGPD no está específicamente dirigido a los encargados del tratamiento, existen disposiciones vinculadas a la responsabilidad proactiva que también contienen obligaciones para ellos, como la llevanza de un registro de las actividades de tratamiento y la designación de un delegado de protección de datos para todas las actividades de tratamiento que lo requieran ([335]). Los encargados del tratamiento deben cerciorarse asimismo de que se han aplicado todas las medidas necesarias para garantizar la seguridad de los datos ([336]). El contrato legalmente vinculante entre el responsable y el encargado debe estipular que el encargado asistirá al

([329]) Reglamento general de protección de datos, artículo 30.

([330]) Ibíd., artículos 37-39.

([331]) Ibíd., artículo 35; Convenio 108 modernizado, artículo 10, apartado 2.

([332]) Reglamento general de protección de datos, artículo 25. Convenio 108 modernizado, párrafos segundo y tercero del artículo 10.

([333]) Ibíd., artículo 12 y artículo 24.

([334]) Ibíd., artículo 40 y artículo 42.

([335]) Ibíd., artículo 5, apartado 2, artículo 30 y artículo 37.

([336]) Ibíd., artículo 28, apartado 3, letra c).

responsable en algunos de los requisitos de cumplimiento, por ejemplo en la realización de una evaluación de impacto de la protección de datos o en la notificación al responsable de cualquier violación de los datos personales en el momento en que sea conocedor de la misma ([337]).

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) adoptó en 2013 unas directrices de privacidad en las que se destacaba que los responsables del tratamiento tienen una función importante a la hora de aplicar la protección de datos en la práctica. Estas directrices desarrollan el principio de responsabilidad proactiva en el sentido de que «todo responsable del tratamiento debería rendir cuentas por el cumplimiento de las medidas que permiten la aplicación de los principios [materiales] antes expuestos» ([338]).

Ejemplo: Un ejemplo legislativo que destaca el principio de responsabilidad proactiva es la modificación de la Directiva 2002/58/CE sobre la privacidad en las comunicaciones electrónicas realizada en 2009 ([339]). De acuerdo con el artículo 4 de su versión modificada, la Directiva impone la obligación de garantizar «la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales». Por tanto, en lo que atañe a las disposiciones de seguridad de dicha Directiva, el legislador decidió que era necesario introducir un requisito explícito de contar con una política de seguridad y aplicarla.

De acuerdo con el dictamen del Grupo de Trabajo del Artículo 29 ([340]), la esencia de la responsabilidad proactiva es la obligación del responsable del tratamiento de:

([337]) Ibíd., artículo 28, apartado 3, letra d).

([338]) OCDE (2013), Directrices relativas a la protección de la intimidad y la circulación transfronteriza de datos personales, artículo 14.

([339]) Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n.º 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO 2009 L 337, p. 11.

([340]) Grupo de Trabajo del Artículo 29, *Dictamen 3/2010 sobre el principio de responsabilidad proactiva*, WP 173, Bruselas, 13 de julio de 2010.

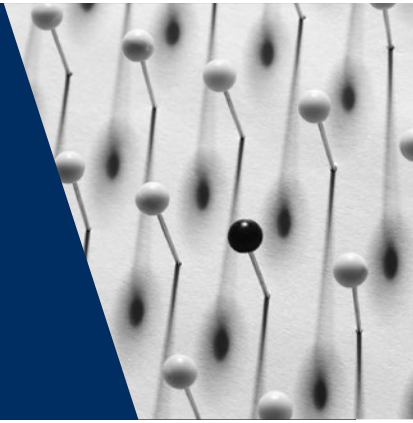
- aplicar medidas que garanticen, en circunstancias normales, que se cumplen las normas en materia de protección de datos en el contexto de las operaciones de tratamiento; y

- tener disponible documentación que demuestre a los interesados y a las autoridades de control qué medidas se han adoptado para conseguir el cumplimiento de las normas en materia de protección de datos.

El principio de responsabilidad proactiva exige, por tanto, que los responsables del tratamiento demuestren dicho cumplimiento de forma activa y que no se limiten a esperar a que los interesados o las autoridades de control señalen las carencias.

4

Normas de la legislación europea en materia de protección de datos



UE	Materias tratadas	CdE
Normas relativas al tratamiento lícito de los datos		
Reglamento general de protección de datos, artículo 6, apartado 1, letra a) TJUE, C-543/09, *Deutsche Telekom AG contra Bundesrepublik Deutschland*, 2011 TJUE, C-536/15, *Tele2 (Netherlands) BV y otros contra Autoriteit Consument en Markt (ACM)*, 2017	**Consentimiento**	Recomendación sobre creación de perfiles, apartado 3.4, letra b), y apartado 3.6 Convenio 108 modernizado, artículo 5, apartado 2
Reglamento general de protección de datos, artículo 6, apartado 1, letra b)	**Relación precontractual**	Recomendación sobre creación de perfiles, apartado 3.4, letra b)
Reglamento general de protección de datos, artículo 6, apartado 1, letra c)	**Obligaciones legales del responsable del tratamiento**	Recomendación sobre creación de perfiles, apartado 3.4, letra a)
Reglamento general de protección de datos, artículo 6, apartado 1, letra d)	**Intereses vitales del interesado**	Recomendación sobre creación de perfiles, apartado 3.4, letra b)
Reglamento general de protección de datos, artículo 6, apartado 1, letra e) TJUE, C-524/06, *Huber contra Bundesrepublik Deutschland* [GS], 2008	**Interés público y ejercicio del poder público**	Recomendación sobre creación de perfiles, apartado 3.4, letra b)

UE	Materias tratadas	CdE
Reglamento general de protección de datos, artículo 6, apartado 1, letra f) TJUE, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contra Rīgas pašvaldības SIA «Rīgas satiksme»*, 2017 TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 2011	**Intereses legítimos de los demás**	Recomendación sobre creación de perfiles, apartado 3.4, letra b) TEDH, *Y contra Turquía*, n.º 648/10, 2015
Reglamento general de protección de datos, artículo 6, apartado 4	**Excepción a la limitación de la finalidad: tratamiento ulterior para otros fines**	Convenio 108 modernizado, artículo 5, apartado 4, letra b)
Normas sobre el tratamiento lícito de datos sensibles		
Reglamento general de protección de datos, artículo 9, apartado 1	**Prohibición general de tratamiento**	Convenio 108 modernizado, artículo 6
Reglamento general de protección de datos, artículo 9, apartado 2	**Excepciones a la prohibición general**	Convenio 108 modernizado, artículo 6
Normas relativas al tratamiento seguro		
Reglamento general de protección de datos, artículo 32	**Obligación de garantizar el tratamiento seguro**	Convenio 108 modernizado, artículo 7, apartado 1 TEDH, *I contra Finlandia*, n.º 20511/03, 2008.
Reglamento general de protección de datos, artículos 28 y 32, apartado 1, letra b)	**Obligación de confidencialidad**	Convenio 108 modernizado, artículo 7, apartado 1
Reglamento general de protección de datos, artículo 34 Directiva sobre la privacidad y las comunicaciones electrónicas, artículo 4, apartado 2	**Notificación de violación de datos personales**	Convenio 108 modernizado, artículo 7, apartado 2
Normas sobre responsabilidad proactiva y promoción del cumplimiento		
Reglamento general de protección de datos, artículos 12, 13 y 14	**Transparencia en general**	Convenio 108 modernizado, artículo 8
Reglamento general de protección de datos, artículos 37, 38 y 39	**Delegados de protección de datos**	Convenio 108 modernizado, artículo 10, apartado 1
Reglamento general de protección de datos, artículo 30	**Registros de las actividades de tratamiento**	

UE	Materias tratadas	CdE
Reglamento general de protección de datos, artículos 35 y 36	Evaluación de impacto y consulta previa	Convenio 108 modernizado, artículo 10, apartado 2
Reglamento general de protección de datos, artículos 33 y 34	Notificación de violación de datos personales	Convenio 108 modernizado, artículo 7, apartado 2
Reglamento general de protección de datos, artículos 40 y 41	Códigos de conducta	
Reglamento general de protección de datos, artículos 42 y 43	Certificación	
Protección de los datos desde el diseño y por defecto		
Reglamento general de protección de datos, artículo 25, apartado 1	Protección de datos desde el diseño	Convenio 108 modernizado, artículo 10, apartado 2
Reglamento general de protección de datos, artículo 25, apartado 2	Protección de datos por defecto	Convenio 108 modernizado, artículo 10, apartado 3

Los principios tienen necesariamente un carácter general. Su aplicación a situaciones concretas deja un cierto margen de interpretación y de elección de las medidas. De conformidad con el **Derecho del CdE**, queda al arbitrio de las Partes del Convenio 108 aclarar este margen de interpretación en sus legislaciones nacionales. La situación es diferente en el **Derecho de la UE**: para establecer la protección de los datos en el mercado interior, se consideró necesario contar con normas más detalladas a escala de la Unión para armonizar el nivel de protección de los datos en las legislaciones nacionales de los Estados miembros. El Reglamento general de protección de datos establece un nivel de normas detalladas conforme a los principios establecidos en su artículo 5, que son de aplicación directa en el ordenamiento jurídico nacional. Por tanto, las siguientes observaciones sobre las normas detalladas en materia de protección de datos a escala europea versan principalmente sobre el Derecho de la UE.

4.1. Normas relativas al tratamiento lícito

Puntos clave

- Los datos personales pueden ser objeto de tratamiento de forma lícita si se cumple al menos uno de los siguientes criterios:
  - el tratamiento se basa en el consentimiento del interesado;
  - una relación contractual requiere el tratamiento de datos personales;

- el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- los intereses vitales de los interesados o de otra persona requieren el tratamiento de sus datos;
- el tratamiento es necesario para cumplir una misión de interés público;
- el motivo del tratamiento son los intereses legítimos de los responsables del tratamiento o de terceros, aunque solo mientras no prevalezcan los intereses o los derechos fundamentales de los interesados.

- El tratamiento lícito de datos personales sensibles está sometido a un régimen especial más estricto.

4.1.1. Motivos lícitos para tratar datos

El capítulo II del Reglamento general de protección de datos, titulado «Principios», estipula que todo tratamiento de datos personales debe cumplir, en primer lugar, los principios relativos a la calidad de los datos establecidos en el artículo 5 del RGPD. Uno de estos principios es que los datos personales deben ser «tratados de manera lícita, leal y transparente». En segundo lugar, para que el tratamiento de los datos sea lícito debe estar basado en uno de los motivos lícitos que legitiman el tratamiento, recogidos en el artículo 6 ([341]) para el caso de los datos personales no sensibles y en el artículo 9 para categorías especiales de datos (o datos sensibles). Del mismo modo, el capítulo II del Convenio 108 modernizado, que recoge los «principios básicos para la protección de datos personales», establece que, para ser lícito, el tratamiento de datos debe ser «proporcionado en relación con el fin legítimo perseguido».

Al margen del motivo lícito en que se base un responsable para iniciar una operación de tratamiento de datos personales, dicho responsable deberá además aplicar las garantías establecidas en el régimen jurídico general de protección de datos.

([341]) TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof contra Österreichischer Rundfunk y otros* y *Christa Neukomm y Joseph Lauermann contra Österreichischer Rundfunk*, 20 de mayo de 2003, apartado 65; TJUE, C-524/06, *Heinz Huber contra Bundesrepublik Deutschland* [GS], 16 de diciembre de 2008, apartado 48; TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 24 de noviembre de 2011, apartado 26.

Consentimiento

En el Derecho del CdE, el consentimiento se menciona en el artículo 5, apartado 2 del Convenio 108 modernizado. También aparece en la jurisprudencia del TEDH y en varias recomendaciones del CdE ([342]). **En el Derecho de la UE**, el consentimiento como base para la licitud del tratamiento de datos está firmemente establecidos en el artículo 6 del RGPD, y el artículo 8 de la Carta también incluye una referencia explícita a este aspecto. Las características del consentimiento válido se explican en la definición de consentimiento del artículo 4, mientras que las condiciones para obtener un consentimiento válido se detallan en el artículo 7 y las normas especiales que se aplican al consentimiento del menor en relación con los servicios de la sociedad de la información están recogidas en el artículo 8 del RGPD.

Como se ha explicado en la sección 2.4, el consentimiento debe ser una manifestación de voluntad libre, específica, informada e inequívoca. El consentimiento debe ser una declaración o una clara acción afirmativa que signifique aceptación del tratamiento, y la persona tiene derecho a retirar su consentimiento en cualquier momento. Los responsables del tratamiento tienen la obligación de mantener un registro verificable del consentimiento.

Consentimiento libre

En el marco del Convenio 108 modernizado del **CdE**, el consentimiento del interesado debe «representar la libre expresión de una decisión intencional» ([343]). La existencia de un consentimiento libre únicamente es válida «si el interesado puede elegir una opción real y no hay ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no se consienta» ([344]). En este sentido, el **Derecho de la UE** estipula que el consentimiento no debe considerarse libremente prestado «cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar consentimiento sin sufrir perjuicio alguno» ([345]). El RGPD resalta que «[a]l evaluar si el consentimiento se ha dado libre-

([342]) Véase, por ejemplo, Consejo de Europa, Comité de Ministros (2010), Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, 23 de noviembre de 2010, apartado 3.4, letra b).

([343]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 42.

([344]) Véase asimismo Grupo de Trabajo del Artículo 29 (2011), *Dictamen 15/2011 sobre la definición de consentimiento*, WP 187, Bruselas, 13 de julio de 2011, p. 12.

([345]) Reglamento general de protección de datos, considerando 42.

mente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato» ([346]). El Informe explicativo del Convenio 108 modernizado establece que «[n]o se podrá ejercer sobre el interesado ninguna influencia o presión indebida (que puede ser de carácter económico o de otra índole), ya sea directa o indirecta, y el consentimiento no deberá considerarse como libremente prestado cuando el interesado no tenga una verdadera capacidad de elección o no pueda negar o retirar su consentimiento sin sufrir perjuicios» ([347]).

Ejemplo: Algunos ayuntamientos del Estado A deciden expedir tarjetas de residencia con un chip integrado. La adquisición de estas tarjetas electrónicas no es obligatoria para los residentes. Sin embargo, los residentes que no poseen la tarjeta no tienen acceso a una serie de importantes servicios administrativos, como la posibilidad de pagar los impuestos municipales en línea, presentar reclamaciones por vía electrónica con un plazo de tres días para obtener respuesta de la administración, e incluso a no hacer colas, comprar entradas a precio reducido para visitar el auditorio municipal y utilizar los lectores de código de barras a la entrada.

En este ejemplo, el tratamiento de datos personales por parte de los municipios no puede basarse en el consentimiento. Dado que existe al menos una presión indirecta para que los residentes obtengan la tarjeta electrónica y acepten el tratamiento de sus datos, el consentimiento no se otorga libremente. Por tanto, la creación de un sistema de tarjetas electrónicas por parte de los ayuntamientos debe basarse en otro motivo legítimo que justifique el tratamiento de datos personales. Por ejemplo, pueden aducir que el tratamiento es necesario para cumplir una misión de interés público, que es un fundamento lícito para el tratamiento de conformidad con el artículo 6, apartado 1, letra e) del RGPD ([348]).

([346]) Ibíd., artículo 7, apartado 4.

([347]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 42.

([348]) Grupo de Trabajo del Artículo 29 (2011), *Dictamen 15/2011 sobre la definición de consentimiento*, WP 187, Bruselas, 13 de julio de 2011, p. 16. Las páginas 14 y 17 de este dictamen contienen ejemplos adicionales de casos en que el tratamiento de datos no puede basarse en el consentimiento, sino que requiere un fundamento jurídico diferente para legitimarlo.

El consentimiento libre también podría ponerse en duda en situaciones de subordinación, en las cuales existe un importante desequilibrio económico o de otro tipo entre el responsable del tratamiento que obtiene el consentimiento y el interesado que lo otorga ([349]). Un ejemplo típico de los desequilibrios y la subordinación descritos es el tratamiento de datos personales por parte de un empleador en el contexto de una relación laboral. De acuerdo con el Grupo de Trabajo del Artículo 29, «[l]os trabajadores casi nunca están en disposición de dar, denegar o revocar el consentimiento libremente, habida cuenta de la dependencia que resulta de la relación empresario/trabajador. Dado el desequilibrio de poder, los trabajadores solo pueden dar su libre consentimiento en circunstancias excepcionales, cuando la aceptación o el rechazo de una oferta no tiene consecuencias» ([350]).

Ejemplo: Una gran empresa tiene previsto crear una base de datos con los nombres de todos los empleados, su función en la empresa y sus direcciones profesionales, con el único fin de mejorar las comunicaciones internas de la empresa. El jefe de personal propone añadir una fotografía de cada empleado a la base de datos para facilitar que los empleados se reconozcan en las reuniones. Los representantes de los trabajadores piden que esto solo se haga si los empleados otorgan individualmente su consentimiento para tal fin.

En esta situación, el consentimiento del empleado debe reconocerse como la base jurídica del tratamiento de las fotos en la base de datos, porque es creíble que no haya ningún tipo de consecuencias para el empleado en función de si decide o no aceptar que se publique su foto en la base de datos.

Ejemplo: La Empresa A está planificando una reunión entre tres de sus empleados y los directores de la Empresa B para debatir sobre las posibilidades de cooperación futura en un proyecto. La reunión tendrá lugar en las instalaciones de la Empresa B, que pide a la Empresa A que le envíe por correo electrónico el nombre, CV y foto de las personas que acudirán. La Empresa B alega que necesita el nombre y la foto de los participantes para

([349]) Véase también Grupo de Trabajo del Artículo 29 (2001), *Dictamen 8/2001 sobre tratamiento de datos personales en el contexto laboral*, WP 48, Bruselas, 13 de septiembre de 2001; Grupo de Trabajo del Artículo 29 (2005), *Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995*, WP 114, Bruselas, 25 de noviembre de 2005; Grupo de Trabajo del Artículo 29 (2017), *Dictamen 2/2017 sobre el tratamiento de datos personales en el trabajo*, WP 249, Bruselas, 8 de junio de 2017.

([350]) Grupo de Trabajo del Artículo 29, *Dictamen 2/2017 sobre el tratamiento de datos personales en el trabajo*, WP 249, Bruselas, 8 de junio de 2017.

que el personal de seguridad pueda verificar que son las personas adecuadas a la entrada del edificio, mientras que los CV permitirá a los directores prepararse mejor para la reunión. En este caso, la transmisión por parte de la Empresa A de los datos personales de sus empleados no puede estar basada en el consentimiento. No se puede considerar que el consentimiento haya sido «libremente prestado», ya que es posible que si los empleados rechazan la oferta sufran consecuencias negativas (por ejemplo, podrían ser sustituidos por otro compañero no solo en la reunión, sino también en el enlace con la Empresa B y en la colaboración en el proyecto con carácter general). Por tanto, el tratamiento de datos personales debe basarse en otro motivo legítimo.

Esto no significa, sin embargo, que el consentimiento nunca pueda ser válido en circunstancias en que la falta de consentimiento tuviera algunas consecuencias negativas. Por ejemplo, si la consecuencia de la falta de consentimiento para tener una tarjeta de cliente de un supermercado es únicamente que no se recibirán pequeños descuentos en los precios de algunos productos, el consentimiento podría ser una base jurídica válida para tratar los datos personales de aquellos clientes que otorguen su consentimiento para tener dicha tarjeta. No existe subordinación entre la empresa y el cliente, y las consecuencias de la falta de consentimiento no son lo suficientemente graves como para limitar la libertad de elección del interesado (siempre que la reducción de precio sea lo suficientemente pequeña como para no afectar a dicha libertad de elección).

Sin embargo, cuando solo sea posible obtener bienes o servicios a cambio de comunicar determinados datos personales al responsable del tratamiento o a terceros, el consentimiento del interesado para que se difundan sus datos, que no son necesarios para el contrato, no podrá considerarse una decisión libre y, por tanto, no será válido conforme a la normativa de protección de datos ([351]). El RGPD es bastante estricto en cuanto a la prohibición de condicionar la provisión de bienes y servicios al consentimiento ([352]).

Ejemplo: La conformidad que los pasajeros manifiestan a una compañía aérea que transmite los registros de nombres de pasajeros (que contienen datos sobre su identidad, hábitos alimentarios o problemas de salud) a las

([351]) Reglamento general de protección de datos, artículo 7, apartado 4.

([352]) Ibíd.

autoridades de inmigración de un determinado país extranjero no puede considerarse un consentimiento válido en virtud de la legislación en materia de protección de datos, ya que los viajeros no tienen elección si desean visitar este país. Para que estos datos se transfieran de forma lícita, será necesaria otra base jurídica distinta del consentimiento, probablemente una legislación específica.

Consentimiento informado

El interesado deberá contar con la suficiente información antes de tomar su decisión. El consentimiento informado suele incluir una descripción precisa y fácilmente comprensible del motivo por el que se requiere el consentimiento. Como explica el Grupo de Trabajo del Artículo 29, el consentimiento debe basarse en una apreciación y comprensión de los hechos y de las implicaciones que conlleva para el interesado el hecho de autorizar el tratamiento. Por tanto, «[e]l individuo afectado debe contar con información exacta y completa, de manera clara y comprensible, sobre todas las cuestiones pertinentes [...], tal como la naturaleza de los datos tratados, los fines del tratamiento de que van a ser objeto los datos, los destinatarios de los mismos y los derechos del interesado» ([353]). Para que el consentimiento sea informado, las personas físicas también deben conocer las consecuencias que se derivan de no consentir el tratamiento de sus datos.

En vista de la importancia del consentimiento informado, el RGPD y el Informe explicativo del Convenio 108 modernizado trataron de aclarar el concepto. Los considerandos del RGPD estipulan que, para que el consentimiento sea informado, «el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales» tratados ([354]).

En el caso excepcional de que el consentimiento se utilice como excepción para garantizar un motivo lícito para una transferencia de datos internacional, el responsable del tratamiento deberá informar al interesado de los posibles riesgos de

([353]) Grupo de Trabajo del Artículo 29 (2007), Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), WP 131, Bruselas, 15 de febrero de 2007.

([354]) Reglamento general de protección de datos, considerando 42.

dicha transferencia, en ausencia de una decisión de adecuación de conformidad o de garantías adecuadas, para que dicho consentimiento se considere válido ([355]).

El Informe explicativo del Convenio 108 modernizado especifica que debe facilitarse información sobre las implicaciones de la decisión del interesado, concretamente «qué conlleva el hecho del consentimiento y el alcance del mismo» ([356]).

La calidad de la información es importante. Para que la información sea de calidad, deberá facilitarse en un lenguaje adaptado a sus destinatarios previsibles. La información debe facilitarse sin jerga técnica, en un lenguaje claro y sencillo que un usuario corriente deba ser capaz de entender ([357]). También debe estar fácilmente disponible para el interesado y puede facilitarse verbalmente o por escrito. La accesibilidad y la visibilidad de la información son elementos importantes: la información debe ser claramente visible y notoria. En un entorno en línea, los avisos informativos por niveles pueden ser una buena solución, ya que permiten a los interesados elegir si acceden a versiones más concisas o más extensas de la información.

Consentimiento específico

Para que el consentimiento sea válido, debe ser además específico para el fin del tratamiento, que debe describirse de manera clara e inequívoca. Esto va de la mano con la calidad de la información que se facilita sobre la finalidad del consentimiento. En este contexto, serán pertinentes las expectativas razonables del interesado medio. Deberá solicitarse de nuevo al interesado su consentimiento en caso de que deban añadirse operaciones de tratamiento o modificarse de un modo que no podría haberse previsto razonablemente cuando se otorgó el consentimiento inicial y que ocasione, por tanto, un cambio de finalidad. Cuando el tratamiento tenga varios fines, deberá darse el consentimiento para todos ellos ([358]).

([355]) Ibíd., artículo 49, apartado 1, letra a).

([356]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 42.

([357]) Grupo de Trabajo del Artículo 29 (2011), *Dictamen 15/2011 sobre la definición de consentimiento*, , WP 187, Bruselas, 13 de julio de 2011, p. 19..

([358]) Reglamento general de protección de datos, considerando 32.

Ejemplos: En *Deutsche Telekom AG* ([359]) el TJUE consideró si un proveedor de telecomunicaciones que tenía que transferir datos personales de sus abonados para que se publicasen en guías necesitaba renovar el consentimiento de los interesados ([360]), ya que los destinatarios de los datos no se nombraron cuando se otorgó el consentimiento original.

El TJUE resolvió que, en virtud del artículo 12 de la Directiva sobre la privacidad y las comunicaciones electrónicas, no era necesario renovar el consentimiento antes de transferir los datos. Dado que los interesados solo habían tenido la opción de consentir la finalidad del tratamiento —que era la publicación de sus datos—, no podían elegir entre distintas guías en las que se pudieran publicar estos datos.

Como subrayó el TJUE, «de una interpretación lógica y sistemática del artículo 12 de la Directiva sobre privacidad y comunicaciones electrónicas se deduce que el consentimiento contemplado en el segundo apartado de este artículo se refiere a la finalidad de la publicación de los datos en una guía pública, y no a la identidad del proveedor concreto de dicha guía» ([361]). Asimismo, «es la propia publicación de los datos de carácter personal en una guía con una finalidad particular lo que puede resultar perjudicial para un abonado» ([362]), en lugar de tratarse de un asunto relacionado con la identidad del editor.

Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV contra Autoriteit Consument en Markt (ACM) ([363]) trataba de que una empresa belga prestadora de servicios de información sobre números de abonados y guías de abonados había solicitado que las empresas que asignan números de teléfono en los Países Bajos le facilitasen datos relativos a sus abonados. La empresa belga se basaba en una obligación recogida en la Directiva de

([359]) TJUE, C-543/09, *Deutsche Telekom AG contra Bundesrepublik Deutschland*, 5 de mayo de 2011. Véanse, en especial, los apartados 53 y 54.

([360]) 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, DO 2002 L 201 (Directiva sobre la privacidad y las comunicaciones electrónicas).

([361]) TJUE, C-543/09, *Deutsche Telekom AG contra Bundesrepublik Deutschland*, 5 de mayo de 2011; apdo. 61.

([362]) Ibíd., apartado 62.

([363]) TJUE, C-536/15, *Tele2 (Netherlands) BV y otros contra Autoriteit Consument en Markt (ACM)*, 15 de marzo de 2017.

servicio universal ([364]), que establece que las empresas que asignan números de teléfono deben facilitar los números a las guías que los soliciten, si los abonados habían dado su consentimiento para que se publicasen sus números. Las empresas neerlandesas se negaron a ello, alegando que no estaban obligadas a facilitar los datos en cuestión a una empresa radicada en otro Estado miembro. Argumentaron que los usuarios habían otorgado su consentimiento para que se publicasen sus números en el entendido de que se publicarían en una guía neerlandesa. El TJUE resolvió que la Directiva de servicio universal abarca todas las solicitudes realizadas por las empresas dedicadas a elaborar guías de abonados, al margen del Estado miembro en que estén radicadas. El TJUE resolvió además que la transmisión de dichos datos a otra empresa que desee publicar una guía, sin que los abonados hayan renovado su consentimiento, no vulnera el contenido esencial del derecho a la protección de datos de carácter personal ([365]). En consecuencia, no es preciso que la empresa que asigna números de teléfono a sus abonados formule la solicitud de consentimiento dirigida al abonado de manera que este exprese dicho consentimiento de manera diferenciada en función del Estado miembro al que pueden transmitirse dichos datos ([366]).

Consentimiento inequívoco

Todos los consentimientos deben otorgarse de forma inequívoca ([367]). Esto significa que no debe existir ninguna duda razonable de que el interesado deseaba dar su consentimiento al tratamiento de sus datos. Por ejemplo, la inactividad de un interesado no indica un consentimiento inequívoco.

Este sería el caso de un responsable del tratamiento que obtuviera el consentimiento incluyendo en sus políticas de privacidad declaraciones del tipo: «al utilizar nuestro servicio, usted consiente el tratamiento de sus datos personales». En ese caso, los responsables del tratamiento podrían tener que asegurarse de

([364]) Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva de servicio universal). DO 2002 L 108, p. 51, en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (Directiva de servicio universal), DO 2009 L 337, p. 11.

([365]) TJUE, C-536/15, *Tele2 (Netherlands) BV y otros contra Autoriteit Consument en Markt (ACM)*, 15 de marzo de 2017, apartado 36.

([366]) Ibíd., apartados 40-41.

([367]) Reglamento general de protección de datos, artículo 4, apartado 11.

que los usuarios expresen su consentimiento con dichas políticas de forma manual e individual.

Si el consentimiento se otorga en forma escrita dentro de un contrato, el consentimiento en el tratamiento de datos personales debe ser individualizado y, en todo caso, «debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace» ([368]).

Requisitos de consentimiento para los niños

El RGPD establece una protección específica para los niños en el contexto de la prestación de servicios de la sociedad de la información porque «pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales» ([369]). En consecuencia, en el **Derecho de la UE**, cuando los proveedores de servicios de la sociedad de la información tratan datos personales de niños menores de dieciséis años basándose en su consentimiento, dicho tratamiento solo será lícito «si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó» ([370]). Los Estados miembros pueden contemplar una edad menor en el Derecho nacional, si bien nunca inferior a 13 años ([371]). El consentimiento del titular de la patria potestad no es necesario «en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños» ([372]). La información y la comunicación, cuando el tratamiento afecte a un niño, debe facilitarse en un lenguaje claro y sencillo que le sea fácil de entender ([373]).

([368]) Ibíd., considerando 42.

([369]) Ibíd., considerando 38.

([370]) Ibíd. Artículo 8, apartado 1, primer guion. El concepto de servicios de la sociedad de la información está definido en el artículo 4, apartado 25 del Reglamento general de protección de datos.

([371]) Reglamento general de protección de datos, artículo 8, apartado 1, segundo guion.

([372]) Ibíd., considerando 38.

([373]) Ibíd., considerando 58. Véase asimismo Convenio 108 modernizado, párrafo segundo del artículo 15, letra e), segundo guion. Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartados 68 y 125.

El derecho a retirar el consentimiento en cualquier momento

El RGPD incluye un derecho general a retirar el consentimiento en cualquier momento ([374]). El interesado debe ser informado de este derecho antes de dar su consentimiento, y podrá ejercer dicho derecho cuando lo considere oportuno. No debe existir obligación de justificar dicha retirada ni riesgo alguno de consecuencias negativas más allá de que cesen todos los beneficios que pudieran haberse derivado del uso de los datos previamente acordado. Retirar el consentimiento debe ser tan fácil como otorgarlo ([375]). No puede existir consentimiento libremente prestado cuando el interesado no puede retirar su consentimiento sin sufrir perjuicio alguno o si no es tan fácil retirarlo como fue darlo ([376]).

Ejemplo: Un cliente acepta recibir correo promocional en la dirección que facilita a un responsable del tratamiento de datos. En caso de que el cliente retire su consentimiento, el responsable del tratamiento deberá dejar de enviar correos promocionales de forma inmediata. No deben imponerse consecuencias punitivas, como por ejemplo tasas. No obstante, la retirada se ejerce de cara al futuro y no tiene efectos retroactivos. El periodo durante el cual se realizó un tratamiento lícito de los datos personales del cliente —debido al consentimiento de este— había sido legítimo. La retirada impide cualquier tratamiento ulterior de esos datos, a menos que dicho tratamiento sea conforme con el derecho de supresión ([377]).

Necesidad para la ejecución de un contrato

En el Derecho de la UE, el artículo 6, apartado 1, letra b) del RGPD establece otro fundamento para el tratamiento legítimo, concretamente si es «necesario para la ejecución de un contrato en el que el interesado es parte». Esta disposición también comprende las relaciones precontractuales. Por ejemplo, en aquellos casos en que una parte pretende celebrar un contrato, pero todavía no lo ha hecho, posiblemente

([374]) Reglamento general de protección de datos, artículo 7, apartado 3. Comité Ad hoc sobre Protección de Datos (CAHDATA), Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 45.

([375]) Reglamento general de protección de datos, artículo 7, apartado 3.

([376]) Reglamento general de protección de datos, considerando 42; Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 42.

([377]) Reglamento general de protección de datos, artículo 17, apartado 1, letra b).

porque todavía faltan por hacer algunas comprobaciones. Si una parte necesita tratar datos para este fin, dicho tratamiento será legítimo en la medida en que sea necesario «con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato» ([378]).

El concepto del tratamiento de datos como «base legítima establecida por la ley» recogido en el artículo 5, apartado 2 del Convenio 108 modernizado también comprende el «tratamiento de datos necesario para el cumplimiento de un contrato (o medidas precontractuales a petición del interesado) en el cual el interesado sea parte» ([379]).

Obligaciones legales del responsable del tratamiento

El **Derecho de la UE** establece otro motivo para legitimar el tratamiento de datos, en concreto, si «es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento» (artículo 6, apartado 1, letra c) del RGPD). Esta disposición se refiere a los responsables del tratamiento que actúan tanto en el sector privado como en el sector público; las obligaciones legales de los responsables del tratamiento de datos del sector público también pueden estar comprendidas en el artículo 6, apartado 1, letra e) del RGPD. Hay muchos ejemplos de situaciones en que la ley obliga a los responsables del tratamiento del sector privado a tratar datos relativos a interesados concretos. Por ejemplo, los empleadores deben tratar los datos de sus empleados por razones de seguridad social y fiscalidad y las empresas deben tratar datos acerca de sus clientes por razones fiscales.

La obligación legal puede tener su origen en el Derecho de la Unión o del Estado miembro, que puede ser la base para una o varias operaciones de tratamiento. Debe ser la ley la que determine la finalidad del tratamiento, establezca especificaciones para determinar el responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal ([380]). Toda ley

([378]) Ibíd., artículo 6, apartado 1, letra b).

([379]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 46.; Consejo de Europa, Comité de Ministros (2010), Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, 23 de noviembre de 2010, apartado 3.4, letra b).

([380]) Reglamento general de protección de datos, considerando 45.

que de este modo sirva de base al tratamiento de datos personales deberá cumplir tanto los artículos 7 y 8 de la Carta como el artículo 8 del CEDH.

Las obligaciones legales del controlador también sirven de base al tratamiento legítimo de los datos personales **en el Derecho del CdE** ([381]). Como se ha señalado anteriormente, las obligaciones legales de un responsable del tratamiento perteneciente al sector privado constituyen únicamente un caso concreto de interés legítimo de otras personas, como menciona el artículo 8, apartado 2, del CEDH. Por tanto, el ejemplo sobre los empleadores que tratan datos de sus empleados es igualmente pertinente para el Derecho del CdE.

Intereses vitales del interesado o de otra persona física

En el Derecho de la UE, el artículo 6, apartado 1, letra d) del RGPD establece que el tratamiento de datos personales es lícito si «es necesario para proteger intereses vitales del interesado o de otra persona física». Este motivo legítimo solo podrá invocarse para el tratamiento de datos basado en los intereses vitales de otra persona física cuando el tratamiento «no pueda basarse manifiestamente en una base jurídica diferente» ([382]). A veces, un tipo de tratamiento se puede basar tanto en razones de interés público como en los intereses vitales del interesado o de otra persona. Así ocurre, por ejemplo, en el control de epidemias y su propagación o en situaciones de emergencia humanitaria.

En el Derecho del CdE, el artículo 8 del CEDH no menciona los intereses vitales del interesado como un motivo de injerencia legítima en el derecho a la protección de datos. Sin embargo, los intereses vitales del interesado se consideran implícitos en el concepto de «base legítima» recogido en el artículo 5, apartado 2 del Convenio 108 modernizado, que trata de legitimidad del tratamiento de datos personales ([383]).

([381]) Consejo de Europa, Comité de Ministros (2010), Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, 23 de noviembre de 2010, apartado 3.4, letra a).

([382]) Reglamento general de protección de datos, considerando 46.

([383]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 46.

Interés público y ejercicio del poder público

Teniendo en cuenta las múltiples formas posibles que existen de organizar los asuntos públicos, el artículo 6, apartado 1, letra e) del RGPD establece que los datos personales podrán ser tratados de forma lícita si «es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento [...]» ([384]).

Ejemplo: En *Huber contra Bundesrepublik Deutschland* ([385]), el Sr. Huber, nacional austriaco residente en Alemania, solicitó a la Oficina Federal de Migración y Refugiados la cancelación de los datos sobre su persona en el Registro Central de Extranjeros (en adelante, «AZR»). Este registro, que contiene datos personales de nacionales de la UE no alemanes con un periodo de residencia en Alemania superior a tres meses, se utiliza con fines estadísticos, así como por las autoridades policiales y judiciales en la investigación y el enjuiciamiento de actividades delictivas o que pongan en peligro la seguridad pública. El órgano jurisdiccional remitente preguntó si el tratamiento de datos personales realizado en un registro como el Registro Central de Extranjeros —al cual tienen acceso otras autoridades públicas— es compatible con el Derecho de la UE, dado que no existe tal registro para los nacionales alemanes.

El TJUE resolvió que, de conformidad con el artículo 7, letra e) de la Directiva 95/46 ([386]), el tratamiento de datos personales puede ser lícito si es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público.

Según el TJUE, «habida cuenta del objetivo consistente en equiparar el nivel de protección en todos los Estados miembros, el concepto de necesidad, tal como resulta del artículo 7, letra e), de la Directiva 95/46 ([387]) [...] no puede tener un contenido variable en función de los Estados miembros. Por lo tanto,

([384]) Véase el Reglamento general de protección de datos, considerando 45.

([385]) TJUE, C-524/06, *Heinz Huber contra Bundesrepublik Deutschland* [GS], 16 de diciembre de 2008.

([386]) Antigua Directiva sobre protección de datos, artículo 7, letra e), actual Reglamento general de protección de datos, artículo 6, apartado 1, letra e).

([387]) Ibíd.

se trata de un concepto autónomo del Derecho comunitario que debe recibir una interpretación idónea para responder plenamente al objeto de dicha Directiva, tal como se define en el artículo 1, apartado 1, de la misma» ([388]).

El TJUE señaló que el derecho de un ciudadano de la Unión a residir en el territorio de un Estado miembro del que no es nacional no es incondicional, sino que puede estar acompañado de las limitaciones y de las condiciones previstas por el Tratado, así como por las disposiciones adoptadas para su aplicación. De este modo, en principio es legítimo que un Estado miembro utilice un registro como el AZR para facilitar el trabajo de las autoridades encargadas de aplicar la normativa relativa al derecho de residencia, si bien dicho registro no podrá contener más información de la necesaria para tal fin. El TJUE concluyó que dicho sistema de tratamiento de datos personales cumple con la legislación de la UE si contiene únicamente los datos necesarios para la aplicación de dicha normativa y si su carácter centralizado permite una aplicación más eficaz de dicha normativa. El órgano jurisdiccional nacional deberá verificar estos extremos en el litigio particular. De no ser así, no existe ningún motivo para considerar que la conservación y el tratamiento de datos personales en un registro como el AZR con fines estadísticos sean necesarios en el sentido del artículo 7, letra e) ([389]), de la Directiva 95/46/CE ([390]).

Por último, en lo que atañe a la cuestión del uso de los datos incluidos en el registro con el fin de combatir la delincuencia, el TJUE resolvió que dicho fin «tiene necesariamente por objeto la persecución de los crímenes y delitos cometidos, con independencia de la nacionalidad de sus autores». El registro controvertido no contiene datos personales relacionados con nacionales del Estado miembro en cuestión y esta diferencia de tratamiento constituye una discriminación prohibida por el artículo 18 del TFUE. Por consiguiente, el TJUE resolvió que esta disposición «se opone a que un Estado miembro instaure, en aras de combatir la delincuencia, un sistema de tratamiento de datos personales específico para los ciudadanos de la Unión que no sean nacionales de dicho Estado miembro» ([391]).

([388]) TJUE, C-524/06, *Heinz Huber contra Bundesrepublik Deutschland* [GS], 16 de diciembre de 2008, apartado 52.

([389]) Antigua Directiva sobre protección de datos, artículo 7, letra e), actual Reglamento general de protección de datos, artículo 6, apartado 1, letra e).

([390]) TJUE, C-524/06, *Heinz Huber contra Bundesrepublik Deutschland* [GS], 16 de diciembre de 2008, apartados 54, 58-59 y 66-68.

([391]) Ibíd., apartados 78 y 81.

El uso de los datos personales por parte de las autoridades que actúen en el ámbito público está igualmente sujeto al artículo 8 del **CEDH** y se entiende cubierto, en su caso, por el párrafo segundo del artículo 5 del convenio 108 modernizado ([392]).

Intereses legítimos perseguidos por el responsable del tratamiento o por un tercero

En el **Derecho de la UE**, el interesado no es la única persona que tiene intereses legítimos. El artículo 6, apartado 1, letra f) del RGPD establece que los datos personales pueden ser tratados de forma lícita si «es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero [salvo los poderes públicos en el desempeño de sus funciones], siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección [...]» ([393]).

La existencia de un interés legítimo requiere una evaluación meticulosa en cada caso concreto ([394]). Si se identifican los interese legítimos del responsable del tratamiento, debe llevarse a cabo un ejercicio de ponderación equilibrada entre esos intereses y los intereses o derechos y libertades fundamentales del interesado ([395]). En dicha evaluación deben tomarse en consideración las expectativas razonables que tenga el interesado para determinar si los intereses del responsable del tratamiento prevalecen sobre los intereses o derechos fundamentales del interesado ([396]). Si los derechos del interesado prevalecen sobre los intereses legítimos del responsable del tratamiento, este podrá adoptar medidas y aplicar salvaguardias para minimizar el impacto sobre los derechos del interesado (como la seudonimización de los datos) e invertir el «equilibrio» antes de poder utilizar lícitamente esta base legítima para el tratamiento. En su Dictamen sobre el concepto de intereses legítimos del responsable del tratamiento, el Grupo de Trabajo del Artículo 29 subraya la importancia esencial de la responsabilidad proactiva y la transparencia y de los derechos del interesado de oposición al tratamiento de sus datos o al acceso, modificación,

([392]) Párrafos 46 y 47 del informe explicativo del convenio 108 modernizado.

([393]) En comparación con la Directiva 95/46, el Reglamento general de protección de datos ofrece más ejemplos de casos que se consideran constitutivos de un interés legítimo.

([394]) Reglamento general de protección de datos, considerando 47.

([395]) Grupo de Trabajo del Artículo 29 (2014), *Dictamen 6/2014 sobre el concepto de intereses legítimos del responsable del tratamiento conforme al artículo 7 de la Directiva 95/46/CE*, 4 de abril de 2014.

([396]) Ibíd.

supresión o transmisión de los mismos, a la hora de ponderar los intereses legítimos del responsable del tratamiento y los derechos fundamentales del interesado ([397]).

En los considerandos del RGPD, se ofrecen algunos ejemplos de lo que constituye un interés legítimo del responsable del tratamiento de que se trate. Por ejemplo, se admite el tratamiento de datos personales sin el consentimiento del interesado cuando se efectúe con fines de mercadotecnia directa o cuando sea «estrictamente necesario para la prevención del fraude» ([398]).

En su jurisprudencia, el TJUE ha desarrollado el criterio para determinar qué constituye un interés legítimo.

Ejemplo: El asunto *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* ([399]) trataba de los daños que se ocasionaron a un trolebús de una empresa de transportes de Rīgas cuando el pasajero de un taxi abrió la puerta del vehículo de forma repentina. Rīgas satiksme quería demandar al pasajero por daños y perjuicios. Sin embargo, la policía solo accedió a proporcionar el nombre del pasajero, pero se negó a facilitar su número de identificación y domicilio, alegando que revelar esa información sería ilegal conforme a la normativa nacional de protección de datos.

El órgano jurisdiccional letón remitió al TJUE una cuestión prejudicial para aclarar si la legislación de la UE en materia de protección de datos impone la obligación de revelar todos los datos personales necesarios para entablar un procedimiento civil contra la persona presuntamente responsable de una infracción administrativa ([400]).

El TJUE aclaró que la normativa de la UE en materia de protección de datos contempla la posibilidad —no la obligación— de comunicar datos a terceros para los fines de los intereses legítimos perseguidos por estos ([401]). El TJUE estableció tres condiciones acumulativas que deben satisfacerse para que

([397]) Grupo de Trabajo del Artículo 29 (2014), Dictamen 6/2014 sobre el concepto de intereses legítimos del responsable del tratamiento conforme al artículo 7 de la Directiva 95/46/CE, 4 de abril de 2014.

([398]) Reglamento general de protección de datos, considerando 47.

([399]) TJUE, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contra Rīgas pašvaldības SIA «Rīgas satiksme»*, 4 de mayo de 2017.

([400]) Ibíd., apartado 23.

([401]) Ibíd., apartado 26.

se determine la licitud del tratamiento con base en el «interés legítimo» ([402]). En primer lugar, el tercero a quien se comuniquen los datos debe perseguir un fin legítimo. En este caso concreto, esto significa que la solicitud de datos personales para demandar a una persona por causar daños en propiedades constituye un interés legítimo de un tercero. En segundo lugar, el tratamiento de datos personales debe ser necesario para los fines de los intereses legítimos perseguidos. En este caso, la obtención de datos personales como el domicilio o el número de identificación es estrictamente necesaria para identificar a esa persona. En tercer lugar, los derechos y libertades fundamentales del interesado no deben prevalecer sobre los intereses legítimos del responsable del tratamiento o de terceros. Los intereses enfrentados deben ponderarse en cada caso teniendo en cuenta elementos como la gravedad de la infracción de los derechos del interesado o incluso la edad del interesado en determinadas circunstancias. No obstante, en este caso concreto, el TJUE no consideró que estuviera justificado negarse a comunicar los datos simplemente porque el interesado fuera menor de edad.

En la sentencia *ASNEF y FECEMD*, el TJUE se refirió de forma explícita a la licitud del tratamiento de datos personales en virtud de «intereses legítimos», que en ese momento estaba consagrado en el artículo 7, letra f) de la Directiva sobre protección de datos ([403]).

Ejemplo: En *ASNEF y FECEMD* ([404]), el TJUE aclaró que la legislación nacional no puede añadir condiciones a las mencionadas en el artículo 7, letra f) de la Directiva en relación con la licitud del tratamiento de los datos ([405]). Dicho asunto hacía referencia a la circunstancia de que la legislación española de protección de datos contenía una disposición por la cual otras partes privadas podían reivindicar un interés legítimo en el tratamiento de datos personales únicamente si ya figuraban en fuentes accesibles al público.

([402]) Ibíd., apartados 28-34.

([403]) Antigua Directiva sobre protección de datos, artículo 7, letra f), actual Reglamento general de protección de datos, artículo 6, apartado 1, letra f).

([404]) TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 24 de noviembre de 2011.

([405]) Antigua Directiva sobre protección de datos, artículo 7, letra f), actual Reglamento general de protección de datos, artículo 6, apartado 1, letra f).

El TJUE señaló en primer lugar que la Directiva 95/46 ([406]) trata de garantizar que el nivel de protección de los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales sea equivalente en todos los Estados miembros. La aproximación de las legislaciones aplicables en esta materia no debe reducir la protección que garantizan. Por el contrario, debe asegurar un alto nivel de protección en la UE ([407]). Así pues, el TJUE resolvió que «se deduce del objetivo consistente en asegurar un nivel de protección equivalente en todos los Estados miembros que el artículo 7 de la Directiva 95/46 ([408]) establece una lista exhaustiva y taxativa de los casos en que un tratamiento de datos personales puede considerarse lícito». Además, «los Estados miembros no pueden ni añadir al artículo 7 de la Directiva 95/46 ([409]) nuevos principios relativos a la legitimación de los tratamientos de datos personales ni imponer exigencias adicionales que vendrían a modificar el alcance de alguno de los seis principios establecidos en dicho artículo ([410])». El TJUE admitió que, en lo que respecta a la ponderación requerida por el artículo 7, letra f), de la Directiva 95/46/CE, cabe tomar en consideración el hecho de que la gravedad de la lesión de los derechos fundamentales de la persona afectada por dicho tratamiento puede variar en función de que los datos figuren ya, o no, en fuentes accesibles al público.

Sin embargo, el artículo 7, letra f) de la Directiva «se opone a que un Estado miembro excluya de forma categórica y generalizada la posibilidad de someter a un tratamiento de datos determinadas categorías de datos personales, sin permitir ponderar los derechos e intereses en conflicto en cada caso concreto».

([406]) Antigua Directiva sobre protección de datos, actual Reglamento general de protección de datos.

([407]) TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 24 de noviembre de 2011, apartado 28. Véase la Directiva sobre protección de datos, considerandos 8 y 10.

([408]) Antigua Directiva sobre protección de datos, artículo 7, actual Reglamento general de protección de datos, artículo 6, apartado 1, letra f).

([409]) Antigua Directiva sobre protección de datos, artículo 7, actual Reglamento general de protección de datos, artículo 6.

([410]) Ibíd.

Habida cuenta de estas consideraciones, el TJUE concluyó que el artículo 7, letra f) de la Directiva 95/46 ([411]) debe interpretarse en el sentido de que «se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no solo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes» ([412]).

Siempre que se lleve a cabo un tratamiento de datos personales basado en «intereses legítimos», la persona física tiene derecho a oponerse a dicho tratamiento en cualquier momento por razones relacionadas con su situación particular, en virtud del artículo 21, apartado 1 del RGPD. El responsable deberá cesar en el tratamiento, a menos que demuestre que existen motivos legítimos imperiosos para continuar realizándolo.

En lo que respecta al **Derecho del CdE**, en el Convenio108 ([413]) modernizado y en las recomendaciones del CdE pueden encontrarse formulaciones similares. La Recomendación sobre creación de perfiles reconoce que el tratamiento de datos personales con el fin de crear perfiles es legítimo si la creación de perfiles es necesaria a los efectos de los intereses legítimos de otras personas «salvo cuando los derechos y libertades fundamentales de la persona interesada prevalezcan sobre dichos intereses» ([414]). Además, «la protección de los derechos y las libertades de los demás» se menciona en el artículo 8, apartado 2 del CEDH, como uno de los motivos para limitar el derecho a la protección de datos.

([411]) Antigua Directiva sobre protección de datos, artículo 7, letra f), actual Reglamento general de protección de datos, artículo 6, apartado 1, letra f).

([412]) TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 24 de noviembre de 2011, apartados 40, 44 y 48-49.

([413]) Informe explicativo del Convenio 108 modernizado, párrafo 46.

([414]) Consejo de Europa, Comité de Ministros (2010), Recomendación CM/Rec(2010)13 y exposición de motivos sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, 23 de noviembre de 2010, apartado 3.4, letra b) (Recomendación sobre creación de perfiles).

Ejemplo: En *Y contra Turquía* ([415]), el demandante era seropositivo. Mientras estaba inconsciente a su llegada al hospital, el personal de la ambulancia comunicó al personal del hospital la condición seropositiva del paciente. El demandante alegó ante el TEDH que la revelación de esta información había violado su derecho al respeto de su vida privada. Sin embargo, dada la necesidad de proteger la seguridad del personal del hospital, no se consideró que la comunicación de esta información violase sus derechos.

4.1.2. Tratamiento de categorías especiales de datos (datos sensibles)

El Derecho del CdE deja en manos de la legislación nacional el establecimiento de medidas de protección apropiadas para el uso de datos sensibles, siempre que se cumplan las condiciones del artículo 6 de Convenio 108 modernizado, por ejemplo, que se adopten salvaguardas legales que complemente las disposiciones del Convenio. El **Derecho de la UE**, en el artículo 9 del RGPD, contiene un régimen detallado para el tratamiento de categorías especiales de datos (también denominados «datos sensibles»). Este tipo de datos revela el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. En principio, queda prohibido el tratamiento de datos sensibles ([416]).

Sin embargo, existe una lista exhaustiva de exenciones de esta prohibición, que se encuentra en el artículo 9, apartado 2 del Reglamento y que constituyen motivos lícitos para el tratamiento de datos sensibles. Estas exenciones incluyen situaciones en las que:

- el interesado dé su consentimiento explícito al tratamiento de los datos;
- el tratamiento sea realizado por un organismo sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical en el curso de sus actividades legítimas y se refiera exclusivamente a sus miembros actuales o antiguos o a personas

([415]) TEDH, *Y contra Turquía*, n.º 648/10, 17 de febrero de 2015.

([416]) Antigua Directiva sobre protección de datos, artículo 7, letra f), actual Reglamento general de protección de datos, artículo 9, apartado 1.

que mantengan contactos regulares con dicho organismo en relación con sus fines;

- el tratamiento se refiera a datos personales que el interesado haya hecho manifiestamente públicos;
- el tratamiento sea necesario:
  - para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del empleo, de la seguridad social y de la protección social;
  - para proteger los intereses vitales del interesado o de otra persona física (cuando el interesado no pueda dar su consentimiento);
  - para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
  - para fines de medicina preventiva o laboral: «evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobra la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario»;
  - con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;
  - por razones de un interés público en el ámbito de la salud pública; o
  - por razones de un interés público esencial.

Por tanto, de cara al tratamiento de categorías especiales de datos, una relación contractual con el interesado no se considera una base jurídica para el tratamiento legítimo de datos sensibles, salvo en el caso de un contrato con un profesional sanitario sujeto a la obligación de secreto profesional ([417]).

([417]) Reglamento general de protección de datos, artículo 9, apartado 2, letra h) y letra i).

Consentimiento explícito del interesado

En el **Derecho de la UE**, la primera condición para que un tratamiento de datos sea lícito, al margen de si son datos sensibles o no, es el consentimiento del interesado. En el caso de los datos sensibles, dicho consentimiento debe ser explícito. No obstante, el Derecho de la Unión o de los Estados miembros puede establecer que la prohibición del tratamiento de categorías especiales de datos no pueda ser levantada por el interesado ([418]). Esto podría ocurrir, por ejemplo, cuando el tratamiento genere riesgos inusuales al interesado.

Derecho laboral o legislación de seguridad y protección social

En el **Derecho de la UE**, la prohibición del artículo 9, apartado 1 se podrá levantar si el tratamiento es necesario para el cumplimiento de obligaciones o el ejercicio de derechos del responsable del tratamiento o del interesado en el ámbito del empleo o de la seguridad social. Sin embargo, el tratamiento ha de estar autorizado por el Derecho de la UE, por la legislación nacional o por un convenio colectivo celebrado conforme a la legislación nacional que establezca garantías adecuadas para los derechos fundamentales e intereses del interesado ([419]). Los expedientes de empleo que posee una organización pueden incluir datos personales sensibles en determinadas condiciones especificadas en el RGPD y en la legislación nacional pertinente. La información sanitaria o de pertenencia a sindicatos pueden ser ejemplos de datos sensibles.

Intereses vitales del interesado o de otra persona física

En el **Derecho de la UE**, como en el caso de los datos no sensibles, los datos sensibles podrán ser tratados con motivo de los intereses vitales del interesado o de otra persona física ([420]). Cuando el tratamiento esté basado en los intereses vitales de otra persona física, solo se podrá invocar este motivo legítimo cuando dicho tratamiento «no pueda basarse manifiestamente en una base jurídica diferente» ([421]). En algunos casos, el tratamiento de datos personales puede proteger intereses individuales y públicos, por ejemplo cuando es necesario con fines humanitarios ([422]).

([418]) Ibíd., artículo 9, apartado 2, letra a).

([419]) Reglamento general de protección de datos, artículo 9, apartado 2, letra b).

([420]) Ibíd., artículo 9, apartado 2, letra c).

([421]) Ibíd., considerando 46.

([422]) Ibíd.

Para que el tratamiento de datos sensibles sea legítimo sobre esta base, debería ser imposible pedir el consentimiento del interesado, por ejemplo, porque el interesado estuviera inconsciente o porque estuviera ausente y no pudiera ser localizado. En otras palabras, porque fuera física o legalmente incapaz de otorgar el consentimiento.

Entidades benéficas o no lucrativas

También se admite el tratamiento de datos personales en el curso de las actividades legítimas de fundaciones, asociaciones u otras entidades no lucrativas cuya finalidad sea política, filosófica, religiosa o sindical. Sin embargo, el tratamiento debe referirse exclusivamente a los miembros actuales o anteriores de estas entidades o a personas que mantengan contactos regulares con ellas ([423]). Los datos sensibles no pueden ser revelados fuera de estas entidades sin el consentimiento del interesado.

Datos que el interesado haya hecho manifiestamente públicos

El artículo 9, apartado 2, letra e) del RGPD establece que el tratamiento no está prohibido si se refiere a datos que el interesado ha hecho manifiestamente públicos. Aunque el significado de la expresión «que el interesado ha hecho manifiestamente públicos» no está definido en el Reglamento, dado que es una excepción a la prohibición del tratamiento de datos sensibles, debe interpretarse en sentido estricto y con la exigencia de que el interesado haga públicos sus datos personales de forma deliberada. De este modo, cuando una emisora de televisión difunde un vídeo obtenido con una cámara de videovigilancia que muestre, por ejemplo, a un bombero sufriendo heridas al tratar de evacuar un edificio, no cabe considerar que el bombero ha hecho manifiestamente públicos sus datos. Por otro lado, si el bombero decide explicar el incidente y publicar el vídeo y las fotos en una página pública en internet, habría realizado un acto deliberado y afirmativo de hacer públicos sus datos personales. Es importante señalar que hacer públicos los propios datos no constituye consentimiento, pero es otra forma de autorizar el tratamiento de categorías especiales de datos.

El hecho de que el interesado haya hecho públicos los datos personales tratados no exime a los responsables del tratamiento de sus obligaciones conforme a la legislación en materia de protección de datos. Por ejemplo, el principio de limitación de la

([423]) Ibíd., artículo 9, apartado 2, letra d).

finalidad sigue siendo de aplicación a los datos personales aunque dichos datos se hayan hecho públicos ([424]).

Reclamaciones

El tratamiento de categorías especiales de datos que «es necesario para la formulación, el ejercicio o la defensa de reclamaciones», ya sea en procedimientos judiciales o en procedimientos administrativos o extrajudiciales ([425]), también está permitido por el RGPD ([426]). En este caso, el tratamiento debe ser pertinente para una reclamación concreta y su ejercicio o defensa, respectivamente, y puede ser solicitado por cualquiera de las partes enfrentadas.

Cuando actúen en ejercicio de su función judicial, los tribunales podrán tratar categorías especiales de datos en el contexto de la resolución de un litigio ([427]). A modo de ejemplos de estas categorías especiales de datos en este contexto cabe citar, por ejemplo, los datos genéticos a la hora de establecer la paternidad, o el estado de salud cuando parte de las pruebas estén relacionadas con los detalles de las lesiones sufridas por la víctima de un delito.

Razones de interés público esencial

En virtud del artículo 9, apartado 2, letra g) del RGPD, los Estados miembros podrán introducir circunstancias adicionales en las que puedan tratarse datos sensibles, siempre que:

- el tratamiento de los datos sea por motivos de un interés público esencial;
- esté establecido por la legislación europea o nacional;
- la legislación europea o nacional sea proporcionada, respete el derecho a la protección de los datos y establezca medidas adecuadas y específicas para proteger los derechos e intereses del interesado ([428]).

([424]) Grupo de Trabajo del Artículo 29 (2013), *Dictamen 3/2013 sobre la limitación a una finalidad específica*, WP 203, Bruselas, 2 de abril de 2013, p. 14..

([425]) Reglamento general de protección de datos, considerando 52.

([426]) Ibíd., artículo 9, apartado 2, letra f).

([427]) Ibíd.

([428]) Ibíd., artículo 9, apartado 2, letra g).

Un ejemplo destacado son los sistemas electrónicos de información sanitaria. Estos sistemas permiten poner los datos de salud obtenidos por los prestadores de servicios sanitarios durante el tratamiento de los pacientes a disposición de otros prestadores de servicios sanitarios que atiendan a estos pacientes a gran escala, normalmente, a escala nacional.

El Grupo de Trabajo del Artículo 29 concluyó que no se podría crear este tipo de sistemas con la normativa vigente de tratamiento de datos de pacientes ([429]). No obstante, es posible que existan sistemas electrónicos de información sanitaria si están basados en «razones de interés público importante» ([430]). Para ello haría falta una base jurídica explícita, que incluyera las salvaguardias necesarias para garantizar que el sistema funciona con seguridad ([431]).

Otros motivos para el tratamiento de datos sensibles

El RGPD establece que se pueden tratar datos sensibles cuando el tratamiento sea necesario para ([432]):

- fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobra la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario;

- razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros, que debe establecer medidas adecuadas y específicas para proteger los derechos del interesado;

([429]) Grupo de Trabajo del Artículo 29 (2007), *Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)*, WP 131, Bruselas, 15 de febrero de 2007. Véase también el Reglamento general de protección de datos, artículo 9, apartado 3.

([430]) Reglamento general de protección de datos, artículo 9, apartado 2, letra g).

([431]) Grupo de Trabajo del Artículo 29 (2007), *Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)*, WP 131, Bruselas, 15 de febrero de 2007.

([432]) Reglamento general de protección de datos, artículo 9, apartado 2, letras h), i) y j).

- fines de archivo, fines de investigación científica o histórica o fines estadísticos, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos del interesado.

Condiciones adicionales conforme al Derecho nacional

El RGPD también permite que los Estados miembros introduzcan o mantengan condiciones adicionales, incluidas las limitaciones para el tratamiento de datos genéticos, biométricos o relativos a la salud ([433]).

4.2. Normas relativas a la seguridad del tratamiento

Puntos clave

- Las normas relativas a la seguridad del tratamiento obligan al responsable del tratamiento y al encargado del tratamiento a aplicar las medidas técnicas y organizativas oportunas para evitar cualquier injerencia no autorizada en las operaciones de tratamiento de datos.
- El nivel necesario de seguridad de los datos viene determinado por:
  - las características de seguridad disponibles en el mercado para un determinado tipo de tratamiento;
  - los costes;
  - los riesgos del tratamiento de los datos para los derechos y libertades fundamentales de los interesados.
- Garantizar la confidencialidad de los datos personales es parte de un principio general reconocido en el Reglamento general de protección de datos.

Tanto en el Derecho de la Unión como en el Derecho del CdE, los responsables del tratamiento tienen una obligación genérica de transparencia y responsabilidad proactiva en el tratamiento de datos personales y, en particular, en el caso de que

([433]) Ibíd., artículo 9, apartado 2, letra h) y artículo 9, apartado 4.

se produzcan violaciones de los datos personales. Los responsables del tratamiento deben notificar las violaciones de la seguridad de los datos personales a las autoridades de control a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Los interesados también deben ser informados de la violación de sus datos personales cuando esta pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas.

4.2.1. Elementos de la seguridad de los datos

De conformidad con las disposiciones pertinentes recogidas en el **Derecho de la UE**:

> *«Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo [...]* ([434])*».*

Estas medidas incluyen, entre otras cosas:

- la seudonimización y el cifrado de datos personales ([435]);
- garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento ([436]);
- restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de pérdida de datos ([437]);
- un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento ([438]).

En el **Derecho del CdE** existe una disposición similar:

([434]) Ibíd., artículo. 32 apartado 1.
([435]) Ibíd., artículo 32, apartado 1, letra a).
([436]) Ibíd., artículo 32, apartado 1, letra b).
([437]) Ibíd., artículo 32, apartado 1, letra c).
([438]) Ibíd., artículo 32, apartado 1, letra d).

«Cada Parte dispondrá que el responsable del tratamiento y, en su caso, el encargado del tratamiento adopte medidas de seguridad adecuadas contra el acceso accidental o no autorizado a los datos personales y su destrucción, pérdida, uso, modificación o difusión» ([439]).

En el **Derecho de la Unión y el Derecho del CdE**, una violación de la seguridad de los datos que pueda afectar a los derechos y libertades de las personas físicas obliga al responsable del tratamiento a notificar dicha violación a la autoridad de control (véase la sección 4.2.3).

Con frecuencia, también existen normas industriales, nacionales e internacionales que tienen por objeto la seguridad del tratamiento de datos personales. El sello europeo de privacidad EuroPriSe, por ejemplo, es un proyecto eTEN (Redes transeuropeas de telecomunicaciones) de la UE que explora las posibilidades de certificación de productos, especialmente programas informáticos, que faciliten el cumplimiento de la legislación europea en materia de protección de datos. La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) fue creada para reforzar la capacidad de la Unión Europea, de los Estados miembros y de la comunidad empresarial para prevenir, abordar y dar respuesta a los problemas de seguridad de las redes y de la información ([440]). ENISA publica periódicamente análisis de las actuales amenazas para la seguridad, así como asesoramiento para hacerles frente ([441]).

La seguridad de los datos no se logra únicamente con el equipo adecuado (hardware y programas informáticos), sino que también exige la existencia de normas internas de organización adecuadas. Lo ideal sería que dichas normas internas comprendieran las siguientes cuestiones:

- el suministro regular de información a todos los empleados sobre normas de seguridad de los datos y sus obligaciones con arreglo a la legislación en materia de protección de datos, en especial en lo referente a sus obligaciones de confidencialidad;

([439]) Convenio 108 modernizado, artículo 7, apartado 1.

([440]) Reglamento (CE) n.º 526/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativo a la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) n.º 460/2004, DO 2013 L 165.

([441]) Por ejemplo, ENISA (2016), Ciberseguridad y resiliencia de los coches inteligentes. Buenas prácticas y recomendaciones; ENISA (2016), Seguridad de los pagos móviles y de las carteras digitales.

- la distribución clara de las responsabilidades y un esquema claro de las competencias en materia de tratamiento de datos, en especial en lo que respecta a las decisiones de tratar datos personales y transmitir datos a terceros o a interesados;

- el uso de los datos personales únicamente con arreglo a las instrucciones de la persona competente o de conformidad con las normas generales establecidas;

- la protección del acceso a las ubicaciones y al hardware y programas informáticos del responsable del tratamiento o del encargado del tratamiento, incluidos los controles de las autorizaciones de acceso;

- garantizar que las autorizaciones para acceder a los datos personales han sido atribuidas por la persona competente y exigen la documentación adecuada;

- protocolos automatizados sobre el acceso electrónico a los datos personales y verificaciones periódicas de tales protocolos por el departamento de control interno (con la consiguiente obligación de registrar todas las actividades de tratamiento de datos);

- la documentación cuidadosa de otras formas de difusión distintas al acceso automatizado de los datos para poder demostrar que no se han producido transmisiones de datos ilegales.

Ofrecer a los miembros del personal formación y educación adecuadas sobre la seguridad de los datos es también un elemento importante de las precauciones de seguridad efectivas que deben adoptarse. Deben establecerse, asimismo, procedimientos de verificación para garantizar que las medidas oportunas no solo existen sobre el papel, sino que también se aplican y funcionan en la práctica (como las auditorías internas o externas).

Entre las medidas para mejorar el nivel de seguridad del responsable del tratamiento o del encargado del tratamiento se incluyen instrumentos como los delegados de protección de datos personales, la educación sobre seguridad para los empleados, las auditorías periódicas, los ensayos de penetración y los sellos de calidad.

Ejemplo: En *I contra Finlandia* ([442]), la demandante no pudo demostrar que otros empleados del hospital donde trabajaba habían accedido a su historial médico de forma ilegítima. Su reclamación de que se había violado su derecho a la protección de datos fue, por tanto, desestimada por los órganos jurisdiccionales nacionales. El TEDH concluyó que había existido una violación del artículo 8 del CEDH, ya que el sistema de registro de las historias clínicas del hospital «era tal que no era posible aclarar de forma retroactiva el uso de las historias de los pacientes tal como habían revelado las cinco últimas consultas y que dichos datos fueron suprimidos una vez que el expediente fue devuelto a los archivos». En opinión del Tribunal, resultó decisivo que el sistema de archivo existente en el hospital incumplía claramente los requisitos legales establecidos en la legislación nacional, un hecho que no fue valorado debidamente por los órganos jurisdiccionales nacionales.

La UE ha adoptado la Directiva sobre la seguridad de las redes y sistemas de información (la Directiva NIS, por sus siglas en inglés) ([443]), que es el primer instrumento jurídico de ámbito de la UE en materia de ciberseguridad. Esta Directiva tiene por objeto mejorar la ciberseguridad a escala nacional, por una parte, y aumentar el nivel de cooperación en la UE, por otra. También impone a los operadores de servicios esenciales (entre los que se incluyen operadores del sector de la energía, la salud, la banca, el transporte, las infraestructuras digitales, etc.) y a los proveedores de servicios digitales la obligación de gestionar los riesgos, garantizar la seguridad de sus redes y sistemas de información y notificar los incidentes de seguridad.

Perspectivas

En septiembre de 2017, la Comisión Europea presentó una propuesta de Reglamento destinada a reformar el mandato de ENISA, para tener en cuenta las nuevas competencias y responsabilidades de la agencia en virtud de la Directiva NIS. El objetivo del Reglamento propuesto es desarrollar las misiones de ENISA y reforzar su función como «punto de referencia en el ecosistema de ciberseguridad de la UE» ([444]). El

([442]) TEDH, *I. contra Finlandia*, n.º 20511/03, 17 de julio de 2008.

([443]) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, DO 2016 L 194.

([444]) Propuesta de Reglamento del parlamento Europeo y del Consejo relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías dela información y la comunicación («Reglamento de Ciberseguridad»), COM(2017) 477, 13 de septiembre de 2017, p. 6.

Reglamento propuesto debe entenderse sin perjuicio de los principios del RGPD y, al aclarar los elementos necesarios que integran los sistemas europeos de certificación de la ciberseguridad, debe además reforzar la seguridad de los datos personales. Paralelamente, en septiembre de 2017, la Comisión Europea presentó una propuesta de Reglamento de ejecución en el que se especificaban los elementos que deben tener en cuenta los proveedores de servicios digitales para velar por la seguridad de sus redes y sistemas de información, tal como requiere el artículo 16, apartado 8 de la Directiva NIS. En el momento de redactar el presente manual, continuaban las negociaciones sobre estas dos propuestas.

4.2.2. Confidencialidad

En el Derecho de la UE, el RGPD reconoce la confidencialidad de los datos como parte un principio general ([445]). Los proveedores de comunicaciones electrónicas públicamente disponibles deben garantizar la confidencialidad. También tienen la obligación de proteger la seguridad de sus servicios ([446]).

Ejemplo: Un empleado de una compañía de seguros recibe una llamada de teléfono en su lugar de trabajo de alguien que dice ser un cliente y le solicita información sobre su contrato de seguro.

El deber de mantener la confidencialidad de los datos de los clientes exige que el empleado aplique unas medidas de seguridad mínimas antes de revelar los datos personales. Por ejemplo, puede ofrecer a su interlocutor devolverle la llamada al número de teléfono que figura en la ficha del cliente.

En virtud del artículo 5, apartado 1, letra f), los datos personales deben ser tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

En virtud del artículo 32, el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas que garanticen un alto nivel de seguridad. Estas medidas incluyen, entre otras, la seudonimización y el cifrado de datos personales,

([445]) Reglamento general de protección de datos, artículo 5, apartado 1, letra f).

([446]) Directiva sobre la privacidad y las comunicaciones electrónicas, artículo 5, apartado 1.

la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes del tratamiento, la verificación y evaluación de la eficacia de las medidas y la capacidad de restaurar el tratamiento en caso de incidente físico o técnico. Además, la adhesión a un código de conducta aprobado o a un mecanismo de certificación aprobado puede utilizarse como elemento de demostración de que se cumple el principio de integridad y confidencialidad. Por otra parte, de acuerdo con el artículo 28 del RGPD, el contrato que vincula al responsable del tratamiento con el encargado debe estipular que el encargado ha de asegurarse de que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

El deber de confidencialidad no se amplía a las situaciones en que los datos llegan a conocimiento de una persona en cuanto que ciudadano particular y no como empleado de un responsable o encargado del tratamiento. En este caso, los artículos 32 y 28 del RGPD no son de aplicación, dado que el uso de datos personales por parte de los particulares queda totalmente exento del mandato del Reglamento cuando dicho uso se circunscribe a lo que se conoce como exención doméstica ([447]). La exención doméstica es el uso de datos personales «efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas» ([448]). No obstante, a partir de la resolución del TJUE en el asunto *Bodil Lindqvist* ([449]), esta exención debe interpretarse de forma restringida, especialmente en lo que respecta a la difusión de los datos. En particular, la exención doméstica no se extenderá a la publicación de los datos personales a un número ilimitado de destinatarios en internet ni al tratamiento de datos que incluya aspectos profesionales o comerciales (para más detalles sobre este asunto, véanse las secciones 2.1.2, 2.2.2 y 2.3.1).

La «confidencialidad de las comunicaciones» es otro aspecto de la confidencialidad que está sujeto a *lex specialis*. Las normas especiales para garantizar la confidencialidad de las comunicaciones electrónicas conforme a la Directiva sobre la privacidad y las comunicaciones electrónicas obligan a los Estados miembros a prohibir la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los metadatos asociados por personas distintas de los usuarios o sin el consentimiento de estos ([450]). La legislación nacional puede

([447]) Reglamento general de protección de datos artículo 2, apartado 2, letra c).

([448]) Ibíd.

([449]) TJUE, C-101/01, Procedimiento penal entablado contra Bodil Lindqvist, 6 de noviembre de 2003.

([450]) Directiva sobre la privacidad y las comunicaciones electrónicas, artículo 5, apartado 1.

autorizar excepciones a este principio únicamente por razones de seguridad nacional, defensa, prevención o detección de delitos y únicamente si estas medidas son necesarias y proporcionadas para los fines perseguidos ([451]). Las mismas normas se aplicarán con el futuro Reglamento sobre la privacidad y las comunicaciones electrónicas, pero el acto jurídico sobre la privacidad electrónica ampliará su ámbito de aplicación para que abarque no solo los servicios de comunicaciones electrónicas públicamente disponibles, sino también las comunicaciones efectuadas por medio de servicios de transmisión libre u OTT (como las aplicaciones móviles).

En el Derecho del CdE, la obligación de confidencialidad está implícita en el concepto de seguridad de los datos en el artículo 7, apartado 1 del Convenio 108 modernizado, que trata sobre la seguridad de los datos.

Para los encargados del tratamiento, la confidencialidad significa que no pueden revelar los datos a terceros ni a otros destinatarios sin autorización. En el caso de los empleados de un responsable o encargado del tratamiento, la confidencialidad exige que utilicen los datos personales únicamente conforme a las instrucciones de sus superiores competentes.

La obligación de confidencialidad deberá estar incluida en cualquier contrato que se celebre entre los responsables y sus encargados. Además, los responsables y los encargados deberán adoptar medidas específicas para imponer un deber legal de confidencialidad a sus empleados, normalmente incluyendo cláusulas de confidencialidad en el contrato de trabajo del empleado.

La infracción del deber profesional de confidencialidad es sancionable conforme al Derecho penal de muchos Estados miembros de la UE y Partes del Convenio 108.

4.2.3. Notificaciones de violaciones de los datos personales

Se entiende por violación de datos personales toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales tratados o la comunicación o acceso no autorizados a dichos datos ([452]). Pese

([451]) Ibíd., artículo 15, apartado 1.

([452]) Reglamento general de protección de datos, artículo 4, apartado 12; véase además Grupo de Trabajo del Artículo 29 (2017), *Directrices sobre la notificación de violaciones de datos personales conforme al Reglamento 2016/679*, WP250, 3 de octubre de 2017, p. 8.

a que las nuevas tecnologías, como el cifrado, ofrecen actualmente más posibilidades para garantizar la seguridad del tratamiento, las violaciones de los datos siguen siendo un problema habitual. Las causas de las violaciones de los datos pueden ir desde errores accidentales cometidos por personas que trabajan en una organización hasta amenazas externas, como piratas informáticos y organizaciones de ciberdelincuentes.

Las violaciones de datos pueden ser muy perjudiciales para la privacidad y los derechos de protección de datos de las personas físicas que, a causa de la violación, pierden el control de sus datos personales. Las violaciones pueden dar lugar a robos de identidad o fraudes, pérdidas financieras o daños materiales, pérdida de confidencialidad de datos personales protegidos por el secreto profesional y daños para la reputación del interesado. En sus Directrices sobre la notificación de violaciones de datos personales conforme al Reglamento 2016/679, el Grupo de Trabajo del Artículo 29 explica que las violaciones pueden afectar a los datos personales de tres maneras: comunicación, pérdida o alteración ([453]). Además de la obligación de adoptar medidas para garantizar la seguridad del tratamiento, como se explica en la sección 4.2, es igualmente importante asegurarse de que, cuando se produzcan violaciones, los responsables del tratamiento las manejen de manera apropiada y oportuna.

Las autoridades de control y las personas físicas a menudo no son conocedoras de que se ha producido una violación de datos y esto impide que las personas físicas actúen para protegerse de sus consecuencias negativas. Para afirmar los derechos de las personas físicas y limitar el impacto de las violaciones de datos, **la UE y el CdE** imponen a los responsables del tratamiento un requisito de notificación en determinadas circunstancias.

De acuerdo con el Convenio 108 modernizado del **CdE**, las Partes Contratantes deben exigir a los responsables del tratamiento, como mínimo, que notifiquen a la autoridad de control competente aquellas violaciones de datos que puedan suponer una grave injerencia en los derechos de los interesados. Esta notificación debe llevarse a cabo «sin dilación» ([454]).

([453]) Grupo de Trabajo del Artículo 29 (2017), *Directrices sobre la notificación de violaciones de datos personales conforme al Reglamento 2016/679*, WP250, 3 de octubre de 2017, p. 6.

([454]) Convenio 108 modernizado, artículo 7, apartado 2; Informe explicativo del Convenio 108 modernizado, párrafos 64-66.

El Derecho de la UE establece un régimen detallado que regula el momento y el contenido de las notificaciones ([455]). En consecuencia, los responsables del tratamiento deben notificar determinadas violaciones de datos a las autoridades de control sin dilaciones indebidas y, cuando sea viable, en un plazo de 72 horas desde el momento en que sean conocedores de la violación. Si sobrepasan el plazo de 72 horas, la notificación deberá ir acompañada de una indicación de los motivos de la dilación. Los responsables del tratamiento solo estarán exentos del requisito de notificación cuando puedan demostrar que no es probable que la violación de la seguridad de los datos ocasione un riesgo para los derechos y libertades de las personas afectadas.

El Reglamento especifica la información mínima que debe incluirse en la notificación para que la autoridad de control pueda actuar según sea necesario ([456]). La notificación debe incluir, como mínimo, una descripción de la naturaleza de la violación de los datos y de las categorías y el número aproximado de interesados afectados, una descripción de las posibles consecuencias de dicha violación y de las medidas adoptadas por el responsable del tratamiento para abordar y mitigar las citadas consecuencias. Además, deben facilitarse el nombre y los datos de contacto del delegado de protección de datos u otro punto de contacto, para que la autoridad de control competente pueda obtener más información si es preciso.

Si es probable que una violación de datos conlleve un alto riesgo para los derechos y libertades de las personas físicas, los responsables del tratamiento deberán comunicar la violación a estas personas (los interesados) sin dilaciones indebidas ([457]). La información proporcionada a los interesados, incluida la descripción de la violación de los datos, debe redactarse en lenguaje claro y sencillo, e incluir información similar a la requerida en el caso de las notificaciones a las autoridades de control. En determinadas circunstancias, los responsables del tratamiento pueden quedar exentos de la obligación de notificar dichas violaciones a los interesados. Las exenciones serán de aplicación cuando el responsable del tratamiento haya aplicado medidas técnicas y organizativas de protección adecuadas y cuando dichas medidas hayan sido aplicadas a los datos personales afectados por la violación, en particular aquellas que hacen que los datos personales sean ininteligibles para cualquier persona no autorizada a obtener acceso a los mismos, como el cifrado. La actuación del responsable del tratamiento tras la violación para velar por que no se materialice el

([455]) Reglamento general de protección de datos, artículos 33 y 34.

([456]) Ibíd., art. 33 apartado 3.

([457]) Ibíd., artículo 34.

perjuicio para los derechos de los interesados también puede eximir al responsable de la obligación de notificar a estos últimos. Por último, si la notificación requiere un esfuerzo desproporcionado por parte del responsable del tratamiento, se podrá comunicar la violación a los interesados por otros medios, como una comunicación pública o medidas similares ([458]).

La obligación de notificar las violaciones de datos a las autoridades de control y a los interesados se impone a los responsables del tratamiento. No obstante, las violaciones de datos pueden producirse con independencia de si el tratamiento es efectuado por un responsable o por un encargado. Por este motivo, es esencial garantizar que los encargados también estén obligados a notificar las violaciones de datos. En este caso, los encargados deberán notificar las violaciones al responsable sin dilaciones indebidas ([459]). El responsable del tratamiento será entonces el responsable de notificar a las autoridades de control y a los interesados afectados, con arreglo a las normas y plazos antes mencionados.

4.3. Normas sobre responsabilidad proactiva y promoción del cumplimiento

Puntos clave

- Para garantizar la responsabilidad proactiva en el tratamiento de datos personales, los responsables y encargados del tratamiento deben llevar registros de las actividades de tratamiento realizadas bajo su responsabilidad y entregarlos a las autoridades de control cuando se les solicite.
- El Reglamento general de protección de datos establece varios instrumentos para promover el cumplimiento:
  - el nombramiento de delegados de protección de datos en determinadas situaciones;
  - la realización de una evaluación de impacto antes de comenzar actividades de tratamiento que puedan generar riesgos elevados para los derechos y libertades de las personas físicas;

([458]) Ibíd., artículo 34, apartado 3, letra c).

([459]) Ibíd., artículo 33, apartado 2.

  - consulta previa con la autoridad de control competente si la evaluación de impacto indica que el tratamiento presenta riesgos que no se pueden paliar;
  - códigos de conducta para responsables y encargados del tratamiento que especifiquen la aplicación del Reglamento en varios sectores de tratamiento;
  - mecanismos de certificación, sellos y marcas.
- El Derecho del CdE propone instrumentos similares para promover el cumplimiento en el Convenio 108 modernizado.

El principio de responsabilidad proactiva es especialmente importante para garantizar la aplicación de las normas de protección de datos en Europa. El responsable del tratamiento es el responsable del cumplimiento de las normas de protección de datos y debe demostrarlo. Los responsables del tratamiento no solo deben rendir cuentas cuando se ha producido una violación, sino que tienen una obligación proactiva de aplicar políticas adecuadas de gestión de datos en todas las fases del tratamiento. La legislación europea en materia de protección de datos obliga a los responsables del tratamiento a aplicar medidas técnicas y organizativas que garanticen y permitan demostrar que el tratamiento se lleva a cabo de conformidad con la ley. Entre estas medidas está la designación de delegados de protección de datos, llevar registros y documentación en relación con el tratamiento y realizar evaluaciones de impacto sobre la privacidad.

4.3.1. Delegados de protección de datos

Los delegados de protección de datos (DPD) son personas que asesoran a las organizaciones que llevan a cabo el tratamiento de datos personales acerca del cumplimiento de las normas de protección de datos. Son la «piedra angular de la responsabilidad proactiva», ya que facilitan el cumplimiento, al tiempo que actúan como intermediarios entre las autoridades de control, los interesados y la organización por la que han sido nombrados.

En el Derecho del CdE, el artículo 10, apartado 1, del Convenio 108 modernizado impone una responsabilidad general de rendición de cuentas a los responsables y encargados del tratamiento. Esto obliga a los responsables y encargados del tratamiento a adoptar todas las medidas adecuadas para cumplir las normas de protección de datos estipuladas en el Convenio y para poder demostrar que el tratamiento de datos bajo su control se ajusta a las disposiciones del Convenio. Aunque el Convenio no especifica las medidas concretas que deben adoptar los responsables y encargados, el Informe explicativo del Convenio 108 modernizado indica que la

designación de un DPD sería una de las posibles medidas para demostrar el cumplimiento. A los DPD se les deben facilitar todos los medios necesarios para cumplir sus mandatos ([460]).

Al contrario que en el Derecho del CdE, **en la UE**, el nombramiento de un DPD no siempre se deja a criterio de los responsables y encargados del tratamiento, sino que es obligatorio en determinadas circunstancias. El RGPD reconoce que el DPD desempeña un papel clave en el nuevo sistema de gobernanza e incluye disposiciones detalladas en relación con su designación, posición, obligaciones y funciones ([461]).

El RGPD obliga a designar un DPD en tres casos concretos: cuando el tratamiento lo lleve a cabo una autoridad u organismo público, cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala, o cuando las actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales relativos a condenas e infracciones penales ([462]). Pese a que el Reglamento no define términos como «observación sistemática a gran escala» o «actividades principales», el Grupo de Trabajo del Artículo 29 ha publicado directrices sobre cómo deben interpretarse estos términos ([463]).

Ejemplo: Las empresas propietarias de redes sociales y motores de búsqueda pueden considerarse responsables cuyas operaciones de tratamiento requieren la observación habitual y sistemática de interesados a gran escala. El modelo de negocio de este tipo de empresas está basado en el tratamiento de ingentes cantidades de datos personales y generan importantes ingresos ofreciendo servicios de publicidad selectiva y permitiendo que las empresas se publiciten en sus sitios. La publicidad selectiva es una manera de colocar anuncios basados en datos demográficos y en el historial o comportamiento de compra de los consumidores. Por tanto, requiere la observación sistemática de hábitos y comportamientos de los interesados.

([460]) Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 87.

([461]) Reglamento general de protección de datos, artículos 37-39.

([462]) Ibíd., artículo. 37 apartado 1.

([463]) Grupo de Trabajo del Artículo 29 (2017), *Directrices sobre los delegados de protección de datos («DPD»)*, WP 243, rev.01, revisadas por última vez y adoptadas el 5 de abril de 2017.

Ejemplo: Un hospital y una compañía de seguros de enfermedad son ejemplos típicos de responsables cuyas actividades consisten en el tratamiento de categorías especiales de datos personales a gran escala. Los datos que revelan información relativa a la salud de una persona física constituyen categorías especiales de datos personales tanto en virtud del Derecho del CdE como del Derecho de la UE, por lo que merece una protección reforzada. El Derecho de la UE reconoce además que los datos genéticos y biométricos constituyen categorías especiales. En la medida en que los centros médicos y las compañías de seguros traten este tipo de datos a gran escala, deben designar un delegado de protección de datos conforme al RGPD.

Además, el artículo 37, apartado 4, del RGPD establece que en casos distintos de los tres obligatorios en virtud del artículo 37, apartado 1, el responsable, el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros.

El resto de organismos no están obligados legalmente a designar un DPD. Sin embargo, el RGPD establece que los responsables y encargados del tratamiento pueden optar voluntariamente por designar un DPD, al tiempo que contempla la posibilidad de que los Estados miembros exijan que dicha designación sea obligatoria para otros tipos de organismos además de los previstos en el Reglamento ([464]).

Una vez que un responsable del tratamiento designa un DPD, debe asegurarse de que «participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales» de la organización ([465]). A modo de ejemplo, los DPD deberán prestar asesoramiento sobre la realización de evaluaciones de impacto de la protección de datos, así como en la creación y el mantenimiento de registros de las actividades de tratamiento que se lleven a cabo en el seno de una organización. Para que los DPD puedan desempeñar sus funciones con eficacia, los responsables y encargados del tratamiento deberán facilitarles los recursos necesarios, incluidos recursos financieros, infraestructuras y equipos. También es obligatorio dar al DPD tiempo suficiente para desempeñar sus funciones y proporcionarle formación continua que le permita incrementar sus conocimientos

([464]) Reglamento general de protección de datos, artículo 37, apartados 3 y 4.

([465]) Ibíd., artículo. 38 apartado 1.

y mantenerse al día de los cambios que se produzcan en la normativa de protección de datos ([466]).

El RGPD establece ciertas garantías básicas para que el DPD actúe con independencia. Los responsables y encargados del tratamiento deben garantizar que el DPD no reciba ninguna instrucción de la empresa en lo que respecta al desempeño de sus funciones relacionadas con la protección de datos, ni siquiera de las personas de más alto nivel directivo. Además, no debe ser despedido ni sancionado en modo alguno por desempeñar sus funciones ([467]). Por ejemplo, supongamos que el DPD aconseja al responsable o encargado del tratamiento que realice una evaluación de impacto de la protección de datos porque considera que el tratamiento puede entrañar un riesgo elevado para los interesados. La empresa está en desacuerdo con el consejo del DPD, considera que carece de fundamento y, en consecuencia, decide no realizar la evaluación de impacto. La empresa puede hacer caso omiso al asesoramiento recibido, pero no puede despedir ni sancionar al DPD por prestárselo.

Por último, las funciones y responsabilidades del DPD están detalladas en el artículo 39 del RGPD; tales funciones y responsabilidades consisten en informar y asesorar a las empresas y a los empleados que participen en el tratamiento acerca de sus obligaciones conforme a la legislación y supervisar el cumplimiento de lo dispuesto en la normativa de protección de datos de la UE, realizando auditorías y formando al personal que participe en las operaciones de tratamiento. El DPD también debe cooperar con la autoridad de control y actuar como punto de contacto de esta última en cuestiones relacionadas con el tratamiento, como por ejemplo una violación de la seguridad de los datos personales.

En relación con los datos personales manejados por instituciones y organismos de la UE, el Reglamento 45/2001 establece que cada institución y organismo de la UE debe designar un DPD. El DPD tiene la misión de velar por que las disposiciones del Reglamento se apliquen correctamente en las instituciones y organismos de la UE y que tanto los interesados como los responsables del tratamiento sean informados de sus derechos y obligaciones ([468]). También tiene la responsabilidad de responder a las peticiones del SEPD y de colaborar con él cuando sea necesario. Al igual que el RGPD, el Reglamento 45/2001 contiene disposiciones relativas a la independencia

([466]) Grupo de Trabajo del Artículo 29 (2017), *Directrices sobre los delegados de protección de datos («DPD»)*, WP 243, rev.01, última versión revisada y adoptada el 5 de abril de 2017, apartado 3.1.

([467]) Reglamento general de protección de datos, artículo 38, apartados 2 y 3.

([468]) Véase la lista completa de funciones del DPD en el artículo 24, apartado 1 del Reglamento (CE) 45/2001.

del DPD en el desempeño de sus funciones y la necesidad de proporcionarle el personal y los recursos necesarios ([469]). Los DPD deben ser notificados antes de que una institución u organismo de la UE (o cualquier departamento de estas organizaciones) realice alguna operación de tratamiento y deben llevar un registro de todas las operaciones de tratamiento notificadas ([470]).

4.3.2. Registros de las actividades de tratamiento

Para poder demostrar el cumplimiento y rendir cuentas, las empresas tienen normalmente la obligación legal de documentar y registrar sus actividades. Un ejemplo importante son las leyes y auditorías fiscales, que obligan a todas las empresas a registrar y documentar información ampliamente. También es importante establecer requisitos similares en otros ámbitos de la ley, especialmente la normativa de protección de datos, ya que los registros son importantes para facilitar el cumplimiento de dicha normativa. De este modo, el **Derecho de la UE** establece que los responsables del tratamiento o sus representantes deben llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad ([471]). Esta obligación tiene por objeto garantizar que, en caso de necesidad, las autoridades de control dispongan de la documentación necesaria para poder confirmar la licitud del tratamiento.

La información a documentar incluye lo siguiente:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable y del DPD;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales objeto de tratamiento;
- información sobre las categorías de destinatarios a quienes se comunicaron o se comunicarán los datos personales;

([469]) Reglamento (CE) n.º 45/2001, artículo 24, apartados 6 y 7.

([470]) Ibíd., artículos 25 y 26.

([471]) Reglamento general de protección de datos, artículo 30.

- información sobre si se han realizado o se realizarán transferencias de datos personales a terceros países u organizaciones internacionales;

- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos personales, así como una descripción general de las medidas técnicas adoptadas para garantizar la seguridad del tratamiento ([472]).

La obligación de llevar un registro de las actividades de tratamiento conforme al RGPD no solo se aplica a los responsables del tratamiento, sino también a los encargados. Este es un avance importante, ya que, antes de adoptarse el Reglamento, el contrato celebrado entre el responsable y el encargado comprendía fundamentalmente las obligaciones del encargado. Su obligación de llevar registros no está directamente prevista por la ley.

El RGPD recoge una excepción a esta obligación. El requisito de llevar registros no se aplica a las empresas u organizaciones (responsables o encargadas) con menos de 250 empleados. No obstante, dicha excepción está sujeta a los requisitos de que la organización de que se trate no efectúe actividades de tratamiento que puedan entrañar un riesgo para los derechos y libertades de los interesados, que el tratamiento sea ocasional y que no incluya categorías especiales de datos conforme al artículo 9, apartado 1 o datos personales relativos a condenas e infracciones penales conforme al artículo 10.

Llevar un registro de las actividades de tratamiento debe permitir a responsables y encargados demostrar el cumplimiento del Reglamento. También debe permitir a las autoridades de control supervisar la licitud del tratamiento. Cuando una autoridad de control solicite acceso a dichos registros, los responsables y los encargados están obligados a cooperar y ponerlos a su disposición.

4.3.3. Evaluación de impacto de la protección de datos y consulta previa

Las operaciones de tratamiento conllevan algunos riesgos intrínsecos para los derechos de las personas físicas. Los datos personales se pueden perder, comunicar a partes no autorizadas o tratar de manera ilícita. Naturalmente, los riesgos varían según la naturaleza y el ámbito de aplicación del tratamiento. Las operaciones

([472]) Ibíd., artículo. 30 apartado 1.

a gran escala que conllevan el tratamiento de datos sensibles, por ejemplo, entrañan un riesgo mucho más elevado para los interesados que cuando una pequeña empresa trata las direcciones y los números de teléfono personales de sus empleados.

Con la aparición de nuevas tecnologías y la creciente complejidad de las actividades de tratamiento, los responsables deben hacer frente a estos riesgos examinando el impacto que puede tener la operación de tratamiento prevista antes de ponerla en marcha. De este modo, las organizaciones pueden identificar, gestionar y mitigar adecuadamente los riesgos de antemano, limitando notablemente la posibilidad de que el tratamiento tenga efectos negativos para los interesados.

Las evaluaciones de impacto de la protección de datos están previstas **tanto en el Derecho del CdE como en el Derecho de la UE**. En el marco jurídico del CdE, el párrafo segundo del artículo 10 del Convenio 108 modernizado obliga a las Partes Contratantes a asegurarse de que los responsables y los encargados «examinen el impacto que puede tener el tratamiento de datos previsto sobre los derechos y libertades fundamentales de los interesados antes de iniciar dicho tratamiento» y, después de la evaluación, diseñar el tratamiento de manera que se prevengan o se minimicen los riesgos vinculados a este.

El Derecho de la UE impone una obligación similar, pero más detallada, a los responsables comprendidos en el ámbito de aplicación del RGPD. El artículo 35 establece que deberá llevarse a cabo una evaluación de impacto cuando el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas. El Reglamento no define cómo ha de valorarse la probabilidad del riesgo, pero indica cuáles podrían ser esos riesgos ([473]). Contiene una lista de operaciones de tratamiento consideradas de alto riesgo y para las cuales es particularmente necesario realizar una evaluación de impacto anterior, concretamente cuando:

- el tratamiento de datos personales tenga por objeto tomar decisiones relativas a personas físicas, después de una evaluación sistemática y exhaustiva de aspectos personales de dichas personas físicas (elaboración de perfiles);

- se realice un tratamiento a gran escala de datos sensibles o datos personales relativos a condenas e infracciones penales;

([473]) Reglamento general de protección de datos, considerando 75.

- el tratamiento implique la observación sistemática a gran escala de una zona de acceso público.

Las autoridades de control deberán adoptar y publicar una lista de los tipos de operaciones de tratamiento que deben someterse a evaluaciones de impacto. También podrán elaborar una lista de operaciones de tratamiento exentas de esta obligación ([474]).

Cuando se requiera una evaluación de impacto, los responsables deberán evaluar la necesidad y proporcionalidad del tratamiento y los posibles riesgos para los derechos de las personas físicas. La evaluación de impacto también debe contener las medidas de seguridad previstas para hacer frente a los riesgos identificados. Para elaborar las listas, las autoridades de control de los Estados miembros deben cooperar entre sí y con el Consejo Europeo de Protección de Datos. De este modo se garantiza un enfoque coherente en todo el territorio de la UE para las operaciones que requieran una evaluación de impacto y los responsables del tratamiento deberán cumplir requisitos similares sea cual sea su localización.

Si de la evaluación de impacto se infiere que el tratamiento entraña un riesgo elevado para los derechos de las personas físicas y no se han adoptado medidas para mitigar el riesgo, el responsable del tratamiento deberá consultar con la autoridad de control competente antes de iniciar la operación de tratamiento ([475]).

El Grupo de Trabajo del Artículo 29 ha publicado directrices sobre las evaluaciones de impacto de la protección de datos y para determinar si el tratamiento entraña o no un alto riesgo ([476]). Ha elaborado nueve criterios para facilitar la determinación de si es necesaria una evaluación de impacto de la protección de datos en un caso concreto: ([477]) 1) evaluación o puntuación; 2) toma de decisiones automatizada con efecto jurídico significativo o similar; 3) observación sistemática; 4) datos sensibles; 5) tratamiento de datos a gran escala; 6) asociación o combinación de conjuntos de datos; 7) datos relativos a interesados vulnerables; 8) uso innovador o aplicación

([474]) Ibíd., artículo 35, apartados 4 y 5.

([475]) Ibíd., artículo 36, apartado 1; Grupo de Trabajo del Artículo 29 (2017), Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, WP 248 rev.01, Bruselas, 4 de octubre de 2017.

([476]) Grupo de Trabajo del Artículo 29 (2017), Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, WP 248 rev.01, Bruselas, 4 de octubre de 2017.

([477]) Ibíd., pp. 9-11.

de nuevas soluciones tecnológicas u organizativas; 9) cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio y ejecutar un contrato». El Grupo de Trabajo del Artículo 29 introdujo la norma empírica de que las operaciones de tratamiento que cumplen menos de dos de estos criterios entrañan riesgos de bajo nivel y no requieren una evaluación de la protección de datos, mientras los que cumplen dos o más criterios sí requieren dicha evaluación. En los casos en que no esté claro si se requiere una evaluación de impacto de la protección de datos, el Grupo de Trabajo del Artículo 29 recomienda realizar dicha evaluación porque «representa un instrumento práctico para ayudar a los responsables del tratamiento a cumplir la legislación de protección de datos» ([478]). Cuando se introduzca una nueva tecnología de tratamiento de datos, es importante que se lleve a cabo una evaluación de impacto de la protección de datos ([479]).

4.3.4. Códigos de conducta

Los códigos de conducta tienen por objeto describir y especificar la aplicación del RGPD en distintos sectores industriales. Para los responsables y encargados del tratamiento, la creación de estos códigos puede mejorar en gran medida el cumplimiento y reforzar la aplicación de las normas de protección de datos de la UE. Los conocimientos especializados de los miembros del sector favorecerán que se encuentren soluciones que resulten prácticas y, por tanto, probablemente se apliquen. Reconociendo la importancia de estos códigos para la aplicación efectiva de la normativa de protección de datos, el RGPD insta a los Estados miembros, a las autoridades de control, a la Comisión y al Supervisor Europeo de Protección de Datos a fomentar la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del Reglamento en todo el territorio de la Unión ([480]). Estos códigos podrían especificar la aplicación del Reglamento en sectores concretos, en aspectos tales como la recopilación de datos personales, la información que se ha de facilitar a los interesados y al público y el ejercicio de los derechos de los interesados.

A fin de garantizar que los códigos de conducta se atengan a lo dispuesto en el RGPD, deben ser presentados a la autoridad de control competente antes de ser adoptados. La autoridad de control dictaminará si el proyecto de código favorece el cumplimiento del Reglamento y, si determina que el código contiene garantías

([478]) Ibíd., p. 9.

([479]) Ibíd.

([480]) Reglamento general de protección de datos, artículo 40, apartado 1.

adecuadas, lo aprobará ([481]). Las autoridades de control deben publicar los códigos de conducta aprobados y los criterios en los que se ha basado su aprobación. Cuando un proyecto de código de conducta guarde relación con actividades de tratamiento en varios Estados miembros, la autoridad de control competente, antes de aprobar el proyecto de código o su modificación o ampliación, lo presentará al Consejo Europeo de Protección de Datos, que dictaminará si el código cumple con el RGPD. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta aprobado que se le ha presentado tiene validez general en el seno de la Unión.

La adhesión a un código de conducta ofrece importantes ventajas tanto para los interesados como para los responsables y encargados del tratamiento. Estos códigos ofrecen directrices detalladas que adaptan los requisitos legales a sectores concretos y favorecen la transparencia de las actividades de tratamiento. Los responsables y encargados del tratamiento también pueden utilizar la adhesión a estos códigos como prueba palpable de que cumplen la normativa de la UE y como forma de reforzar su imagen pública en tanto que organizaciones que priorizan y se comprometen con la protección de datos en sus operaciones. Los códigos de conducta aprobados, junto con compromisos vinculantes y exigibles, pueden utilizarse como garantías adecuadas para la transferencia de datos a terceros países. Para garantizar que las organizaciones adheridas a los códigos de conducta de hecho los cumplan, se podrá designar un organismo especial (acreditado por la autoridad de control competente) que vigile y garantice dicho cumplimiento. Para desempeñar sus funciones con eficacia, el organismo debe ser independiente, tener pericia probada en relación con el objeto del código y haber establecido procedimientos y estructuras transparentes que le permitan atender reclamaciones relativas a infracciones del código ([482]).

En el **Derecho del CdE**, el Convenio 108 modernizado establece que el nivel de protección de datos garantizado por la legislación nacional se puede reforzar de manera útil con medidas de regulación voluntarias, cómo códigos de buenas prácticas o códigos de conducta profesional. Sin embargo, se trata únicamente de medidas voluntarias conforme al Convenio 108 modernizado: no se puede derivar ninguna obligación legal de la aplicación de este tipo de medidas, aunque es aconsejable, y las medidas no son de por sí suficientes para garantizar el pleno cumplimiento del Convenio ([483]).

([481]) Ibíd., art. 40 apartado 5.

([482]) Ibíd., artículo 41, apartados 1 y 2.

([483]) Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 33.

4.3.5. Certificación

Además de los códigos de conducta, otro medio que pueden utilizar responsables y encargados del tratamiento para demostrar el cumplimiento del RGPD son los mecanismos de certificación y sellos y marcas de protección de datos. Con este fin, el Reglamento establece un sistema de certificación voluntario, por el que determinados organismos o autoridades de control pueden expedir certificaciones. Los responsables y encargados del tratamiento que opten por adherirse a un mecanismo de certificación pueden ganar visibilidad y credibilidad, ya que las certificaciones, los sellos y las marcas permiten a los interesados valorar rápidamente el nivel de protección del tratamiento de datos que existe en una organización. Cabe destacar que el hecho de que el responsable o encargado del tratamiento posea una certificación de este tipo no reduce sus obligaciones y responsabilidades de cumplimiento de todos los requisitos del Reglamento.

4.4. Protección de los datos desde el diseño y por defecto

Protección de datos desde el diseño

El **Derecho de la UE** requiere que los responsables del tratamiento adopten medidas para aplicar de manera efectiva los principios de protección de datos e integrar las garantías necesarias para cumplir los requisitos del Reglamento y proteger los derechos de los interesados ([484]). Estas medidas deben aplicarse tanto en el momento del tratamiento como al determinar los medios utilizados para llevarlo a cabo. En la aplicación de estas medidas, el responsable del tratamiento debe tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, ámbito y fines del tratamiento de los datos personales y los riesgos y su gravedad para los derechos y libertades del interesado ([485]).

El **Derecho del CdE** exige que los responsables y encargados del tratamiento evalúen los efectos que puede tener el tratamiento de datos personales para los derechos y libertades de los interesados antes de iniciar el tratamiento. Además, los

([484]) Reglamento general de protección de datos, artículo 25, apartado 1.

([485]) Grupo de Trabajo del Artículo 29 (2017), *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679*, WP 248 rev.01, 4 de octubre de 2017. Véase también ENISA (2015), Privacidad y protección de datos desde el diseño: de la política a la ingeniería, 12 de enero de 2015.

responsables y encargado del tratamiento están obligados a diseñar el tratamiento de manera que se evite o se minimice el riesgo de injerencia en dichos derechos y libertades así como que se adopten medidas técnicas y organizativas que tenga en cuenta las implicaciones del derecho de protección de datos en todas las fases del tratamiento de los datos personales ([486]).

Protección de datos por defecto

El **Derecho de la UE** exige que el responsable del tratamiento aplique medidas adecuadas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para los fines perseguidos. Esta obligación se aplica a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad ([487]). Estas medidas deben garantizar, por ejemplo, que no todos los empleados del responsable del tratamiento tengan acceso a los datos personales de los interesados. El SEPD estableció directrices adicionales en sus *Herramientas para determinar la necesidad* ([488]).

El **Derecho del CdE** exige que los responsables y encargados del tratamiento apliquen medidas técnicas y organizativas para considerar las implicaciones del derecho a la protección de los datos así como que se adopten medidas técnicas y organizativas que tenga en cuenta las implicaciones del derecho de protección de datos en todas las fases del tratamiento de los datos personales ([489]).

En 2016, ENISA publicó un informe sobre las herramientas y servicios de privacidad disponibles ([490]). Entre otras consideraciones, esta evaluación proporciona un índice de criterios y parámetros que constituyen indicadores de buenas o malas prácticas de privacidad. Mientras algunos criterios guardan relación directa con las disposiciones del RGPD —como el uso de la seudonimización o de mecanismos de certificación aprobados—, otros representan iniciativas innovadoras para garantizar la privacidad desde el diseño y por defecto. Por ejemplo, el criterio de usabilidad, aunque

([486]) Convenio 108 modernizado, artículo 10, apartado 2. Informe explicativo del Convenio 108 modernizado, párrafo 89.

([487]) Reglamento general de protección de datos, artículo 25, apartado 2.

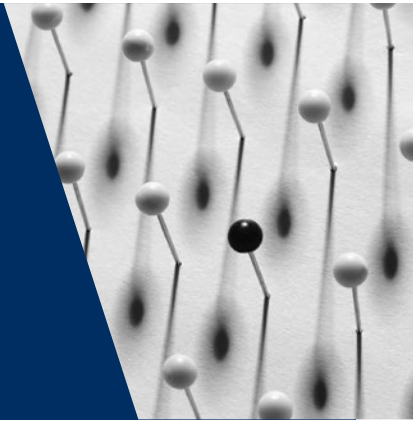
([488]) Supervisor Europeo de Protección de Datos (SEPD) (2017), *Herramientas para determinar la necesidad*, Bruselas, 11 de abril de 2017.

([489]) Convenio 108 modernizado, artículo 10, apartado 3. Informe explicativo del Convenio 108 modernizado, párrafo 89.

([490]) ENISA, Matriz de controles de PET: enfoque sistemático para evaluar herramientas de privacidad en línea y móviles, 20 de diciembre de 2016.

no guarda relación directa con la privacidad, puede reforzar esta, ya que puede facilitar una adopción más extensa de una herramienta o servicio de privacidad. De hecho, las herramientas de privacidad que son difíciles de aplicar en la práctica pueden tener niveles de adopción muy bajos por parte del público en general, aunque ofrezcan garantías de privacidad muy firmes. Además, el criterio de madurez y estabilidad de la herramienta de privacidad —es decir, la forma en que una herramienta evoluciona a lo largo del tiempo y responde a retos nuevos o actuales al respecto de la privacidad— tiene importancia crucial. Otras tecnologías de protección de la privacidad, por ejemplo, en el contexto de la seguridad de las comunicaciones, son el cifrado punto a punto (comunicación por la cual las únicas personas que pueden leer los mensajes son las personas que se están comunicando), el cifrado cliente-servidor (cifrar el canal de comunicación establecido entre un cliente y un servidor), la autenticación (verificación de la identidad de las partes que se comunican) y la comunicación anónima (ningún tercero puede identificar a las partes que se comunican).

5 Control independiente



UE	Materias tratadas	CdE
La Carta, artículo 8, apartado 3 Tratado de Funcionamiento de la Unión Europea, artículo 16, apartado 2 Reglamento general de protección de datos, artículos 51-59 TJUE, C-518/07, *Comisión Europea contra República Federal de Alemania* [GS], 2010 TJUE, C-614/10, *Comisión Europea contra República de Austria* [GS], 2012 TJUE, C-288/12, *Comisión Europea contra Hungría* [GS], 2014 TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 2015	**Autoridades de control**	Convenio 108 modernizado, artículo 15
Reglamento general de protección de datos, artículos 60-67	**Cooperación entre autoridades de control**	Convenio 108 modernizado, artículos 16-21
Reglamento general de protección de datos, artículos 68-76	**Consejo Europeo de Protección de Datos**	

Puntos clave

- El control independiente es un componente esencial de la normativa europea sobre protección de datos y está consagrado en el artículo 8, apartado 3 de la Carta.
- Para garantizar una protección de datos efectiva, el Derecho nacional deberá establecer autoridades de control independientes.
- Las autoridades de control deberán actuar con total independencia, que deberá quedar garantizada en una ley fundamental y reflejada en una estructura organizativa específica de la autoridad de control.
- Las autoridades de control tienen competencias y funciones específicas, entre las que se incluyen las siguientes:
  - vigilar y promover la protección de datos a escala nacional;
  - asesorar a los interesados y a los responsables del tratamiento, así como a los gobiernos y al público en general;
  - oír las reclamaciones y prestar ayuda a los interesados en los casos de supuestas violaciones de los derechos de protección de datos;
  - supervisar a los responsables y a los encargados del tratamiento.
- Las autoridades de control también tienen la facultad de intervenir si es necesario:
  - avisando, amonestando o incluso multando a los responsables y a los encargados del tratamiento;
  - ordenando que se rectifiquen, se bloqueen o se supriman datos;
  - imponiendo una prohibición sobre el tratamiento o una multa administrativa;
  - sometiendo los asuntos a los órganos jurisdiccionales.
- Dado que en el tratamiento de los datos personales suelen participar responsables, encargados e interesados radicados en diferentes Estados, las autoridades de control deben cooperar entre sí en cuestiones transfronterizas para garantizar la protección efectiva de las personas físicas en Europa.
- En la UE, el Reglamento general de protección de datos establece un mecanismo de ventanilla única para los casos de tratamiento transfronterizo. Algunas empresas realizan actividades de tratamiento transfronterizas porque tienen que tratar datos personales en el contexto de las actividades de establecimientos radicados en más de un Estado miembro o en el contexto de un único establecimiento en el territorio de la Unión pero que afecta sustancialmente a interesados radicados en más de un Estado miembro. De acuerdo con este mecanismo, estas empresas solo tendrán que tratar con una autoridad nacional de control de protección de datos.

- Un mecanismo de cooperación y coherencia permitirá un enfoque coordinado entre todas las autoridades de control que participen en el caso. La autoridad de control principal —del establecimiento principal o único— consultará y presentará su proyecto de decisión al resto de autoridades de control concernidas.
- Del mismo modo que el actual Grupo de Trabajo del Artículo 29, la autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos (SEPD) formarán parte del Consejo Europeo de Protección de Datos.
- El Consejo Europeo de Protección de Datos tiene la misión, por ejemplo, de vigilar la correcta aplicación del Reglamento, asesorar a la Comisión en materias pertinentes y publicar dictámenes, directrices o buenas prácticas sobre diversos temas.
- La principal diferencia es que el Consejo Europeo de Protección de Datos no solo emite dictámenes, como en virtud de la Directiva 95/46/CE. También adopta decisiones vinculantes en relación con casos en que una autoridad de control haya planteado una objeción pertinente y motivada en un caso de ventanilla única; cuando existan puntos de vista contradictorios sobre cuál de las autoridades de control es la principal; y, por último, cuando la autoridad de control competente no solicite o no se atenga al dictamen del CEPD. El objetivo es garantizar una aplicación coherente del Reglamento en todos los Estados miembros.

El control independiente es un componente esencial de la legislación europea sobre protección de datos. Tanto el Derecho de la UE como el Derecho del CdE consideran que la existencia de las autoridades de control independientes es indispensable para la protección efectiva de los derechos y libertades de las personas físicas en relación con el tratamiento de sus datos personales. Dado que el tratamiento de datos es actualmente omnipresente y cada vez más complejo para que lo entiendan las personas físicas, estas autoridades son los centinelas de la era digital. En la UE, la existencia de autoridades de control independientes se considera uno de los elementos más esenciales del derecho a la protección de los datos personales, consagrado en el Derecho primario de la Unión. El artículo 8, apartado 3 de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 2 del TFUE reconocen que la protección de los datos personales es un derecho fundamental y afirman que el cumplimiento de la normativa de protección de datos debe estar sujeto al control de una autoridad independiente.

La importancia del control independiente para la normativa de protección de datos también se ha reconocido en la jurisprudencia.

Ejemplo: En *Schrems* ([491]), el TJUE tenía que determinar si la transferencia de datos personales a los Estados Unidos en virtud del primer Acuerdo de puerto seguro entre la UE y los EE. UU. era conforme con la legislación de la UE sobre protección de datos, a la luz de las revelaciones de Edward Snowden sobre la práctica de vigilancia masiva de la Agencia Nacional de Seguridad de los EE. UU. La transferencia de datos personales a los EE. UU. se basó en una decisión adoptada por la Comisión Europea en 2000, que permitía la transferencia de datos personales desde la UE a organizaciones estadounidenses que autocertificasen su adhesión a los principios de puerto seguro, sobre la base de que estos principios garantizan un nivel adecuado de protección de los datos personales. Cuando se le solicitó que investigase la reclamación del demandante en cuanto a la legalidad de las transferencias de datos tras las revelaciones de Snowden, la autoridad de control irlandesa rechazó la reclamación alegando que la existencia de la decisión de la Comisión sobre la idoneidad del régimen de protección de datos estadounidense reflejada en los principios de puerto seguro (la «Decisión de puerto seguro») le impedía continuar investigando.

El TJUE, sin embargo, resolvió que la existencia de una decisión de la Comisión autorizando las transferencias de datos a terceros países que garanticen niveles adecuados de protección no elimina ni reduce las competencias de las autoridades de control nacionales. El TJUE señaló que las competencias de estas autoridades para vigilar y garantizar el cumplimiento de las normas de la UE sobre protección de datos derivan del Derecho primario de la Unión, en particular del artículo 8, apartado 3 de la Carta y del artículo 16, apartado 2 del TFUE. «La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales» ([492]).

Por consiguiente, el TJUE decidió que, aunque la transferencia de datos personales haya sido objeto de una decisión de idoneidad de la Comisión, cuando se presente una reclamación a una autoridad de control nacional, dicha autoridad deberá examinar la reclamación con diligencia. La autoridad de control podrá rechazar la reclamación si determina que es infundada. En ese caso, el TJUE hizo hincapié en que el derecho a un recurso judicial

([491]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015.

([492]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015, apartado 41.

efectivo requiere que las personas puedan impugnar dicha decisión ante los órganos jurisdiccionales nacionales, que pueden remitir el asunto al TJUE para solicitar un pronunciamiento prejudicial sobre la validez de la decisión de la Comisión. Cuando la autoridad de control considere que la reclamación es fundada, deberá poder iniciar un procedimiento legal para poner el asunto en conocimiento de los órganos jurisdiccionales nacionales. Los órganos jurisdiccionales nacionales podrán remitir el asunto al TJUE, ya que es el único organismo competente para resolver sobre la validez de una decisión de idoneidad de la Comisión ([493]).

El TJUE examinó a continuación la validez de la Decisión de puerto seguro para determinar si el sistema de transferencias se ajustaba a la normativa de protección de datos de la UE. Determinó que el artículo 3 de la Decisión de puerto seguro limitaba la facultad de las autoridades de control nacionales (otorgadas con arreglo a la Directiva sobre protección de datos) de actuar para impedir las transferencias de datos en el caso de que el nivel de protección de los datos personales fuera inadecuado en los Estados Unidos. En vista de la importancia que tiene que las autoridades de control independientes velen por el cumplimiento de la legislación sobre protección de datos, el TJUE resolvió que, en virtud de la Directiva sobre protección de datos e interpretada a la luz de la Carta, la Comisión no tenía la facultad de limitar de ese modo las competencias de las autoridades de control independientes. La limitación de las competencias de las autoridades de control fue una de las razones por las que el TJUE invalidó la Decisión de puerto seguro.

La legislación europea requiere la existencia de un control independiente como mecanismo importante para garantizar una protección de datos efectiva. Las autoridades de control independientes son el primer punto de contacto para los interesados en los casos de violación de la privacidad ([494]). En el Derecho del CdE y de la UE, es obligatorio crear autoridades de control. Ambos marcos jurídicos describen las competencias y funciones de dichas autoridades de manera similar a como se especifican en el RGPD. En principio, las autoridades de control deberían, por tanto, funcionar de la misma forma tanto en el Derecho de la UE como en el del CdE ([495]).

([493]) Ibíd., apartados 53-66.

([494]) Reglamento general de protección de datos, artículo 13, apartado 2, letra d).

([495]) Ibíd., artículo 51; Convenio 108 modernizado, artículo 15.

5.1. Independencia

El **Derecho de la UE** y el **Derecho del CdE** requieren que cada una de las autoridades de control actúe con total independencia en el desempeño de sus funciones y en el ejercicio de sus competencias ([496]). La independencia de la autoridad de control y de sus miembros, así como de su personal, frente a influencias externas directas o indirectas es fundamental para garantizar la objetividad plena en la toma de decisiones sobre protección de datos. La legislación que fundamenta la creación de un órgano de control no solo debe incluir disposiciones que garanticen de forma específica la independencia, sino que la estructura organizativa de la autoridad también debe demostrar independencia. En 2010, el TJUE examinó por primera vez hasta qué punto tienen que ser independientes las autoridades de control de protección de datos ([497]). Los ejemplos resaltados ilustran la definición que hace el TJUE del concepto de «total independencia».

Ejemplo: En el asunto *Comisión Europea contra República Federal de Alemania* ([498]), la Comisión había solicitado al TJUE que declarase que Alemania había adaptado de forma incorrecta el requisito de «total independencia» de las autoridades de control responsables de garantizar la protección de los datos y, por tanto, había incumplido sus obligaciones en virtud del artículo 28, apartado 1, de la Directiva sobre protección de datos. En opinión de la Comisión, el hecho de que Alemania hubiera puesto a las autoridades de control que supervisan el tratamiento de datos personales en los distintos estados federales (*Länder*) bajo vigilancia estatal para garantizar el cumplimiento de la legislación sobre protección de datos constituía una violación del requisito de independencia.

El TJUE subrayó que la expresión «con total independencia» debía interpretarse con arreglo al texto concreto de esa disposición y a los objetivos y al sistema de la legislación de la UE en materia de protección de datos ([499]). El TJUE resaltó que las autoridades de control son «las guardianas»

([496]) Reglamento general de protección de datos, artículo 52, apartado 1; Convenio 108 modernizado, artículo 15, apartado 5.

([497]) FRA (2010), *Derechos fundamentales: retos y logros en 2010, Informe anual 2010*, p. 59; FRA (2010), *Protección de datos en la Unión Europea: el papel de las autoridades nacionales de control de la protección de datos*, mayo de 2010.

([498]) TJUE, C-518/07, *Comisión Europea contra República Federal de Alemania* [GS], 9 de marzo de 2010, apartado 27.

([499]) Ibíd., apartados 17 y 29.

de los derechos aplicables al tratamiento de datos personales. Por tanto, su creación en los Estados miembros se considera «un elemento esencial de la protección de las personas frente al tratamiento de datos personales» ([500]). El TJUE concluyó que «en el ejercicio de sus funciones, las autoridades de control deben actuar con objetividad e imparcialidad y, para ello, han de estar a resguardo de toda influencia externa, incluida la ejercida directa o indirectamente» por las autoridades públicas ([501]).

El TJUE resolvió además que el significado de «total independencia» debe interpretarse a la luz de la independencia del SEPD, tal como queda definido en el Reglamento de protección de datos de las instituciones de la UE. En dicho Reglamento, el concepto de independencia requiere que el SEPD no pueda solicitar ni recibir instrucciones de nadie.

En consecuencia, el TJUE dictaminó que las autoridades de control de Alemania —a causa de la supervisión de las autoridades públicas— no eran totalmente independientes en el sentido de la legislación de la UE sobre protección de datos.

Ejemplo: En *Comisión Europea contra República de Austria* ([502]), el TJUE señaló problemas similares en relación con la independencia de determinados miembros y el personal de la autoridad austriaca de protección de datos (*Datenschutzkommission*, Comisión de Protección de Datos, DSK, por sus siglas en alemán). El TJUE concluyó que el hecho de que la Cancillería Federal facilitase personal a la autoridad de control iba en menoscabo del requisito de independencia establecido en la legislación de la UE sobre protección de datos. El TJUE también resolvió que el requisito de informar a la Cancillería permanentemente acerca de su trabajo invalidaba la total independencia de la autoridad de control.

Ejemplo: En *Comisión Europea contra Hungría* ([503]), se prohibieron prácticas nacionales similares que afectaban a la independencia del personal. El TJUE señaló que «la exigencia [...] según la cual debe garantizarse que cada

([500]) Ibíd., apartado 23.

([501]) Ibíd., apartado 25.

([502]) CJEU, C-614/10, *Comisión Europea contra República de Austria* [GS], 16 de octubre de 2012, apartados 59 y 63.

([503]) TJUE, C-288/12, *Comisión Europea contra Hungría* [GS], 8 de abril de 2014, apartados 50 y 67.

autoridad de control ejerza con total independencia las funciones que le son atribuidas, implica que el Estado miembro de que se trate está obligado a respetar la duración del mandato de tal autoridad hasta que llegue a su término inicialmente previsto». El TJUE resolvió asimismo que «Hungría ha incumplido las obligaciones que le incumben en virtud de la Directiva 95/46 [...] al poner fin antes de tiempo al mandato de la autoridad de control de la protección de datos personales».

El concepto y los criterios de «total independencia» están ahora expresamente recogidos en el RGPD, que incorpora los principios establecidos en las sentencias del TJUE descritas. De conformidad con el Reglamento, la total independencia en el desempeño de sus funciones y el ejercicio de sus competencias requiere que ([504]):

- los miembros de cada autoridad de control permanezcan ajenos a toda influencia externa, ya sea directa o indirecta, y no admitan instrucciones de nadie;
- los miembros de cada autoridad de control se abstengan de cualquier acción que sea incompatible con sus funciones, para evitar conflictos de interés;
- los Estados miembros faciliten a cada autoridad de control los recursos humanos, técnicos y financieros y las infraestructuras que necesiten para el cumplimiento efectivo de sus funciones;
- los Estados miembros garanticen que cada autoridad de control pueda elegir a su propio personal;
- el control financiero al que cada autoridad de control esté sujeto en virtud de la legislación nacional no afecte a su independencia. Las autoridades de control deben tener presupuestos anuales públicos e independientes, que les permitan funcionar debidamente.

La independencia de las autoridades de control también se considera un requisito esencial en el Derecho del CdE. El Convenio 108 modernizado exige que las autoridades de control «actúen con total independencia e imparcialidad en el desempeño de sus funciones y en el ejercicio de sus competencias», sin solicitar ni admitir instrucciones ([505]). De este modo, el Convenio reconoce que estas autoridades no pueden

([504]) Reglamento general de protección de datos, artículo 52.

([505]) Convenio 108 modernizado, artículo 15, apartado 5.

proteger efectivamente los derechos y libertades de las personas físicas en relación con el tratamiento de datos si no ejercen sus funciones con total independencia. El Informe explicativo del Convenio 108 modernizado establece una serie de elementos que contribuyen a salvaguardar esta independencia. Estos elementos incluyen la posibilidad de que las autoridades de control contraten a su propio personal y adopten decisiones sin estar sujetas a injerencias externas, así como factores relativos a la duración del ejercicio de sus funciones y las condiciones en las que pueden cesar en sus funciones ([506]).

5.2. Competencia y poderes

En el Derecho de la UE, el RGPD describe las competencias y la estructura organizativa de las autoridades de control y los mandatos de que deben ser competentes y tener poder para desempeñar las funciones que les corresponden con arreglo al Reglamento.

La autoridad de control es el principal organismo del Derecho nacional que vela por el cumplimiento de la legislación de la UE en materia de protección de datos. Las autoridades de control tienen todo un catálogo de funciones y competencias además de la vigilancia, que incluyen actividades de supervisión proactiva y preventiva. Para desempeñar estas funciones, las autoridades de control deben tener poderes de investigación, correctivos y consultivos adecuados, que se enumeran en el artículo 58 del RGPD, como por ejemplo ([507]):

- asesorar a los responsables del tratamiento y a los interesados en todas las cuestiones relativas a la protección de datos;
- autorizar cláusulas contractuales tipo, normas corporativas vinculantes o acuerdos administrativos;
- investigar las operaciones de tratamiento e intervenir en caso necesario;
- exigir la presentación de cualquier información pertinente para la supervisión de las actividades del responsable del tratamiento;

([506]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 129.

([507]) Reglamento general de protección de datos, artículo 58. Véase asimismo el Convenio 108, Protocolo Adicional, artículo 1.

- sancionar a los responsables del tratamiento con advertencias o apercibimientos y ordenar que se comuniquen a los interesados las violaciones de la seguridad de los datos personales;
- ordenar la rectificación, el bloqueo, la supresión o la destrucción de los datos;
- imponer una prohibición temporal o definitiva del tratamiento o imponer multas administrativas;
- someter los asuntos a los órganos jurisdiccionales.

Para ejercer sus funciones, la autoridad de control deberá tener acceso a todos los datos personales y a la información que resulte necesaria para su investigación, así como a todos los locales en los que un responsable del tratamiento conserve la información relevante. Según el TJUE, los poderes de la autoridad de control deben interpretarse en sentido amplio para garantizar la plena eficacia de la protección de datos para los interesados en la UE.

> Ejemplo: En *Schrems*, el TJUE tenía que determinar si la transferencia de datos personales a los Estados Unidos en virtud del primer Acuerdo de puerto seguro entre la UE y los EE. UU. era conforme con la legislación de la UE sobre protección de datos, a la luz de las revelaciones de Edward Snowden. El TJUE motivó su resolución en que las autoridades de control nacionales —en su calidad de supervisores independientes del tratamiento de datos realizado por los responsables del tratamiento— pueden impedir que se transfieran datos personales a un tercer país aunque exista una decisión de idoneidad, si existen pruebas razonables de que en dicho tercer país ya no está garantizada una protección adecuada ([508]).

Cada autoridad de control es competente para ejercer poderes de investigación y poderes de intervención en su territorio. Sin embargo, dado que las actividades de los responsables y encargados del tratamiento suelen ser transfronterizas y que el tratamiento afecta a interesados radicados en varios Estados miembros, se plantea la duda en relación con la división de competencias entre las distintas autoridades

([508]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015, apartados 26-36 y 40-41.

de control. El TJUE tuvo la oportunidad de examinar esta cuestión en el asunto *Weltimmo*.

Ejemplo: En *Weltimmo* ([509]), el TJUE tenía que examinar la competencia de las autoridades de control nacionales para resolver cuestiones que afectaban a organizaciones no radicadas en su jurisdicción. Weltimmo era una empresa con domicilio social en Eslovaquia, que gestionaba una web de operaciones inmobiliarias con fincas húngaras. Los anunciantes presentaron una reclamación a la autoridad húngara de control de la protección de datos por una infracción de la legislación húngara en la materia, y la autoridad de control multó a Weltimmo. La empresa recurrió la multa ante los órganos jurisdiccionales nacionales, que remitieron el asunto al TJUE para determinar si la Directiva europea sobre protección de datos permitía a las autoridades de control de un Estado miembro aplicar su legislación nacional sobre protección de datos a una empresa con domicilio social en otro Estado miembro.

El TJUE interpretó que el artículo 4, apartado 1, letra a) de la Directiva sobre protección de datos permitía la aplicación de la legislación sobre protección de datos de un Estado miembro distinto de aquel en que el responsable del tratamiento tenga su domicilio social «siempre que este ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento». El TJUE observó que, de acuerdo con la información de que disponía, Weltimmo ejercía una actividad efectiva y real en Hungría, ya que la empresa tenía un representante en Hungría incluido en el registro de sociedades eslovaco con un domicilio húngaro, además de una cuenta bancaria y una dirección de correo húngaras, y también desarrollaba actividades en Hungría escritas en húngaro. Esta información indicaba la existencia de un establecimiento, y sometía la actividad de Weltimmo a la legislación húngara de protección de datos y a la jurisdicción de la autoridad de control húngara. Sin embargo, el TJUE dejó en manos del órgano jurisdiccional nacional la verificación de la información y la decisión de si efectivamente Weltimmo tenía un establecimiento en Hungría.

([509]) TJUE, C-230/14, *Weltimmo s. r. o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 de octubre de 2015.

En el caso de que el órgano jurisdiccional remitente determinase que Weltimmo tenía un establecimiento en Hungría, la autoridad de control húngara estaría facultada para imponer una multa. Pero si el órgano jurisdiccional nacional resolviese lo contrario, es decir, que Weltimmo no tenía un establecimiento en Hungría, la legislación aplicable sería, en consecuencia, la del Estado miembro en que se hubiera constituido la sociedad. En este caso, puesto que los poderes de las autoridades de control deben ejercerse en cumplimiento de la soberanía territorial de otros Estados miembros, la autoridad húngara no podría imponer sanciones. No obstante, como la Directiva sobre protección de datos imponía a las autoridades de control el deber de cooperación, la autoridad húngara podía solicitar a su homóloga eslovaca que examinara el asunto, determinara si existía una infracción de la ley eslovaca e impusiera las sanciones previstas en la legislación eslovaca.

Con la adopción del RGPD, actualmente existen disposiciones detalladas en relación con la competencia de las autoridades de control en asuntos transfronterizos. El Reglamento establece un «mecanismo de ventanilla única» e incluye disposiciones que obligan a las distintas autoridades de control a cooperar entre sí. Para lograr una cooperación efectiva en los casos transfronterizos, el RGPD exige que se establezca una autoridad de control principal que actúe como autoridad de control del principal establecimiento o único establecimiento del responsable o encargado del tratamiento ([510]). La autoridad de control principal se encarga de los casos transfronterizos, es la única interlocutora del responsable o encargado del tratamiento y coordina la cooperación con otras autoridades de control para alcanzar un consenso. La cooperación comprende el intercambio de información, la asistencia mutua en materia de supervisión e investigación y la adopción de resoluciones vinculantes ([511]).

En el Derecho del CdE, las competencias y facultades de las autoridades de control están recogidas en el artículo 15 del Convenio 108 modernizado. Estas competencias se corresponden con las que se otorgan a las autoridades de control en virtud del Derecho de la UE e incluyen competencias en investigación e intervención, competencias para adoptar resoluciones e imponer sanciones administrativas por las violaciones de las disposiciones del Convenio y competencias para entablar procedimientos legales. Las autoridades de control independientes también tienen competencia para examinar las solicitudes y reclamaciones presentadas por los interesados, para sensibilizar al público sobre la normativa de protección de datos y para

([510]) Reglamento general de protección de datos, artículo 56, apartado 1.

([511]) Ibíd., artículo 60.

asesorar a los órganos de decisión nacionales en relación con cualquier medida legislativa o administrativa que contemple el tratamiento de datos personales.

5.3. Cooperación

El RGPD establece un marco general de cooperación entre autoridades de control y contiene disposiciones más específicas sobre la cooperación de las autoridades de control en actividades transfronterizas de tratamiento de datos.

Con arreglo al RGPD, las autoridades de control han de prestarse asistencia mutua y compartir información pertinente para ejecutar y aplicar el Reglamento de manera coherente ([512]). Ello incluye que la autoridad de control solicitada realice consultas, inspecciones e investigaciones. Las autoridades de control pueden realizar operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas en las que participe personal de todas las autoridades de control ([513]).

En la UE, los responsables y encargados del tratamiento operan cada vez más a nivel transnacional. Ello requiere una estrecha cooperación entre las autoridades de control competentes de los Estados miembros para garantizar que el tratamiento de datos personales cumpla las disposiciones del RGPD. De acuerdo con el mecanismo de «ventanilla única» del Reglamento, si un responsable o encargado del tratamiento cuenta con establecimientos en varios Estados miembros, o si tiene un único establecimiento, pero las operaciones de tratamiento afectan sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal (o único) es la autoridad principal para las actividades transfronterizas del responsable o encargado. Las autoridades principales están facultadas para adoptar medidas ejecutivas contra el responsable o el encargado. El mecanismo de ventanilla única tiene por objeto mejorar la armonización y la aplicación uniforme de la legislación de la UE en materia de protección de datos en los distintos Estados miembros. También es beneficioso para las empresas, ya que solo tienen que tratar con la autoridad principal y no con varias autoridades de control. De este modo se refuerza la seguridad jurídica de las empresas y, en la práctica, también debe suponer que las decisiones se adopten con mayor rapidez y que las empresas no se encuentren con distintas autoridades de control que les impongan requisitos contradictorios.

([512]) Ibíd., artículo 61, apartados 1-3 y artículo 62, apartado 1.

([513]) Ibíd., artículo. 62 apartado 1.

Para establecer cuál es la autoridad de control hay que determinar la ubicación del establecimiento principal de una empresa en la UE. El término «establecimiento principal» está definido en el RGPD. Además, el Grupo de Trabajo del Artículo 29 ha publicado directrices para identificar a la autoridad de control principal de un responsable o encargado, que incluyen los criterios para determinar cuál es el establecimiento principal ([514]).

Para garantizar un alto nivel de protección de datos en todo el territorio de la UE, la autoridad de control principal no actúa por sí sola. Debe cooperar con el resto de autoridades de control afectadas para adoptar resoluciones sobre el tratamiento de datos personales realizado por responsables y encargados, en un esfuerzo por llegar a consensos y garantizar la coherencia. La cooperación entre las autoridades de control pertinentes incluye el intercambio de información, la prestación de asistencia mutua, la realización de investigaciones conjuntas y la supervisión de actividades ([515]). Cuando se presten asistencia mutua, las autoridades de control deberán atender con exactitud las peticiones de información realizadas por otras autoridades de control y aplicar medidas de supervisión, como por ejemplo autorizaciones y consultas previas, inspecciones e investigaciones. Se deberá responder a las solicitudes de asistencia mutua de autoridades de control de otros Estados miembros sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud ([516]).

Cuando el responsable tenga establecimientos en varios Estados miembros, las autoridades de control podrán realizar operaciones conjuntas, incluidas investigaciones y medidas ejecutivas en las que participen miembros del personal de las autoridades de control de otros Estados miembros ([517]).

La cooperación entre diferentes autoridades de control es también un importante requisito en el Derecho del CdE. El Convenio 108 modernizado establece que las autoridades de control deben cooperar entre sí en la medida necesaria para desempeñar sus funciones ([518]). Una forma de hacerlo, por ejemplo, es intercambiar información útil y pertinente y coordinar las investigaciones y realizar acciones conjuntas.

([514]) Grupo de Trabajo del Artículo 29 (2016), *Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento*, WP 244, Bruselas, 13 de diciembre de 2016, versión revisada el 5 de abril de 2017.

([515]) Reglamento general de protección de datos, artículo 60, apartados 1-3.

([516]) Ibíd., artículo 61, apartados 1 y 2.

([517]) Ibíd., artículo. 62 apartado 1.

([518]) Convenio 108 modernizado, artículos 16 y 17.

5.4. El Comité Europeo de Protección de Datos

En este capítulo ya se ha explicado la importancia de unas autoridades de control independientes y las principales competencias que poseen conforme a la legislación europea de protección de datos. El Comité Europeo de Protección de Datos (CEPD) es otro agente importante para garantizar la aplicación efectiva y coherente de las normas de protección de datos en todo el territorio de la UE.

El CEPD es un organismo de la Unión creado por el RGPD, que goza de personalidad jurídica ([519]). Es el sucesor del Grupo de Trabajo del Artículo 29 ([520]), que la Directiva sobre protección de datos había creado para asesorar a la Comisión sobre cualquier medida de ámbito de la Unión que afectase a los derechos de las personas físicas en relación con el tratamiento de datos personales y la privacidad, para promover la aplicación uniforme de la Directiva y para dar su opinión experta a la Comisión sobre cuestiones relacionadas con la protección de datos. El Grupo de Trabajo del Artículo 29 estaba formado por representantes de las autoridades de control de los Estados miembros de la Unión, junto con representantes de la Comisión y el SEPD.

Como el Grupo de Trabajo, el CEPD está formado por los directores de las autoridades de control de los Estados miembros y por el SEPD, o sus representantes respectivos ([521]). El SEPD goza de igual derecho a voto, con la excepción de los casos relacionados con la resolución de conflictos, en los que solo puede votar decisiones relativas a los principios y normas aplicables a las instituciones de la UE que correspondan en cuanto al fondo a las contempladas en el RGPD. La Comisión tiene derecho a participar en las actividades y reuniones del CEPD, pero no tiene derecho a voto ([522]). Entre sus miembros, el Comité elige por mayoría simple un presidente (en quien recae su representación) y dos vicepresidentes para un mandato de cinco años. Además, el CEPB dispone de una secretaría, a cargo del SEPD, como apoyo analítico, administrativo y logístico para el Comité ([523]).

([519]) Reglamento general de protección de datos, artículo 68.

([520]) De acuerdo con la Directiva 95/46/CE, el Grupo de Trabajo del Artículo 29 tenía la misión de asesorar a la Comisión en relación con cualquier medida de la UE que afectase a los derechos de las personas físicas con respecto al tratamiento de datos personales y a la intimidad, promover la aplicación uniforme de la Directiva y dar su opinión experta a la Comisión sobre cuestiones relacionadas con la protección de datos. El Grupo de Trabajo del Artículo 29 estaba formado por representantes de las autoridades de control de los Estados miembros de la Unión, junto con la Comisión y el SEPD.

([521]) Reglamento general de protección de datos, artículo 68, apartado 3.

([522]) Ibíd., artículo 68, apartados 4 y 5.

([523]) Ibíd., artículos 73 y 75.

Las funciones del CEPD se detallan en los artículos 64, 65 y 70 del RGPD e incluyen amplios deberes que pueden englobarse en tres actividades principales:

- **Coherencia:** El CEPD puede adoptar decisiones jurídicamente vinculantes en tres casos: cuando una autoridad de control haya manifestado una objeción pertinente y motivada en un caso de ventanilla única; cuando existan puntos de vista enfrentados sobre cuál de las autoridades de control es la «principal»; y, por último, cuando la autoridad de control competente no solicite o no se atenga al dictamen del CEPD ([524]). La principal responsabilidad del CEPD es velar por que el RGPD se aplique de manera coherente en todo el territorio de la Unión y desempeña un papel clave en el mecanismo de coherencia, descrito en la sección 5.5.

- **Consulta:** Una de las funciones del CEPD es asesorar a la Comisión sobre cualquier materia relacionada con la protección de datos de carácter personal en la Unión, como modificaciones del RGPD, revisiones de normas de la UE que impliquen tratamiento de datos y puedan entrar en conflicto con las normas de protección de datos de la Unión o la adopción de decisiones de adecuación de la Comisión que permitan la transferencia de datos personales a un país tercero u organización internacional.

- **Orientación:** El Comité también publica directrices, recomendaciones y buenas prácticas para fomentar la aplicación coherente del Reglamento y promueve la cooperación y el intercambio de conocimientos entre las autoridades de control. Además, debe animar a las asociaciones de responsables o encargados del tratamiento a elaborar códigos de conducta, así como establecer mecanismos y sellos de certificación de protección de datos.

Las decisiones del CEPD pueden recurrirse ante el TJUE.

5.5. El mecanismo de coherencia del RGPD

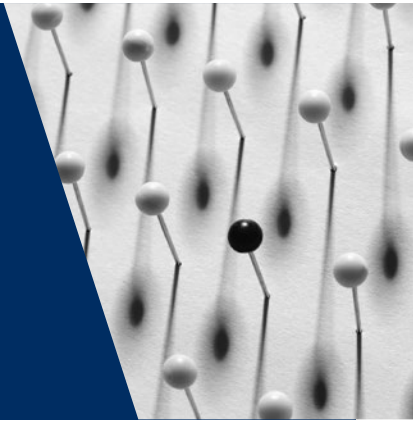
El RGPD establece un mecanismo de coherencia para velar por que el Reglamento se aplique de manera coherente en todos los Estados miembros y que las autoridades de control cooperen entre sí y, en su caso, con la Comisión. El mecanismo de coherencia se utiliza en dos situaciones. La primera se refiere a los dictámenes emitidos por el CEPD en casos en que una autoridad de control competente pretenda

([524]) Ibíd., artículo 65.

adoptar medidas, como una lista de operaciones de tratamiento que requieran una evaluación de impacto de la protección de datos (EIPD), o establecer cláusulas contractuales tipo. La segunda se refiere a las decisiones del CEPD vinculantes para las autoridades de control en casos de ventanilla única y cuando una autoridad de control no solicite o no se atenga a un dictamen del CEPD.

6

Los derechos de los interesados y su observancia



UE	Materias tratadas	CdE
Derecho a ser informado		
Reglamento general de protección de datos, artículo 12 TJUE, C-473/12, *Institut professionnel des agents immobiliers (IPI) contra Englebert*, 2013 TJUE, C-201/14, *Smaranda Bara y otros contra Casa Națională de Asigurări de Sănătate y otros*, 2015	**Transparencia de la información**	Convenio 108 modernizado, artículo 8
Reglamento general de protección de datos, artículo 13, apartados 1 y 2, y artículo 14, apartados 1 y 2	**Contenido de la información**	Convenio 108 modernizado, artículo 8, apartado 1
Reglamento general de protección de datos, artículo 13, apartado 1, y artículo 14, apartado 3	**Momento de suministro de la información**	Convenio 108 modernizado, artículo 9, apartado 1, letra b)
Reglamento general de protección de datos, artículo 12, apartados 1, 5 y 7	**Medios de suministro de la información**	Convenio 108 modernizado, artículo 9, apartado 1, letra b)
Reglamento general de protección de datos, artículo 13, apartado 2, letra d), y artículo 14, apartado 2, letra e), artículos 77, 78 y 79	**Derecho a presentar una reclamación**	Convenio 108 modernizado, artículo 9, apartado 1, letra f)
Derecho de acceso		
Reglamento general de protección de datos, artículo 15, apartado 1 TJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam contra M. E. E. Rijkeboer*, 2009	**Derecho de acceso a los propios datos**	Convenio 108 modernizado, artículo 9, apartado 1, letra b) TEDH, *Leander contra Suecia*, n º 9248/81, 1987

UE	Materias tratadas	CdE
TJUE, asuntos acumulados C-141/12 y C-372/12, *YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel contra M y S*, 2014 TJUE, C-434/16, *Peter Nowak contra Data Protection Commissioner*, 2017		
Derecho de rectificación		
Reglamento general de protección de datos, artículo 16	Rectificación de datos personales inexactos	Convenio 108 modernizado, artículo 9, apartado 1, letra e) TEDH, *Cemalettin Canli contra Turquía*, n.º 22427/04, 2008 TEDH, *Ciubotaru contra Moldavia*, n.º 27138/04, 2010
Derecho de supresión		
Reglamento general de protección de datos, artículo 17, apartado 1	Supresión de los datos personales	Convenio 108 modernizado, artículo 9, apartado 1, letra e) TEDH, *Segerstedt-Wiberg y otros contra Suecia*, n.º 62332/00, 2006
TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 2014 TJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 2017	El derecho al olvido	
Derecho a la limitación del tratamiento		
Reglamento general de protección de datos, artículo 18, apartado 1	Derecho de limitación del uso de los datos personales	
Reglamento general de protección de datos, artículo 19	Obligación de notificación	
Derecho a la portabilidad de los datos		
Reglamento general de protección de datos, artículo 20	Derecho a la portabilidad de los datos	

UE	Materias tratadas	CdE
Derecho de oposición		
Reglamento general de protección de datos, artículo 21, apartado 1 TJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 2017	**Derecho de oposición debido a la situación particular del interesado**	Recomendación sobre creación de perfiles, apartado 5.3 Convenio 108 modernizado, artículo9, apartado 1, letra d)
Reglamento general de protección de datos, artículo 21, apartado 2	**Derecho de oposición al uso de los datos para fines de mercadotecnia**	Recomendación sobre mercadotecnia directa, apartado 4.1
Reglamento general de protección de datos, artículo 21, apartado 5	**Derecho de oposición por medios automatizados**	
Derechos relacionados con las decisiones automatizadas y la elaboración de perfiles		
Reglamento general de protección de datos, artículo 22	**Derechos relacionados con las decisiones automatizadas y la elaboración de perfiles**	Convenio 108 modernizado, artículo 9, apartado 1, letra a)
Reglamento general de protección de datos, artículo 21	**Derecho de oposición a las decisiones automatizadas**	
Reglamento general de protección de datos, artículo 13, apartado 2, letra f)	**Derecho a una explicación elocuente**	Convenio 108 modernizado, artículo 9, apartado 1, letra c)
Recursos, responsabilidad, sanciones e indemnización		
La Carta, artículo 47 TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 2015 Reglamento general de protección de datos, artículos 77-84	**Para infracciones de la legislación nacional sobre protección de datos**	CEDH, artículo 13 (solo para los Estados miembros del CdE) Convenio 108 modernizado, artículo 9, apartado 1, letra f) y artículos 12, 15, 16-21. TEDH, *K.U. contra Finlandia*, n.º 2872/02, 2008 TEDH, *Biriuk contra Lituania*, n.º 23373/03, 2008

UE	Materias tratadas	CdE
Reglamento de protección de datos de las instituciones de la UE, artículos 34 y 49 TUE, C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd* [GS], 2010	**Para infracciones de la legislación de la UE por parte de las instituciones y organismos de la UE**	

La eficacia de las normas jurídicas en general y de los derechos de los interesados en particular depende en gran medida de la existencia de los mecanismos adecuados para hacer que se cumplan. En la era digital, el tratamiento de datos es omnipresente y cada vez más difícil de comprender para las personas físicas. Para mitigar los desequilibrios de poder entre los interesados y los responsables del tratamiento, se han conferido a las personas físicas ciertos derechos para que ejerzan un mayor control sobre el tratamiento de su información personal. El derecho de acceso a los propios datos y el derecho de rectificación de los mismos están consagrados en el artículo 9, apartado 2 de la Carta de los Derechos Fundamentales de la Unión Europea, un documento que constituye Derecho primario de la Unión y que tiene un valor fundamental en el ordenamiento jurídico de la UE. A través del Derecho derivado de la UE —en particular, el Reglamento general de protección de datos— se ha establecido un marco jurídico coherente que da poder a los interesados otorgándoles derechos con respecto a los responsables del tratamiento. Además de los derechos de acceso y rectificación, el RGPD reconoce una serie de otros derechos, como el derecho de supresión (el «derecho al olvido»), el derecho de oposición o de limitación del tratamiento y derechos relacionados con las decisiones automatizadas y la elaboración de perfiles. El Convenio 108 modernizado incluye garantías similares para que los interesados puedan ejercer un control efectivo sobre sus datos. El artículo 8 enumera los derechos que deben poder ejercer las personas físicas en relación con el tratamiento de sus datos personales. Las Partes Contratantes deben velar por que todos los interesados de su jurisdicción dispongan de estos derechos, así como de medios legales y prácticos efectivos para que puedan ejercerlos.

Además de otorgar derechos a las personas físicas, es igualmente importante establecer mecanismos que permitan a los interesados denunciar las violaciones de sus derechos, exigir responsabilidades a los responsables del tratamiento y reclamar indemnizaciones. El derecho a la tutela judicial efectiva garantizado en el CEDH y en la Carta exige que todas las personas tengan a su disposición recursos judiciales.

6.1. Los derechos de los interesados

Puntos clave

- Todos los interesados tienen derecho a ser informados acerca de cualquier tratamiento de sus datos personales que pueda estar efectuando un responsable, sujeto a excepciones limitadas.
- Los interesados tendrán derecho a:
  - obtener acceso a sus propios datos y cierta información sobre el tratamiento;
  - que sus datos sean rectificados por el responsable del tratamiento en el caso de que sean inexactos;
  - que el responsable del tratamiento suprima sus datos, si procede, en el caso de que esté efectuando el tratamiento de manera ilegal;
  - limitar el tratamiento temporalmente;
  - la portabilidad de sus datos a otro responsable en determinadas condiciones.
- Además, los interesados tendrán derecho a oponerse al tratamiento:
  - por razones relacionadas con su situación particular;
  - cuando sus datos se utilicen con fines de mercadotecnia directa.
- Los interesados tienen derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles, que tengan efectos jurídicos o que les afecten de manera significativa. Los interesados también tienen derecho a:
  - obtener intervención humana por parte del responsable del tratamiento;
  - expresar su punto de vista e impugnar las decisiones basadas en el tratamiento automatizado.

6.1.1. Derecho a ser informado

De conformidad tanto con el **Derecho del CdE** como con el **Derecho de la UE**, los responsables de operaciones de tratamiento de datos están obligados a informar al interesado acerca del tratamiento previsto en el momento en que recojan sus datos personales. Esta obligación no depende de que exista una petición por parte del interesado, sino que debe cumplirse de forma proactiva por parte del responsable

del tratamiento, con independencia de si el interesado muestra interés en la información o no.

En el Derecho del CdE, en virtud del artículo 8 del Convenio 108 modernizado, las Partes Contratantes deben disponer que los responsables del tratamiento informen a los interesados acerca de su identidad y residencia habitual, la base jurídica y la finalidad del tratamiento, las categorías de datos personales objeto del tratamiento, los destinatarios de sus datos personales (si los hubiere) y los procedimientos para ejercer sus derechos en virtud del artículo 9, que incluyen los derechos de acceso, rectificación y recurso jurídico. También debe comunicarse a los interesados cualquier otra información adicional que se considere necesaria para garantizar que el tratamiento de datos personales se efectúa de manera leal y transparente. El Informe explicativo del Convenio 108 modernizado aclara que la información presentada a los interesados «debe ser fácilmente accesible, legible, comprensible y adaptada a los interesados correspondientes» ([525]).

En el Derecho de la UE, el principio de transparencia exige que todo tratamiento de datos personales debe ser transparente con carácter general para las personas físicas. Las personas físicas tienen derecho a saber cómo y qué datos personales son recogidos, utilizados o tratados, así como a ser informadas de los riesgos, las salvaguardias y los derechos que tienen en relación con el tratamiento ([526]). El artículo 12 del RGPD establece una obligación muy amplia para los responsables del tratamiento en cuanto al suministro de información transparente y la comunicación de los procedimientos de que disponen los interesados para ejercer sus derechos ([527]). La información debe ser concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Debe facilitarse por escrito, incluso, si procede, por medios electrónicos, e incluso puede facilitarse verbalmente a petición del interesado siempre que se demuestre su identidad fuera de toda duda. La información se facilitará sin dilaciones ni costes excesivos ([528]).

Los artículos 13 y 14 del RGPD tratan del derecho de los interesados a ser informados, respectivamente, cuando los datos personales se hayan obtenido directamente del interesado o cuando no se hayan obtenido del interesado.

([525]) Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 68.

([526]) Reglamento general de protección de datos, considerando 39.

([527]) Ibíd., artículos 13 y 14; Convenio 108 modernizado, artículo 8, apartado 1.

([528]) Reglamento general de protección de datos, artículo 12, apartado 5; Convenio 108 modernizado, artículo 9, apartado 1, letra b).

El alcance del derecho a la información y sus limitaciones conforme al Derecho de la UE se han aclarado en la jurisprudencia del TJUE.

Ejemplo: En *Institut professionnel des agents immobiliers (IPI) contra Englebert* ([529]), se solicitó al TJUE que interpretase el artículo 13, apartado 1, de la Directiva 95/46. Este artículo daba a los Estados miembros la opción de adoptar medidas legislativas para limitar el alcance del derecho del interesado a ser informado en caso necesario para proteger, entre otras cosas, los derechos y libertades de otras personas y para prevenir e investigar delitos o infracciones de la deontología de una profesión regulada. El IPI es un organismo profesional de los agentes inmobiliarios de Bélgica que se encarga de velar por el buen ejercicio de la práctica de la profesión de agente inmobiliario. Solicitó a un órgano jurisdiccional nacional que declarase que los acusados habían violado normas profesionales y que les ordenara cesar en diversas actividades inmobiliarias. La demanda se basó en pruebas aportadas por detectives privados contratados por el IPI.

El órgano jurisdiccional nacional tenía dudas sobre el valor que se debía atribuir a las pruebas aportadas por los detectives, habida cuenta de la posibilidad de que se hubieran obtenido sin observar las exigencias en materia de protección de datos establecidas en la legislación belga, en particular la obligación de informar a los interesados del tratamiento de sus datos personales antes de recoger la información. El TJUE señaló que el artículo 13, apartado 1, decía que los Estados miembros «podrán», pero no tienen obligación de establecer en sus Derechos nacionales excepciones a la obligación de informar a los interesados acerca del tratamiento de sus datos. Puesto que el artículo 13, apartado 1, incluye la prevención, la investigación, la detección y la represión de los delitos penales o de las infracciones de la deontología como motivos por los que los Estados miembros pueden limitar los derechos de las personas físicas, la actividad de un organismo como el IPI y de los detectives privados que actuaron en su nombre podía fundamentarse en dicha disposición. Sin embargo, en el caso de que un Estado miembro no hubiera establecido tal excepción, los interesados deberían ser informados.

([529]) TJUE, C-473/12, *Institut professionnel des agents immobiliers (IPI) contra Geoffrey Englebert y otros*, 7 de noviembre de 2013.

Ejemplo: En *Smaranda Bara y otros contra Casa Națională de Asigurări de Sănătate y otros* ([530]), el TJUE debía aclarar si el Derecho de la UE se opone a que una administración pública nacional transfiera datos personales a otra administración pública para su tratamiento ulterior sin que los interesados sean informados de dicha transferencia y del tratamiento. En ese caso, la administración nacional ANAF no había informado a los demandantes de que había transferido sus datos a la Caja Nacional del Seguro de Enfermedad previamente a la transferencia.

El TJUE consideró que la exigencia conforme al Derecho de la UE de informar al interesado sobre el tratamiento de sus datos personales «resulta especialmente importante en la medida en que es una condición necesaria para el ejercicio por estos de su derecho de acceso a los datos objeto de tratamiento [...] y de su derecho de oposición al tratamiento de esos datos». El principio de tratamiento leal exige que se informe a los interesados acerca de la transferencia de sus datos a otra administración pública para su tratamiento ulterior por esta última. De acuerdo con el artículo 13, apartado 1, de la Directiva 95/46, los Estados miembros pueden limitar el derecho a ser informados si se considera necesario para salvaguardar un interés económico importante del Estado, como los asuntos fiscales. Sin embargo, estas limitaciones deben imponerse con medidas legislativas. Puesto que ni la definición de los datos objeto de transferencia ni las condiciones detalladas de la transferencia se habían establecido en una medida legislativa, sino únicamente en un protocolo entre las dos administraciones públicas, no se cumplían las condiciones de excepción establecidas en el Derecho de la UE. Los demandantes debían haber sido informados de antemano de la transferencia de sus datos a la Caja Nacional del Seguro de Enfermedad y del tratamiento ulterior de dichos datos por este organismo.

Contenido de la información

Conforme al artículo 8, apartado 1, del Convenio 108 modernizado, el responsable del tratamiento está obligado a proporcionar al interesado cualquier información que garantice que el tratamiento de los datos personales se realice de forma leal y transparente, que debe incluir:

([530]) TJUE, C-201/14, *Smaranda Bara y otros contra Casa Națională de Asigurări de Sănătate y otros*, 1 de octubre de 2015.

- la identidad y el lugar habitual de residencia o establecimiento del responsable;
- la base jurídica y los fines del tratamiento previsto;
- las categorías de datos personales objeto de tratamiento;
- los destinatarios o categorías de destinatarios de los datos personales, en su caso;
- los procedimientos de que disponen los interesados para ejercer sus derechos.

Conforme al RGPD, cuando los datos personales sean obtenidos del propio interesado, el responsable está obligado a proporcionar la siguiente información al interesado en el momento en que obtenga los datos personales ([531]):

- la identidad y los datos de contacto del responsable y, en su caso, del DPD;
- los fines y la base jurídica del tratamiento, es decir, un contrato u obligación legal;
- los intereses legítimos del responsable, si en ellos se basa el tratamiento;
- los destinatarios o categorías de destinatarios de los datos personales;
- si los datos serán transferidos a un tercer país u organización internacional y si esto se basa en una decisión de adecuación o se hace con garantías adecuadas;
- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible concretar dicho plazo, los criterios utilizados para determinar el plazo de conservación de los datos;
- los derechos de los interesados en relación con el tratamiento, como los derechos de acceso, rectificación, supresión y limitación del tratamiento u oposición al mismo;

([531]) Reglamento general de protección de datos, artículo 13, apartado 1.

- si la comunicación de datos personales es un requisito legal o contractual, si el interesado está obligado a facilitar los datos personales, así como las consecuencias de no facilitar tales datos;

- la existencia de decisiones automatizadas, incluida la elaboración de perfiles;

- el derecho a presentar una reclamación ante una autoridad de control;

- la existencia del derecho a retirar el consentimiento.

En los casos de decisiones automatizadas, incluida la elaboración de perfiles, los interesados deberán recibir información significativa sobre la lógica aplicada en dicha elaboración de perfiles, así como la importancia y las consecuencias previstas de dicho tratamiento.

En los casos en que los datos personales no se obtengan del interesado directamente, el responsable del tratamiento debe notificar a la persona física el origen de los datos. En cualquier caso, el controlador deberá, entre otras cosas, informar a los interesados acerca de la existencia de decisiones automatizadas, incluida la elaboración de perfiles ([532]). Por último, si un responsable tiene intención de tratar datos personales con un fin distinto del originalmente declarado al interesado, los principios de limitación de la finalidad y de transparencia exigen que el responsable facilite al interesado información acerca de este nuevo fin. Los responsables deben facilitar la información con anterioridad a cualquier tratamiento ulterior. En otras palabras, cuando el interesado haya dado su consentimiento al tratamiento de los datos personales, el responsable deberá obtener un nuevo consentimiento si la finalidad del tratamiento cambia o si se añaden fines ulteriores.

Momento de suministro de la información

El RGPD distingue entre dos escenarios y dos momentos en los que el responsable del tratamiento debe facilitar información al interesado:

([532]) Reglamento general de protección de datos, artículo 13, apartado 2 y artículo 14, apartado 2, letra f).

- Cuando los datos personales se obtengan directamente del interesado, el responsable deberá comunicar al interesado toda su información y los derechos que le asisten en virtud del RGPD en el momento de obtener los datos ([533]).

  Si el responsable tiene intención de realizar un tratamiento ulterior de los datos personales con un fin distinto, deberá facilitar toda la información pertinente antes de llevar a cabo el tratamiento.

- Cuando los datos personales no se hayan obtenido del interesado, el responsable está obligado a facilitar la información sobre el tratamiento al interesado «dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes», o antes de comunicar los datos a un tercero ([534]).

El Informe explicativo del Convenio 108 modernizado estipula que si no es posible informar a los interesados al comenzar el tratamiento, puede hacerse en un momento posterior, por ejemplo cuando el responsable se ponga en contacto con el interesado por cualquier motivo ([535]).

Distintos modos de suministrar información

Tanto en el Derecho del CdE como en el Derecho de la UE, la información que el responsable debe facilitar a los interesados debe ser concisa, transparente, inteligible y de fácil acceso. Debe facilitarse por escrito, o por otros medios, incluidos los medios electrónicos, con lenguaje claro y sencillo y fácil de comprender. Cuando facilite información, el responsable puede utilizar iconos normalizados para facilitar la información de manera fácilmente visible e inteligible ([536]). Por ejemplo, se puede utilizar un icono que represente un candado para indicar que los datos se han obtenido de manera segura o que están cifrados. Los interesados pueden solicitar que la información se les facilite verbalmente. La información debe ser gratuita, a menos que las peticiones del interesado sean de carácter manifiestamente infundado

([533]) Ibíd., artículo 13, apartados 1 y 2, texto introductorio con el que el Reglamento general de protección de datos se refiere a que la información sobre la obligación es aplicable «en el momento en que [los datos personales] se obtengan».

([534]) Ibíd., artículo 13, apartado 3 y artículo 14, apartado 3; véase también la referencia a los intervalos razonables y sin dilación excesiva en el Convenio 108 modernizado, artículo 8, apartado 1, letra b).

([535]) Informe explicativo del Convenio 108 modernizado, apartado 70.

([536]) La Comisión Europea desarrollará posteriormente la información que se ha de presentar por medio de iconos y los procedimientos para proporcionar iconos normalizados por medio de actos delegados; véase el Reglamento general de protección de datos, artículo 12, apartado 8.

o excesivo (es decir, repetitivo) ([537]). La facilidad de acceso a la información proporcionada es esencial para que el interesado pueda ejercer los derechos que le asisten conforme a la legislación de la UE sobre protección de datos.

El principio de tratamiento leal exige que la información sea fácil de comprender para los interesados. Debe utilizarse lenguaje adecuado para los destinatarios. El nivel y el tipo de lenguaje que se utilicen tendrán que ser distintos en función de si el público destinatario es, por ejemplo, adulto o infantil, el público en general o expertos académicos. La cuestión de cómo equilibrar este aspecto de información comprensible se considera en el Dictamen del Grupo de Trabajo del Artículo 29 sobre una mayor armonización de las disposiciones relativas a la información. En él se promueve la idea de los avisos de múltiples niveles ([538]), que permiten al interesado decidir qué nivel de detalle prefiere. Sin embargo, esta forma de presentar la información no libera al responsable de su obligación en virtud de los artículos 13 y 14 del RGPD. El responsable sigue obligado a facilitar toda la información al interesado.

Uno de los modos más eficaces de proporcionar información es que la página de inicio del responsable del tratamiento incluya las cláusulas de información oportunas, como una política de privacidad del sitio web. Sin embargo, buena parte de la población no utiliza internet, por lo que las empresas o administraciones públicas deberán tener esto en cuenta en sus políticas de información.

Un aviso de privacidad acerca del tratamiento de datos personales en una página web podría ser algo así:

¿Quiénes somos?

El «responsable» del tratamiento de los datos es Bed and Breakfast C&U, con domicilio social en [dirección: xxx], Tel.: xxx; Fax: xxx; Correo electrónico: ; datos de contacto con el delegado de protección de datos: [xxx].

El aviso de información de datos personales forma parte de los términos y condiciones por los que se rigen nuestros servicios hoteleros.

([537]) Reglamento general de protección de datos, artículo 12, apartados 1, 5 y 7, y Convenio 108 modernizado, artículo 9, apartado 1, letra b).

([538]) Grupo de Trabajo del Artículo 29 (2004), *Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información*, WP 100, Bruselas, 25 de noviembre de 2004.

¿Qué datos recogemos de usted?

Recogemos de usted los siguientes datos personales: nombre, dirección postal, número de teléfono, dirección de correo electrónico, información de estancia, número de tarjeta de crédito y débito y direcciones IP o nombres de dominio de los ordenadores que utiliza para conectarse a nuestra web.

¿Por qué recogemos sus datos?

Tratamos sus datos con su consentimiento y con objeto de realizar reservas, formalizar y cumplir los contratos relativos a los servicios que le ofrecemos y cumplir los requisitos que impone la ley, como por ejemplo la Ley de tasas locales, que nos obliga a recoger datos personales con el fin de realizar el pago de la tasa municipal de alojamientos.

¿Cómo tratamos sus datos?

Sus datos personales se conservarán durante un plazo de tres meses. Sus datos no están sujetos a procedimientos de decisión automatizados.

Nuestro Bed and Breakfast C&U sigue estrictos procedimientos de seguridad para cuidar de que sus datos personales no sean dañados, destruidos o revelados a terceros sin su permiso, así como para evitar accesos no autorizados. Los ordenadores que conservan la información se mantienen en un entorno seguro con acceso físico restringido. Utilizamos cortafuegos y otras medidas para limitar el acceso electrónico. Si debemos transferir los datos a un tercero, exigimos que apliquen medidas similares para proteger sus datos personales.

El acceso a toda la información que recogemos o registramos está restringido a nuestras oficinas. Solo las personas que necesitan dicha información para cumplir con sus obligaciones en virtud del presente contrato reciben acceso a los datos personales. Cuando necesitemos información que le identifique, se la solicitaremos expresamente. Es posible que les pidamos que colaboren con nuestros controles de seguridad antes de poner información a su disposición. Podrán actualizar los datos personales que nos faciliten en cualquier momento poniéndose en contacto con nosotros directamente.

¿Cuáles son sus derechos?

Tiene derecho de acceso a sus datos, a obtener una copia de sus datos, a solicitar su supresión o rectificación o a solicitar la portabilidad de sus datos a otro responsable.

Puede enviarnos sus peticiones a la dirección de contacto . Bed and Breakfast C&U tiene la obligación de contestar a su petición en el plazo de un mes, pero si dicha petición es excesivamente compleja o recibimos un número demasiado elevado de peticiones, le comunicaremos que este periodo puede prorrogarse otros dos meses.

Acceso a sus datos personales

Tiene usted derecho de acceso a sus datos, a ser informado —cuando lo solicite— de las razones que motivan el tratamiento de los datos, a solicitar su supresión o rectificación y a no ser objeto de una decisión puramente automatizada sin que se tengan en cuenta sus puntos de vista. Puede enviarnos sus peticiones a la dirección de contacto . También tiene derecho de oposición al tratamiento, a retirar su consentimiento y a presentar una reclamación ante la autoridad de control nacional si considera que este tratamiento de los datos vulnera la ley y a reclamar que se le indemnice por los daños y perjuicios ocasionados a consecuencia del tratamiento ilícito.

Derecho a presentar una reclamación

El RGPD obliga al responsable del tratamiento a informar a los interesados acerca de los mecanismos de ejecución establecidos conforme al Derecho nacional y al Derecho de la UE para los casos de violación de la seguridad de los datos personales. El responsable debe informar a los interesados acerca de su derecho a presentar una reclamación por violación de datos personales ante una autoridad de control y, si fuera necesario, ante un órgano jurisdiccional nacional ([539]). El Derecho del CdE también dispone el derecho de los interesados a ser informados sobre los modos de ejercicio de sus derechos, incluyendo el derecho a un recurso ([540]).

([539]) Reglamento general de protección de datos, artículo 13, apartado 2, letra d) y artículo 14, apartado 2, letra e); Convenio 108 modernizado, artículo 8, apartado 1, letra f).

([540]) Convenio 108 modernizado; párrafo primero (f) del artículo 9.

Excepciones a la obligación de informar

El RGPD contempla excepciones a la obligación de informar. De acuerdo con el artículo 13, apartado 4 y el artículo 14, apartado 5 del RGPD, la obligación de informar a los interesados no es de aplicación si el interesado ya dispone de toda la información pertinente ([541]). Además, cuando los datos personales no se hayan obtenido del interesado, la obligación de informar no será de aplicación cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ([542]).

Además, el RGPD otorga a los Estados miembros cierta discrecionalidad para limitar los derechos y obligaciones conferidos por el Reglamento a las personas físicas cuando esta sea una medida necesaria y proporcionada en una sociedad democrática, por ejemplo, para salvaguardar la seguridad nacional y pública, la defensa, la protección de las investigaciones y los procedimientos judiciales o la protección de intereses económicos y financieros, así como intereses privados que sean más imperiosos que los intereses de protección de los datos ([543]).

Todas las excepciones o limitaciones deben ser necesarias en una sociedad democrática y proporcionada para el fin que persiguen. En casos muy excepcionales, por ejemplo, por indicaciones médicas, la protección del interesado podrá exigir por sí misma una limitación de la transparencia, lo cual hace especial referencia a la limitación del derecho de acceso de todo interesado ([544]). No obstante, como nivel mínimo de protección, la legislación nacional debe respetar el contenido esencial de los derechos y libertades fundamentales protegidos por el Derecho de la UE ([545]). Para ello es preciso que la legislación nacional contenga disposiciones específicas que aclaren la finalidad del tratamiento, las categorías de datos personales que incluye, garantías y otros requisitos procedimentales ([546]).

Cuando los datos se recojan con fines de investigación científica o histórica, fines estadísticos o fines de archivo en interés público, el Derecho de la Unión o de los

([541]) Ibíd., artículo 13, apartado 4 y artículo 14, apartado 5, letra a).

([542]) Ibíd., artículo 14, apartado 5, letras b) hasta e); Convenio 108 modernizado, artículo 11.

([543]) Reglamento general de protección de datos, artículo 23, apartado 14; Convenio 108 modernizado, artículos 8 y 9.

([544]) Reglamento general de protección de datos, artículo 15; Convenio 108 modernizado, artículo 8.

([545]) Reglamento general de protección de datos, artículo 23, apartado 1.

([546]) Ibíd., artículo 23, apartado 2.

Estados miembros puede contemplar excepciones a la obligación de informar siempre que sea probable que se pueda imposibilitar u obstaculizar gravemente el logro de estos fines específicos ([547]).

Existen limitaciones similares en el Derecho del CdE, donde los derechos garantizados bajo el artículo 9 del Convenio 108 modernizado pueden quedar sujetos a las restricciones del artículo 11, bajo estrictas condiciones. Además, de conformidad al párrafo segundo del artículo 10, la obligación de transparencia en el tratamiento impuesta a los responsables del tratamiento no se aplica cuando el interesado ya dispone de la información.

El derecho de acceso a los propios datos

En el Derecho del CdE, el derecho de acceso de una persona física a sus propios datos está expresamente reconocido en el artículo 8 del Convenio 108 modernizado. En él se establece que toda persona física tiene derecho a obtener, cuando lo solicite, información acerca del tratamiento de datos personales relacionados con ella, y que le sea comunicada de manera inteligible. El derecho de acceso no solo está reconocido en las disposiciones del Convenio 108 modernizado, sino también en la jurisprudencia del TEDH. El TEDH ha dictaminado reiteradamente que las personas físicas tienen derecho de acceso a la información acerca de sus datos personales y que este derecho nace de la necesidad de respetar la vida privada ([548]). Sin embargo, el derecho de acceso a los datos personales conservados por organizaciones públicas o privadas puede limitarse en determinadas circunstancias ([549]).

En el Derecho de la UE, el derecho de acceso a los propios datos está expresamente reconocido en el artículo 15 del RGPD y también está recogido como uno de los elementos del derecho fundamental a la protección de los datos personales en el artículo 8, apartado 2 de la Carta de los Derechos Fundamentales de la Unión Europea ([550]). El derecho de una persona física a obtener acceso a sus propios

([547]) Ibíd., artículo 89, apartados 2 y 3.

([548]) TEDH, *Gaskin contra Reino Unido*, n.º 10454/83, 7 de julio de 1989; TEDH, *Odièvre contra Francia* [GS], n.º 42326/98, 13 de febrero de 2003; TEDH, *K.H. y otros contra Eslovaquia,* n.º 32881/04, 28 de abril de 2009; TEDH, *Godelli contra Italia*, n.º 33783/09, 25 de septiembre de 2012.

([549]) TEDH, *Leander contra Suecia*, n.º 9248/81, 26 de marzo de 1987.

([550]) Véase también TJUE, asuntos acumulados C-141/12 y C-372/12, *YS contra Minister voor Immigratie, Integratie en Asiel* y *Minister voor Immigratie, Integratie en Asiel contra M y S*, 17 de julio de 2014; TJUE, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) contra Autoridad Europea de Seguridad Alimentaria (EFSA), Comisión Europea*, 16 de julio de 2015.

datos personales es un elemento clave de la legislación europea sobre protección de datos ([551]).

El RGPD establece que todo interesado tiene derecho de acceso a sus datos personales y a determinada información sobre el tratamiento que los responsables deben facilitar ([552]). En particular, todos los interesados tienen derecho a obtener (del responsable) confirmación de si se están tratando datos relativos a su persona o no, así como información, como mínimo, acerca de lo siguiente:

- los fines del tratamiento;
- las categorías de datos de que se trate;
- los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;
- el plazo previsto de conservación de los datos o, de no ser posible, los criterios utilizados para determinar ese plazo;
- la existencia de los derechos de rectificación o supresión de los datos personales o de limitación del tratamiento;
- el derecho a presentar una reclamación ante una autoridad de control;
- cualquier información disponible sobre el origen de los datos objeto de tratamiento si dichos datos no se han obtenido del propio interesado;
- en los casos de decisiones automatizadas, la lógica aplicada al tratamiento automatizado de los datos.

El responsable debe facilitar al interesado una copia de los datos personales objeto de tratamiento. Toda la información que se comunique al interesado debe facilitarse en forma inteligible, lo que significa que el responsable debe asegurarse de que el interesado pueda comprender la información que se le facilita. Por ejemplo, la inclusión de abreviaturas técnicas, términos codificados o acrónimos en respuesta a una

([551]) TJUE, asuntos acumulados C-141/12 y C-372/12, *YS contra Minister voor Immigratie, Integratie en Asiel y Minister voor Immigratie, Integratie en Asiel contra M y S*, 17 de julio de 2014.

([552]) Reglamento general de protección de datos, artículo 15, apartado 1.

solicitud de acceso no suele ser suficiente, a menos que se explique el significado de dichos términos. Cuando se adopten decisiones automatizadas, incluida la elaboración de perfiles, será necesario explicar la lógica general aplicada a la decisión, incluidos los criterios especiales que se hayan considerado al evaluar al interesado. En el **Derecho del CdE** existen requisitos similares ([553]).

Ejemplo: El acceso a sus datos personales ayudará al interesado a determinar si los datos son precisos o no. Por tanto, es esencial que se comuniquen al interesado, de manera inteligible, no solo los datos personales propiamente dichos que son objeto de tratamiento, sino también las categorías de datos que se tratan, como el nombre, la dirección IP, las coordenadas de geolocalización, el número de tarjeta de crédito, etc.

En la respuesta a una petición de acceso deberá facilitarse información sobre el origen de los datos, cuando no se hayan obtenido del propio interesado, siempre que se disponga de dicha información. Esta disposición ha de interpretarse en el contexto de los principios de lealtad, transparencia y responsabilidad proactiva. Un responsable no puede destruir información sobre el origen de los datos a fin de quedar exento de la obligación de revelarla, a menos que la destrucción hubiera tenido lugar pese a recibirse la petición de acceso, y deberá cumplir con sus requisitos generales de «responsabilidad proactiva».

Tal como se establece en la jurisprudencia del TJUE, el derecho de acceso a los datos personales no puede restringirse indebidamente por límites de tiempo. Además, los interesados deben tener una oportunidad razonable de obtener información sobre las operaciones de tratamiento de datos que hayan tenido lugar en el pasado.

Ejemplo: En *Rijkeboer* ([554]), se pidió al TJUE que determinara si el derecho de acceso de una persona física a la información sobre los destinatarios o las categorías de destinatarios de los datos personales, y al contenido de dichos datos, podía circunscribirse al periodo de un año anterior a la solicitud de acceso.

([553]) Véase el Convenio 108 modernizado, artículo 9, apartado 1, letra c).

([554]) TJUE, C-553/07, *College van burgemeester en wethouders van Rotterdam contra M. E. E. Rijkeboer*, 7 de mayo de 2009.

Para determinar si la legislación de la UE autoriza dicha limitación en el tiempo, el TJUE decidió interpretar el artículo 12 a la luz de los fines de la Directiva. El TJUE declaró en primer lugar que el derecho de acceso es indispensable para que el interesado pueda ejercer su derecho a que el responsable rectifique, suprima o bloquee sus datos o notifique tal rectificación, supresión o bloqueo a los terceros a quienes se hayan comunicado los datos. También es necesario el derecho de acceso efectivo para que el interesado pueda ejercer su derecho de oposición al tratamiento de datos personales o su derecho a presentar una reclamación y exigir una indemnización ([555]).

Para garantizar el efecto práctico de los derechos de que gozan los interesados, el TJUE dictaminó que «el citado derecho debe necesariamente afectar al pasado. De no ser así, el interesado no estaría en condiciones de ejercer eficazmente su derecho a exigir la rectificación, la supresión o el bloqueo de los datos que se presumen ilícitos o incorrectos, ni de interponer un recurso judicial y obtener la compensación por el daño sufrido».

6.1.2. Derecho de rectificación

En el Derecho de la UE y **en el Derecho del CdE**, los interesados tienen derecho a que se rectifiquen sus datos personales. La exactitud de los datos personales es esencial para garantizar un alto nivel de protección de datos para los interesados ([556]).

Ejemplo: En *Ciubotaru contra Moldavia* ([557]), el demandante no pudo modificar la inscripción de su origen étnico de moldavo a rumano en los registros oficiales, supuestamente debido al hecho de que no había fundamentado su petición. El TEDH consideró aceptable que los Estados exijan pruebas objetivas cuando registran la identidad étnica de una persona física. Cuando dicha petición estuviera basada en motivos meramente subjetivos e infundados, las autoridades podrían denegarla. Sin embargo, la reclamación del demandante se había basado en algo más que en una percepción subjetiva de su propia etnia, ya que había aportado vínculos objetivamente verificables con el grupo

([555]) Reglamento general de protección de datos, artículos 15, apartado 1, letras c) y f), artículo 16, artículo 17, apartado 2, y artículo 21, y capítulo VIII.

([556]) Ibíd., artículo 16 y considerando 65; Convenio 108 modernizado, artículo 9, apartado 1, letra e).

([557]) TEDH, *Ciubotaru contra Moldavia*, n.º 27138/04, 27 de abril de 2010, apartados 51 y 59.

étnico rumano, como la lengua, el nombre, la empatía y otros elementos. Sin embargo, conforme a la legislación nacional, se exigió al demandante que aportase pruebas de que sus padres habían pertenecido al grupo étnico rumano. Dada la realidad histórica de Moldavia, dicha exigencia había creado un obstáculo insuperable para registrar una identidad étnica distinta de la que habían inscrito las autoridades soviéticas en el registro respecto de sus padres. Al evitar que se examinase la reclamación del demandante a la luz de pruebas objetivamente verificables, el Estado no había cumplido con su obligación positiva de garantizar al demandante el respeto efectivo a su vida privada. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

En algunos casos, bastará que el interesado simplemente pida la rectificación, por ejemplo, de la ortografía de un nombre, o un cambio de dirección o de número de teléfono. De acuerdo con el **Derecho de la UE** y el **Derecho del CdE**, los datos personales inexactos deben rectificarse sin dilación indebida o excesiva ([558]). No obstante, si este tipo de peticiones están vinculadas a cuestiones jurídicas significativas, como la identidad jurídica del interesado o el lugar de residencia correcto para la entrega de documentos jurídicos, las solicitudes de rectificación no serán suficientes y el responsable del tratamiento puede estar facultado para solicitar pruebas de la supuesta inexactitud. Estas peticiones no deben imponer la carga de la prueba sobre el interesado de manera irrazonable y, por tanto, impedir que los interesados consigan que se rectifiquen sus datos. El TEDH consideró que se había violado el artículo 8 del CEDH en diversos asuntos en que el demandante no fue capaz de refutar la exactitud de la información conservada en registros secretos ([559]).

Ejemplo: En *Cemalettin Canli contra Turquía* ([560]), el TEDH resolvió que los informes policiales incorrectos en procedimientos penales violaban el artículo 8 del CEDH.

El demandante había estado implicado dos veces en procedimientos penales debido a su supuesta pertenencia a organizaciones ilegales, pero nunca había sido condenado. Cuando el demandante fue detenido de nuevo y acusado de

([558]) Reglamento general de protección de datos, artículo 16; Convenio 108 modernizado, artículo 9, apartado 1.

([559]) TEDH, *Rotaru contra Rumanía* [GS], n.º 28341/95, 4 de mayo de 2000.

([560]) TEDH, *Cemalettin Canli contra Turquía*, n.º 22427/04, 18 de noviembre de 2008, apartados 33 y 42-43; TEDH, *Dalea contra Francia*, n.º 964/07, 2 de febrero de 2010.

otro delito, la policía envió al órgano jurisdiccional penal un informe titulado «*formulario de información sobre otros delitos*», en el cual se decía que el demandante había sido miembro de dos organizaciones ilegales. La petición del demandante de obtener el informe y de que se modificase el expediente policial no tuvo éxito. El TEDH resolvió que la información contenida en el informe policial estaba comprendida en el ámbito de aplicación del artículo 8 del CEDH, ya que la información pública recogida sistemáticamente y conservada en expedientes en poder de las autoridades también podía inscribirse en el concepto de «vida privada». Además, el texto del informe policial no era correcto y su envío al órgano jurisdiccional penal no se había realizado de conformidad con la legislación nacional. El Tribunal concluyó que había existido una violación del artículo 8.

Durante el litigio o procedimiento civil ante una autoridad pública para decidir si los datos son correctos o no, los interesados pueden solicitar que se realice una inscripción o anotación en su fichero de datos para indicar que se ha impugnado su exactitud y que está pendiente de resolución oficial ([561]). Durante este periodo, el responsable del tratamiento no deberá presentar los datos como correctos o no sujetos a modificación, especialmente a terceros.

6.1.3. Derecho de supresión («el derecho al olvido»)

Es especialmente importante asegurar el derecho de los interesados a la supresión de sus propios datos para la aplicación efectiva de los principios de protección de datos, y en particular del principio de minimización de datos (los datos personales deben limitarse a lo necesario para los fines del tratamiento de dichos datos). Por lo tanto, el derecho de supresión está recogido en instrumentos jurídicos del CdE y de la UE ([562]).

Ejemplo: En *Segerstedt-Wiberg y otros contra Suecia* ([563]), los demandantes se habían afiliado a determinados partidos políticos liberales y comunistas. Sospechaban que se había introducido dicha información sobre ellos en los registros policiales de seguridad y solicitaron su supresión. El TEDH

([561]) Reglamento general de protección de datos, artículo 16, segunda frase.

([562]) Ibíd., artículo 17.

([563]) TEDH, *Segerstedt-Wiberg y otros contra Suecia*, n.º 62332/00, 6 de junio de 2006, apartados 89 y 90; véase, asimismo, por ejemplo, TEDH, *M.K. contra Francia*, n.º 19522/09, 18 de abril de 2013.

quedó convencido de que la conservación de los datos en cuestión tenía un fundamento jurídico y perseguía un fin legítimo. Sin embargo, respecto de algunos de los demandantes, el TEDH consideró que la conservación continuada de los datos suponía una injerencia desproporcionada en sus vidas privadas. Por ejemplo, en el caso de uno de los demandantes, las autoridades conservaban información de que en 1969 había defendido supuestamente la resistencia violenta a un control policial durante unas manifestaciones. El TEDH consideró que esta información no tenía ningún interés relevante para la seguridad nacional, en especial debido a su carácter histórico. El Tribunal determinó que existía una violación del artículo 8 del TEDH en relación con cuatro de los cinco demandantes ya que, dado el largo tiempo transcurrido desde los actos presuntamente cometidos por los demandantes, la conservación continuada de sus datos carecía de relevancia.

Ejemplo: En *Brunet contra Francia* ([564]), los demandantes denunciaron la conservación de sus datos personales en una base de datos policial que contenía información sobre personas convictas, personas acusadas y víctimas. Aunque los procedimientos penales contra el demandante se habían retirado, sus datos aparecían en esa base de datos. El Tribunal resolvió que había existido una violación del artículo 8 del CEDH. Para llegar a esta conclusión, el Tribunal consideró que, en la práctica, no había posibilidad de que el demandante suprimiera sus datos personales de la base de datos. El TEDH también consideró la naturaleza de la información incluida en la base de datos y estimó que invadía la privacidad del demandante, ya que contenía detalles de su identidad y su personalidad. Además, resolvió que el periodo de conservación de ficheros personales en la base de datos, que ascendía a veinte años, era excesivo, en particular porque ningún órgano jurisdiccional había condenado jamás al demandante.

El Convenio 108 modernizado reconoce expresamente que todas las personas físicas tienen derecho a que se supriman datos inexactos, falsos o tratados de forma ilícita ([565]).

En el Derecho de la UE, el artículo 17 del RGPD hace efectivas las peticiones de supresión o eliminación de datos por parte de los interesados. El derecho de

([564]) TEDH, *Brunet contra Francia*, n.º 21010/10, 18 de septiembre de 2014.

([565]) Convenio 108 modernizado, artículo 9, apartado 1, letra e).

supresión de los propios datos personales sin dilación indebida se aplicará cuando concurra alguna de las circunstancias siguientes:

- que los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- que el interesado retire el consentimiento en que se base el tratamiento y este no se base en otro fundamento jurídico;
- que el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento;
- que los datos personales hayan sido tratados ilícitamente;
- que los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
- que los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8 del RGPD ([566]).

La carga de la prueba de que el tratamiento de los datos es legítimo recae en el responsable del tratamiento, ya que es responsable de la licitud del tratamiento ([567]). De acuerdo con el principio de responsabilidad proactiva, el responsable deberá poder demostrar en cualquier momento que su operación de tratamiento de datos tiene una base jurídica sólida. De no ser así, deberá cesar en el tratamiento ([568]). El RGPD define excepciones al derecho al olvido, incluso cuando el tratamiento de datos personales sea necesario:

- para ejercer el derecho a la libertad de expresión e información;
- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión

([566]) Reglamento general de protección de datos, artículo 17, apartado 1.

([567]) Ibíd.

([568]) Ibíd., artículo 5, apartado 2.

realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

- por razones de interés público en el ámbito de la salud pública;
- con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;
- para la formulación, el ejercicio o la defensa de reclamaciones ([569]).

El TJUE ha ratificado la importancia del derecho de supresión para garantizar un alto nivel de protección de datos.

> Ejemplo: En *Google Spain* ([570]), el TJUE examinó si Google estaba obligada a suprimir de los resultados de sus búsquedas información anticuada sobre las dificultades financieras del demandante. Entre otras cosas, Google rechazó ser responsable, alegando que se limitaba a proporcionar un hipervínculo a la página web del editor que aloja la información, en este caso un periódico que informaba sobre los problemas de insolvencia del demandante ([571]). Google alegó que la petición de suprimir información anticuada de una página web debía dirigirse al alojamiento de la página web y no a Google, que simplemente proporcionaba un enlace a la página original. El TJUE concluyó que Google, cuando busca información y páginas web en internet y cuando indexa contenido para ofrecer los resultados de una búsqueda, se convierte en un responsable del tratamiento de los datos que tiene responsabilidades y obligaciones con arreglo al Derecho de la Unión.

([569]) Ibíd., art. 17 apartado 3.

([570]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014, apartados 55-58.

([571]) Google también rechazó la aplicación de las normas de protección de datos de la UE debido al hecho de que Google Inc. tiene su domicilio social en los Estados Unidos y el tratamiento de datos personales objeto de este asunto también se había llevado a cabo en los Estados Unidos. Un segundo argumento para la inaplicabilidad de la legislación sobre protección de datos de la UE tenía que ver con la reivindicación de que los motores de búsqueda no pueden ser considerados «responsables» del tratamiento de los datos que muestran en sus resultados, ya que no tienen conocimiento de los datos ni ejercen control alguno sobre ellos. El TJUE desestimó ambos argumentos, declarando que la Directiva 95/46/CE era aplicable en ese caso, y continuó con el examen del alcance de los derechos que garantizaba, en particular el derecho de supresión de los datos personales.

El TJUE aclaró que los motores de búsqueda en internet y los resultados de las búsquedas que proporcionan datos personales pueden facilitar la creación de un perfil detallado de una persona física ([572]). Los motores de búsqueda hacen que la información contenida en la lista de resultados sea ubicua. En vista de su posible gravedad, esa injerencia no puede justificarse por el mero interés económico que tenga el operador de un motor de este tipo en ese tratamiento. Es preciso buscar un equilibrio justo, en particular entre el interés legítimo de los usuarios de internet en el acceso a la información y los derechos fundamentales del interesado en virtud de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. En una sociedad cada vez más digitalizada, el requisito de que los datos personales sean precisos y no excedan de lo estrictamente necesario (es decir, informar al público) es fundamental para garantizar un alto nivel de protección de datos a las personas físicas. El «responsable del tratamiento, debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicho tratamiento cumple los requisitos» del Derecho de la UE, a fin de que las garantías legales establecidas tengan pleno efecto ([573]). Esto significa que el derecho de supresión de los propios datos personales cuando el tratamiento esté anticuado o ya no sea necesario también alcanza a los responsables del tratamiento que reproducen la información ([574]).

Tras examinar si Google estaba obligada a suprimir los enlaces relacionados con el demandante, el TJUE dictaminó que, en determinadas condiciones, las personas físicas tienen derecho a solicitar que se supriman sus datos personales. Este derecho puede invocarse cuando la información relativa a una persona física sea inexacta, inadecuada, irrelevante o excesiva para los fines del tratamiento de datos. El TJUE reconoció que este derecho no es absoluto, sino que debe ponderarse con otros derechos e intereses, en particular el interés del público en general en obtener acceso a determinada información. Cada solicitud de supresión requiere una valoración específica para alcanzar un equilibrio entre los derechos fundamentales a la protección de los datos personales y a la vida privada del interesado, por una parte, y los

([572]) Ibíd., apartados 36, 38, 80-81 y 97.

([573]) Ibíd., apartados 81-83.

([574]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014, apartado 88. Véase también Grupo de Trabajo del Artículo 29 (2014), *Directrices sobre la aplicación de la sentencia del TJUE «Google Spain y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González», C-131/12*, WP 225, Bruselas, 26 de noviembre de 2014, y Recommendation CM/Rec 2012(3) of the Committee of Ministers to Member States on the protection of human rights with regard to search engines, 4 de abril de 2012.

intereses legítimos de todos los usuarios de internet, incluidos los editores, por otra. El TJUE ofreció orientaciones sobre los factores que deben tenerse en cuenta durante este ejercicio de ponderación equilibrada. La naturaleza de la información en cuestión es un factor especialmente importante. Si la información se refiere a la vida privada de la persona física y cuando no exista interés público en la disponibilidad de la información, la protección de datos y la privacidad prevalecerían sobre el derecho del público en general a obtener acceso a la información. Por el contrario, si parece que el interesado es una figura pública o que la información es de tal naturaleza que está justificado ponerla a disposición del público en general, entonces el interés preponderante del público en general en tener acceso a la información puede justificar la injerencia en los derechos fundamentales del interesado a la protección de datos y a la privacidad.

Tras esta sentencia, el Grupo de Trabajo del Artículo 29 adoptó directrices para aplicar el fallo del TJUE ([575]). Estas directrices incluyen una lista de criterios comunes que deben aplicar las autoridades de control cuando atienden reclamaciones relacionadas con peticiones de supresión realizadas por personas físicas, con explicaciones sobre lo que comprende dicho derecho de supresión y orientaciones para realizar la ponderación de derechos. Estas directrices reiteran que las evaluaciones han de realizarse caso por caso. Dado que el derecho al olvido no es absoluto, el resultado de una solicitud puede ser diferente según el caso de que se trate. Esto también se ilustra en la jurisprudencia del TJUE posterior a Google.

Ejemplo: En *Camera di Commercio di Lecce contra Manni* ([576]), el TJUE debía examinar si una persona física tenía derecho a obtener la supresión de sus datos personales publicados en el registro público de sociedades, una vez que esta compañía había dejado de existir. El Sr. Manni había solicitado a la Cámara de Comercio de Lecce que suprimiera sus datos personales de ese registro, tras descubrir que sus clientes potenciales podían consultarlo y ver que había sido administrador de una sociedad que se había declarado en quiebra hacía más de una década. El demandante creía que esta información sería disuasoria para posibles clientes.

([575]) Grupo de Trabajo del Artículo 29 (2014), Directrices sobre la aplicación de la sentencia del TJUE «Google Spain y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González», C-131/12, WP 225, Bruselas, 26 de noviembre de 2014.

([576]) TJUE, C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni, 9 de marzo de 2017.

Para ponderar el derecho del Sr. Manni a la protección de sus datos personales con el interés del público en general en el acceso a la información, el TJUE examinó en primer lugar la finalidad del registro público. Señaló el hecho de que la publicidad estaba establecida por la ley, y en particular por una Directiva de la UE que tenía por objeto facilitar el acceso de terceros a la información de las sociedades. Los terceros debían por tanto tener acceso y poder examinar los documentos básicos de una empresa y otra información referente a la misma, «concretamente la identidad de las personas que tienen el poder de obligarla». La publicación también tenía la finalidad de garantizar la seguridad jurídica en vista de la intensificación del comercio entre los Estados miembros, al garantizar que los terceros tengan acceso a toda la información pertinente sobre empresas de toda la UE.

El TJUE señaló además que, incluso con el paso del tiempo y después de disuelta una empresa, a menudo continúan existiendo derechos y obligaciones legales en relación con esa empresa. Los conflictos relacionados con la disolución pueden prolongarse en el tiempo y pueden plantearse cuestiones relativas a una empresa, sus administradores y sus liquidadores muchos años después de que la empresa haya dejado de existir. El TJUE resolvió que, en vista de la diversidad de posibles escenarios y de las diferencias en los periodos de limitación establecidos en cada uno de los Estados miembros, «en el estado actual resulta imposible identificar un plazo único desde la disolución de una sociedad a cuya expiración la inscripción de estos datos en el registro y su publicidad ya no sea necesaria». Debido al fin legítimo de la publicidad y a las dificultades para establecer un plazo al final del cual se pudieran suprimir los datos personales del registro sin perjudicar los intereses de terceros, el TJUE dictaminó que las normas de protección de datos de la UE no garantizan el derecho a la supresión de datos personales a las personas en la situación del Sr. Manni.

Cuando el responsable del tratamiento haya hecho públicos datos personales y reciba una solicitud de supresión de la información, el responsable estará obligado y deberá adoptar medidas «razonables» para comunicar la petición de supresión del interesado a otros responsables que traten los mismos datos. Las actividades del responsable del tratamiento deben tener en cuenta las tecnologías disponibles y el coste de su aplicación ([577]).

([577]) Reglamento general de protección de datos, artículo 17, apartado 2 y considerando 66.

6.1.4. Derecho a la limitación del tratamiento

El artículo 18 del RGPD permite a los interesados limitar temporalmente el tratamiento de sus datos personales por el responsable. Los interesados pueden solicitar al responsable que limite el tratamiento cuando:

- se haya impugnado la exactitud de los datos personales;
- el tratamiento sea ilícito y el interesado solicite que se limite el uso de los datos personales o que se supriman;
- los datos deban conservarse para el ejercicio o la defensa de reclamaciones;
- exista una resolución pendiente sobre si los intereses legítimos del responsable del tratamiento prevalecen sobre los intereses del interesado ([578]).

Entre los métodos que puede utilizar un responsable para limitar el tratamiento de datos personales cabe incluir, por ejemplo, los consistentes en trasladar temporalmente los datos a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos personales ([579]). El responsable debe informar al interesado antes de que se levante la limitación del tratamiento ([580]).

Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable debe comunicar cualquier rectificación o supresión de datos personales o cualquier limitación del tratamiento a cada uno de los destinatarios a quienes el responsable haya comunicado los datos personales, en la medida en que esto no sea ni imposible ni desproporcionado ([581]). Si el interesado solicita información acerca de los destinatarios, el responsable deberá facilitarle tal información ([582]).

([578]) Ibíd., artículo. 18 apartado 1.

([579]) Ibíd., considerando 67.

([580]) Ibíd., art. 18 apartado 3.

([581]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 81.

([582]) Reglamento general de protección de datos, artículo 19.

6.1.5. Derecho a la portabilidad de los datos

En virtud del RGPD, los interesados gozan del derecho a la portabilidad de sus datos en circunstancias en que los datos personales que hayan facilitado a un responsable sean objeto de tratamiento por medios automatizados o cuando el tratamiento de los datos personales sea necesario para cumplir un contrato y se lleve a cabo de forma automatizada. Esto significa que el derecho a la portabilidad de los datos no será de aplicación en situaciones en que el tratamiento de los datos personales tenga un fundamento jurídico que no sea el consentimiento o un contrato ([583]).

Si el derecho a la portabilidad de los datos es aplicable, los interesados tendrán derecho a que sus datos personales sean transmitidos directamente de un responsable a otro cuando esto sea técnicamente posible ([584]). Para facilitar esta operación, el responsable debe desarrollar formatos interoperables que permitan la portabilidad de los datos de los interesados ([585]). El RGPD especifica que estos formatos deben ser estructurados, de uso común y lectura mecánica, a fin de facilitar la interoperabilidad ([586]). La interoperabilidad puede definirse en sentido amplio como la capacidad de los sistemas de información para intercambiar datos y facilitar la puesta en común de información ([587]). Aunque la finalidad de los formatos utilizados es conseguir la interoperabilidad, el RGPD no impone recomendaciones concretas sobre el formato específico que se ha de facilitar: los formatos pueden ser diferentes según los sectores ([588]).

Según las directrices del Grupo de Trabajo del Artículo 29, el derecho a la portabilidad de los datos «respalda la elección, el control y la capacitación de los usuarios», con el fin de que los interesados tengan control sobre sus propios datos personales ([589]). Las directrices aclaran los principales elementos de la portabilidad de datos, que incluyen:

([583]) Ibíd., considerando 68 y artículo 20, apartado 1.

([584]) Ibíd., artículo 20, apartado 2.

([585]) Ibíd., considerando 68 y artículo 20, apartado 1.

([586]) Ibíd., considerando 68.

([587]) Comisión Europea, Comunicación sobre sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final, 2 de abril de 2016.

([588]) Grupo de Trabajo del Artículo 29 (2016), *Directrices sobre el derecho a la portabilidad de los datos*, WP 242, 13 de diciembre de 2016, revisadas el 5 de abril de 2017, p. 13.

([589]) Ibíd.

- el derecho de los interesados a recibir sus propios datos personales tratados por el responsable en un formato estructurado, de uso común, de lectura mecánica e interoperable;

- el derecho a transmitir datos personales de un responsable a otro sin limitaciones cuando esto sea técnicamente posible;

- el régimen de responsabilidad: cuando un responsable responda a una solicitud de portabilidad de los datos, actuará conforme a las instrucciones del interesado, lo que significa que no será responsable de que el destinatario cumpla la normativa de protección de datos, puesto que es el interesado quien decide a quién se portan los datos;

- el ejercicio del derecho a la portabilidad de los datos se entiende sin perjuicio de ningún otro derecho, como ocurre con todos los derechos recogidos en el RGPD.

6.1.6. Derecho de oposición

Los interesados pueden invocar su derecho de oposición al tratamiento de datos personales por razones relacionadas con su situación particular y datos tratados con fines de mercadotecnia directa. El derecho de oposición puede ejercerse por medios automatizados.

Derecho de oposición por motivos relacionados con la situación particular del interesado

Los interesados no tienen un derecho general de oposición al tratamiento de sus datos ([590]). El artículo 21, apartado 1, del RGPD da derecho al interesado a oponerse por motivos relacionados con su situación particular, cuando la base jurídica del tratamiento sea que el responsable realice una función en interés público o cuando el tratamiento esté basado en los intereses legítimos del responsable ([591]) El derecho

([590]) Véase también TEDH, *M.S. contra Suecia*, n.º 20837/92, 27 de agosto de 1997 [en el que se habían comunicado datos médicos sin consentimiento o sin posibilidad de oposición]; TEDH, *Leander contra Suecia*, n.º 9248/81, 26 de marzo de 1987; TEDH, *Mosley contra Reino Unido*, n.º 48009/08, 10 de mayo de 2011.

([591]) Reglamento general de protección de datos, considerando 69, artículo 6, apartado 1, letras e) y f).

de oposición se aplica a las actividades de elaboración de perfiles. Se ha reconocido un derecho similar en el Convenio 108 modernizado ([592]).

El derecho de oposición por motivos relacionados con la situación particular del interesado pretende alcanzar el equilibrio correcto entre los derechos de protección de datos del interesado y los derechos legítimos de otras personas en el tratamiento de sus datos. No obstante, el TJUE ha aclarado que los derechos del interesado prevalecen «con carácter general» sobre los intereses económicos del responsable del tratamiento en función de «la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información» ([593]). De acuerdo con el RGPD, la carga de la prueba recae en los responsables, que deben demostrar que existen motivos imperiosos para proseguir con el tratamiento ([594]). Del mismo modo, el Informe explicativo del Convenio 108 modernizado aclara que los motivos legítimos para el tratamiento de los datos (que pueden prevalecer sobre el derecho de oposición de los interesados) deberán demostrarse caso por caso ([595]).

Ejemplo: En *Manni* ([596]), el TJUE dictaminó que, debido a que la publicidad de los datos personales en el registro de sociedades perseguía un fin legítimo, en particular la necesidad de proteger los intereses de terceros y garantizar la seguridad jurídica, en principio, el Sr. Manni no tenía derecho a obtener la supresión de sus datos personales del registro de sociedades. Sin embargo, reconocía la existencia del derecho a oponerse al tratamiento, diciendo que «no es posible excluir que puedan existir situaciones particulares en las que razones preponderantes y legítimas propias de la situación concreta del interesado justifiquen excepcionalmente que el acceso a los datos personales

([592]) Convenio 108 modernizado, artículo 9, apartado 1, letra d); Recomendación sobre creación de perfiles, artículo 5, apartado 3.

([593]) TJUE, C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014, apartado 81.

([594]) Véase además Convenio 108 modernizado, artículo 8, apartado 1, letra d), que dice que el interesado puede oponerse al tratamiento de sus datos «salvo que el responsable demuestre razones legítimas para llevar a cabo el tratamiento que prevalezcan sobre sus intereses o derechos y libertades fundamentales».

([595]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 78.

([596]) TJUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 9 de marzo de 2017, apartados 47 y 60.

que les conciernen, inscritos en el registro, se limite, al expirar un plazo suficientemente largo [...] a los terceros que justifiquen un interés específico en su consulta».

El TJUE consideró que era responsabilidad de los órganos jurisdiccionales nacionales valorar cada caso, teniendo en cuenta todas las circunstancias pertinentes de la persona física y si existían razones preponderantes y legítimas que pudieran excepcionalmente justificar la limitación del acceso de terceros a los datos personales incluidos en los registros de sociedades. Sin embargo, aclaró que, en el caso del Sr. Manni, no cabía considerar que el mero hecho de que la publicidad de sus datos personales en el registro supuestamente afectase a su clientela constituyese una razón preponderante y legítima. Los clientes potenciales del Sr. Manni tienen un interés legítimo en la información relativa a la quiebra de su anterior empresa.

El efecto de una oposición admitida es que el responsable ya no puede tratar los datos en cuestión. Sin embargo, las operaciones de tratamiento efectuadas con los datos del interesado antes de la oposición seguirán siendo legítimas.

Derecho de oposición al tratamiento de los datos con fines de mercadotecnia directa

El artículo 21, apartado 2, del RGPD recoge específicamente el derecho a oponerse al uso de datos personales con fines de mercadotecnia directa, que aclara todavía más el artículo 13 de la Directiva sobre la privacidad y las comunicaciones electrónicas. Este derecho también está recogido en el Convenio 108 modernizado, así como en la Recomendación del CdE sobre mercadotecnia directa ([597]). El Informe explicativo del Convenio 108 modernizado aclara que la oposición al tratamiento de datos con fines de mercadotecnia directa debe acarrear la supresión o eliminación incondicional de los datos personales en cuestión ([598]).

El interesado tiene derecho a oponerse al uso de sus datos personales con fines de mercadotecnia directa en cualquier momento y sin cargo alguno. Los interesados

([597]) Consejo de Europa, Comité de Ministros (1985), *Recommendation Rec(85)20 to Member States on the protection of personal data used for the purposes of direct marketing*, 25 de octubre de 1985, artículo 4, apartado 1.

([598]) Informe explicativo del Convenio 108 modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 79.

deben ser informados de este derecho de manera clara e independiente de cualquier otra información.

Derecho de oposición por medios automatizados

Cuando la información personal se utiliza y se trata en relación con servicios de la sociedad de la información, el interesado puede ejercer su derecho a oponerse al tratamiento de sus datos personales por medios automatizados.

Los servicios de la sociedad de la información se definen como todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios ([599]).

Los responsables del tratamiento que ofrecen servicios de la sociedad de la información deben adoptar medidas técnicas y procedimientos adecuados para garantizar que el derecho de oposición por medios automatizados pueda ejercerse de manera efectiva ([600]). Por ejemplo, esto puede hacerse bloqueando las cookies en las páginas web o desactivando el rastreo dela navegación por internet.

Derecho de oposición para fines de investigación científica o histórica o para fines estadísticos

En el Derecho de la UE, la investigación científica debe interpretarse en un sentido amplio, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado ([601]). La investigación histórica también incluye la investigación para fines genealógicos, teniendo en cuenta que el Reglamento no es de aplicación a personas fallecidas ([602]). Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos ([603]). Una vez más, la situación concreta del interesado es la base jurídica del derecho de oposición al tratamiento

([599]) Directiva 98/34/CE en su versión modificada por la Directiva 98/48/CE por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas, artículo 1, apartado 2.

([600]) Reglamento general de protección de datos, artículo 21, apartado 5.

([601]) Ibíd., considerando 159.

([602]) Ibíd., considerando 160.

([603]) Ibíd., considerando 162.

de datos personales con fines de investigación ([604]). La única excepción es que el tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público. Sin embargo, el derecho de supresión no es aplicable si el tratamiento es necesario (con o sin razones de interés público) para fines de investigación científica o histórica o para fines estadísticos ([605]).

El RGPD pondera los requisitos de la investigación científica, estadística o histórica y los derechos de los interesados con garantías y excepciones específicas en el artículo 89. De este modo, el Derecho de la Unión o de los Estados miembros puede establecer excepciones al derecho de oposición en la medida en que dicho derecho pueda imposibilitar u obstaculizar gravemente el logro de los fines científicos, y si dichas excepciones son necesarias para alcanzar esos fines.

En el **Derecho del CdE**, el artículo 9, apartado 2 del Convenio 108 modernizado establece que la ley podrá establecer limitaciones a los derechos de los interesados, incluido el derecho de oposición, en relación con el tratamiento de datos con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos cuando no exista riesgo reconocible de violación de los derechos y libertades fundamentales de los interesados.

Sin embargo, el Informe explicativo (apartado 41) reconoce asimismo que los interesados deben tener la oportunidad de dar su consentimiento únicamente a determinadas áreas de investigación o partes de proyectos de investigación en la medida en que el fin previsto lo permita, y oponerse en caso de que perciban que el tratamiento invade en exceso sus derechos y libertades sin un motivo legítimo.

En otras palabras, dicho tratamiento se consideraría por tanto compatible *a priori* siempre que existan otras garantías y que las operaciones, en principio, excluyan cualquier uso de la información obtenida para adoptar decisiones o medidas en relación con una persona concreta.

6.1.7. Decisiones individuales automatizadas, incluida la elaboración de perfiles

Las decisiones automatizadas son decisiones adoptadas mediante el uso de datos personales tratados únicamente mediante procedimientos automatizados, sin

([604]) Ibíd., artículo 21, apartado 6.

([605]) Ibíd., artículo 17, apartado 3, letra d).

intervención humana. **En el Derecho de la UE**, los interesados no deben ser objeto de decisiones automatizadas que surtan efectos legales o tengan efectos de similar importancia. Si es posible que dichas decisiones tengan un impacto significativo en las vidas de las personas físicas a las que conciernen puesto que, por ejemplo, hacen referencia a la solvencia, la contratación en red, el rendimiento profesional, el análisis de la conducta o la fiabilidad, será necesario establecer una protección especial para evitar consecuencias negativas. Las decisiones automatizadas incluyen la elaboración de perfiles, que consiste en cualquier forma de evaluación automática de «aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos» ([606]).

Ejemplo: Para valorar rápidamente la solvencia de un futuro cliente, las agencias de referencia de crédito recopilan determinados datos, por ejemplo, cómo ha mantenido el cliente sus cuentas de crédito o servicios públicos, los detalles de los domicilios anteriores del cliente, así como información de fuentes públicas, como el censo electoral, registros públicos (incluidas sentencias judiciales) o datos de quiebra o insolvencia. Estos datos personales se incorporan automáticamente a un algoritmo de calificación, que calcula el valor total que representa la solvencia del cliente potencial.

De acuerdo con el Grupo de Trabajo del Artículo 29, el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado que pueda surtir efectos jurídicos para el interesado o que le afecten de forma significativa equivale a una prohibición general y no requiere que el interesado realice una oposición proactiva a tal decisión ([607]).

No obstante, de acuerdo con el RGPD, las decisiones automatizadas con efectos jurídicos que afecten significativamente a las personas físicas pueden ser aceptables si son necesarias para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, o si el interesado ha dado su consentimiento explícito. Además, las decisiones automatizadas son aceptables si están autorizadas

([606]) Ibíd., considerando 71, artículo 4, apartado 4 y artículo 22.

([607]) Grupo de Trabajo del Artículo 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 de octubre de 2017, p. 15.

por la ley si se salvaguardan debidamente los derechos, libertades e intereses legítimos del interesado ([608]).

El RGPD también establece que entre las obligaciones del responsable con respecto a la información que ha de facilitar cuando recoge datos personales, los interesados deben ser informados acerca de la existencia de las decisiones automatizadas, incluida la elaboración de perfiles ([609]). El derecho de acceso a los datos personales tratados por el responsable permanece inalterado ([610]). Esta información no solo debe incluir el hecho de que se va a producir la elaboración de perfiles, sino que además debe contener información significativa sobre la lógica aplicada en la elaboración de perfiles y las consecuencias previstas del tratamiento para el interesado ([611]). Por ejemplo, una compañía de seguros de enfermedad que tome decisiones automatizadas sobre las solicitudes deberá facilitar a los interesados información general sobre el funcionamiento del algoritmo y qué factores utiliza este para calcular las primas de sus seguros. Del mismo modo, en el ejercicio de su «derecho de acceso», los interesados pueden solicitar al responsable información sobre la existencia de decisiones automatizadas e información significativa sobre la lógica aplicada ([612]).

La información facilitada a los interesados tiene como finalidad la transparencia y que los interesados puedan otorgar un consentimiento informado, si es el caso, o bien obtener intervención humana. El responsable del tratamiento está obligado a aplicar medidas adecuadas para salvaguardar los derechos, libertades e intereses legítimos del interesado. Esto incluye al menos el derecho a obtener intervención humana por parte del responsable y la posibilidad de que el interesado exprese sus puntos de vista e impugne la decisión basándose en el tratamiento automatizado de sus datos personales ([613]).

El Grupo de Trabajo del Artículo 29 ha formulado orientaciones adicionales sobre el uso de las decisiones automatizadas en virtud del RGPD ([614]).

([608]) Reglamento general de protección de datos, artículo 22, apartado 2.

([609]) Ibíd., artículo 12.

([610]) Ibíd., artículo 15.

([611]) Ibíd., artículo 13, apartado 2, letra f).

([612]) Ibíd., artículo 15, apartado 1, letra h).

([613]) Ibíd., art. 22 apartado 3.

([614]) Grupo de Trabajo del Artículo 29 (2017), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, 3 de octubre de 2017.

En el Derecho del CdE, las personas físicas tienen derecho a no ser objeto de una decisión que les afecte de forma significativa y que esté basada exclusivamente en el tratamiento automatizado sin tener en cuenta sus puntos de vista ([615]). El requisito de tener en cuenta los puntos de vista del interesado cuando las decisiones se basen exclusivamente en un tratamiento automatizado implica que tiene derecho a impugnar dichas decisiones y debe poder impugnar cualquier imprecisión en los datos personales utilizados por el responsable, así como poner en duda la pertinencia de cualquier perfil que se le aplique ([616]). Sin embargo, el interesado no podrá ejercer este derecho si la decisión automatizada está autorizada por una ley a la que esté sometido el responsable y que también establezca medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado. Además, los interesados tienen derecho a conocer, previa solicitud, los motivos que justifican el tratamiento de datos llevado a cabo ([617]). El Informe explicativo del Convenio 108 modernizado ofrece el ejemplo de la calificación crediticia. Las personas físicas deben tener derecho a conocer no solo la propia decisión de calificación positiva o negativa, sino también la *lógica* aplicada al tratamiento de sus datos personales que ha dado lugar a tal decisión. «Conocer estos elementos contribuye al ejercicio efectivo de otras salvaguardias esenciales como el derecho de oposición y el derecho de reclamación ante una autoridad competente» ([618]).

La Recomendación sobre creación de perfiles, aunque no es legalmente vinculante, especifica las condiciones para la recogida y el tratamiento de datos personales en el contexto de la elaboración de perfiles ([619]). Incluye disposiciones sobre la necesidad de garantizar que el tratamiento, en el contexto de la creación de perfiles, sea leal, lícito, proporcionado y para fines específicos y legítimos. También incluye disposiciones sobre la información que los responsables del tratamiento deben facilitar a los interesados. El principio de calidad de los datos —que obliga a los responsables a adoptar medidas para corregir los factores de inexactitud, limitar los riesgos o errores que puede conllevar la elaboración de perfiles y evaluar periódicamente la calidad de los datos y algoritmos utilizados— también aparece en la Recomendación.

([615]) Convenio 108 modernizado, artículo 9, apartado 1, letra a).

([616]) Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 75.

([617]) Convenio 108 modernizado, artículo 9, apartado 1, letra c).

([618]) Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 77.

([619]) Consejo de Europa, Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, artículo 5, apartado 5.

6.2. Recursos, responsabilidad, sanciones e indemnización

Puntos clave

- De acuerdo con el Convenio 108 modernizado, el Derecho nacional de las Partes Contratantes debe establecer recursos y sanciones apropiados contra las violaciones del derecho a la protección de datos.
- En la UE, el RGPD establece recursos para los interesados en casos de violación de sus derechos, así como sanciones contra los responsables y encargados del tratamiento que no cumplan las disposiciones del Reglamento. También contempla el derecho a indemnización y responsabilidad.
  - Los interesados tienen derecho a presentar una reclamación ante una autoridad de control por presuntas infracciones del Reglamento, así como el derecho a la tutela judicial efectiva y a recibir indemnización.
  - En el ejercicio de su derecho a la tutela judicial efectiva, las personas físicas pueden ser representadas por organizaciones sin ánimo de lucro activas en el campo de la protección de datos.
  - El responsable o encargado es responsable de cualquier daño material o inmaterial derivado de la infracción.
  - Las autoridades de control están facultadas para imponer multas administrativas por infracciones del Reglamento de hasta 20 000 000 EUR o, tratándose de una empresa, del 4 % del volumen de negocio total anual global, optándose por la de mayor cuantía.
- Los interesados podrán, como último recurso y en determinadas circunstancias, interponer un recurso contra las violaciones de la legislación en materia de protección de datos ante el TEDH.
- Toda persona física o jurídica tiene derecho a interponer un recurso de anulación de las decisiones del Comité Europeo de Protección de Datos ante el TJUE, en las condiciones previstas en los Tratados.

Adoptar instrumentos jurídicos no es suficiente para garantizar la protección de los datos personales en Europa. Para que la normativa europea de protección de datos sea efectiva, es necesario establecer mecanismos que permitan a las personas físicas oponerse a la violación de sus derechos y reclamar indemnizaciones por los daños y perjuicios que puedan haber sufrido. También es importante que las

autoridades de control tengan poder para imponer sanciones que sean efectivas, disuasorias y proporcionadas a la infracción en cuestión.

Los derechos garantizados por la legislación en materia de protección de datos podrán ser ejercidos únicamente por las personas cuyos derechos estén en juego; es decir, los interesados. Sin embargo, los interesados podrán estar representados por otras personas —que cumplan los requisitos establecidos por el Derecho nacional— para ejercer sus derechos. En algunas legislaciones nacionales, los niños y las personas con discapacidad intelectual deben estar representados por sus tutores ([620]). La legislación de la UE sobre protección de datos contempla que los interesados puedan estar representados por una asociación —cuyo fin lícito sea proteger los derechos en materia de protección de datos— ante una autoridad de control o un órgano jurisdiccional ([621]).

6.2.1. Derecho a presentar una reclamación ante una autoridad de control

Tanto en el **Derecho del CdE** como en el **Derecho de la UE**, las personas físicas tienen derecho a presentar solicitudes y reclamaciones a la autoridad de control competente si consideran que el tratamiento de sus datos personales no se está efectuando con arreglo a la ley.

El Convenio 108 modernizado reconoce el derecho de los interesados a contar con la ayuda de una autoridad de control en el ejercicio de sus derechos con arreglo al Convenio, sea cual sea su nacionalidad o residencia ([622]). Las peticiones de ayuda solo podrán denegarse en circunstancias excepcionales y los costes y tasas relacionados con la ayuda no deberán ser sufragados por los interesados ([623])

En el ordenamiento jurídico de la UE existen disposiciones similares. El RGPD requiere que las autoridades de control adopten medidas para facilitar la presentación de reclamaciones, por ejemplo mediante la creación de un formulario de presentación

([620]) FRA (2015), *Manual de legislación europea sobre los derechos del niño*, Luxemburgo, Oficina de Publicaciones; FRA (2013), *Capacidad jurídica de las personas con discapacidad intelectual y de las personas con trastornos de salud mental*, Luxemburgo, Oficina de Publicaciones.

([621]) Reglamento general de protección de datos, artículo 80.

([622]) Convenio 108 modernizado, artículo 18.

([623]) Ibíd., artículos 16-17.

de reclamaciones por medios electrónicos ([624]). El interesado puede presentar la reclamación ante la autoridad de control del Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción ([625]). Las reclamaciones deben ser investigadas y la autoridad de control debe informar al reclamante sobre el curso y el resultado de la reclamación ([626]).

Las posibles infracciones cometidas por instituciones u órganos de la UE pueden ponerse en conocimiento del Supervisor Europeo de Protección de Datos ([627]). Si el SEPD no responde en un plazo de seis meses, la reclamación se considerará desestimada. Contra las decisiones del SEPD se pueden interponer recursos ante el TJUE en el marco del Reglamento (CE) n.º 45/2001, que obliga a las instituciones y los órganos de la UE a cumplir con la normativa de protección de datos.

Debe existir posibilidad de recurrir las decisiones de una autoridad de control nacional ante los órganos jurisdiccionales. Esto se aplica tanto a los interesados como a los responsables y encargados del tratamiento que hayan participado en el procedimiento ante una autoridad de control.

Ejemplo: En septiembre de 2017, la Agencia Española de Protección de Datos multó a Facebook por violar varias normas de protección de datos. La autoridad de control condenó a la red social por recoger, conservar y tratar datos personales —incluso datos personales de categorías especiales— con fines publicitarios y sin obtener el consentimiento de los interesados. La decisión fue el resultado de una investigación realizada por iniciativa propia de la autoridad de control.

6.2.2. Derecho a la tutela judicial efectiva

Además del derecho a reclamar ante la autoridad de control, las personas físicas deben tener derecho a la tutela judicial efectiva y a exponer su caso ante un órgano jurisdiccional. El derecho a un recurso jurídico está totalmente consagrado en la tradición jurídica europea y reconocido como derecho fundamental, tanto en el

([624]) Reglamento general de protección de datos, artículo 57, apartado 2.

([625]) Ibíd., artículo. 77 apartado 1.

([626]) Ibíd., artículo 77, apartado 2.

([627]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO 2001 L 8.

artículo 47 de la Carta de los Derechos Fundamentales de la Unión Europea como en el artículo 13 del CEDH ([628]).

En el Derecho de la UE, la importancia de que los interesados dispongan de recursos jurídicos efectivos en caso de violación de sus derechos queda clara tanto en las disposiciones del RGPD —que establece el derecho a la tutela judicial efectiva contra las autoridades de control y los responsables y encargados del tratamiento— como en la jurisprudencia del TJUE.

Ejemplo: En *Schrems* ([629]) el TJUE declaró inválida la decisión de adecuación de puerto seguro. Esa decisión había permitido las transferencias de datos internacionales desde la UE hasta organizaciones radicadas en los EE. UU. que se habían autocertificado conforme al régimen de puerto seguro. El TJUE consideró que el régimen de puerto seguro tenía varias deficiencias que comprometían los derechos fundamentales de los ciudadanos de la Unión a la protección de la vida privada y los datos personales, así como el derecho a una tutela judicial efectiva.

En relación con la violación de los derechos a la vida privada y la protección de datos, el TJUE resaltó que la legislación estadounidense permitía que determinadas autoridades públicas tuvieran acceso a los datos personales transferidos desde los Estados miembros a los EE. UU. y los tratasen de una manera incompatible con los fines originales de la transferencia y más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional. Sobre el derecho a la tutela judicial efectiva, señaló que los interesados no disponían de ningún medio administrativo o judicial de recurso para conseguir el acceso a los datos que les concernían y su rectificación o supresión, según procediera. El TJUE concluyó que una legislación que no ofrece ninguna posibilidad de interponer recursos jurídicos de acceso, rectificación o supresión de sus datos personales «no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta». Puso de relieve que la existencia de un recurso judicial que garantice el cumplimiento de la legalidad es inherente a la existencia de un Estado de Derecho.

([628]) Véase por ejemplo TEDH, *Karabeyoğlu contra Turquía*, n.º 30083/10, 7 de junio de 2016; TEDH, *Mustafa Sezgin Tanrıkulu contra Turquía*, n.º 27473/06, 18 de julio de 2017.

([629]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015.

Las personas físicas, los responsables o los encargados que deseen impugnar una decisión jurídicamente vinculante de una autoridad de control tienen derecho a ejercitar acciones ante un órgano jurisdiccional ([630]). El término «decisión» deberá interpretarse en un sentido amplio, que comprenda el ejercicio de las competencias de investigación, sanción y autorización de las autoridades de control, así como las decisiones de desestimar o denegar una reclamación. Sin embargo, las medidas que no sean jurídicamente vinculantes, como los dictámenes publicados por las autoridades de control o el asesoramiento que estas presten, no pueden formar parte del objeto de una acción ejercitada ante un órgano jurisdiccional ([631]). La acción debe ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control de que se trate ([632]).

Cuando el responsable o encargado vulnere los derechos de un interesado, este tendrá derecho a reclamar ante un tribunal ([633]). En los procedimientos incoados contra un responsable o encargado del tratamiento, es especialmente importante que se dé a los interesados la opción de elegir dónde interponer la demanda. Puede optar por hacerlo en el Estado miembro en el que el responsable o el encargado tengan un establecimiento o en el Estado miembro en el que el interesado en cuestión tenga su residencia habitual ([634]). La segunda posibilidad facilita mucho a las personas físicas el ejercicio de sus derechos, ya que les permite ejercitar acciones en el Estado en el que residen y en una jurisdicción conocida. El hecho de limitar la jurisdicción de los procedimientos contra responsables y encargados del tratamiento al Estado miembro en el que estos últimos tengan un establecimiento podría disuadir a los interesados residentes en otros Estados miembros de ejercitar una acción judicial, ya que implicaría desplazamientos y otros costes, y el procedimiento podría llevarse a cabo en una jurisdicción y una lengua extranjeras. La única excepción se refiere a los casos en que el responsable o el encargado sean autoridades públicas y el tratamiento se haya efectuado en el ejercicio de sus poderes públicos. En este caso, solo los órganos jurisdiccionales del Estado de la autoridad pública de que se trate serán competentes para conocer la reclamación ([635]).

([630]) Reglamento general de protección de datos, artículo 78.

([631]) Ibíd., considerando 143.

([632]) Ibíd., artículo 78, apartado 3.

([633]) Ibíd., artículo 79.

([634]) Ibíd., artículo 79, apartado 2.

([635]) Ibíd.

Aunque los casos relativos a las normas de protección de datos se decidirán casi siempre en los órganos jurisdiccionales de los Estados miembros, algunos casos pueden llevarse al TJUE. La primera posibilidad es cuando un interesado, un responsable, un encargado o una autoridad de control solicite la anulación de una decisión del CEPD. Sin embargo, esta acción está sujeta a las condiciones del artículo 263 del TFUE, de modo que, para que pueda admitirse a trámite, estas personas físicas y entidades deben demostrar que la decisión del Comité les afecta de forma directa e individual.

La segunda posibilidad se refiere a aquellos casos en que instituciones u organismos de la UE realicen un tratamiento ilícito de datos personales. Cuando las instituciones de la UE vulneren la legislación sobre protección de datos, los interesados podrán presentar una reclamación directamente ante el Tribunal General de la UE (que forma parte del TJUE). El Tribunal General es competente, en primera instancia, para conocer reclamaciones sobre infracciones de la legislación de la UE por parte de instituciones de la UE. De este modo, las reclamaciones contra el SEPD —que también es una institución de la UE— pueden presentarse igualmente ante el Tribunal General ([636]).

Ejemplo: En *Bavarian Lager* ([637]), la empresa solicitó a la Comisión Europea acceso al acta completa de una reunión que había celebrado la Comisión, en la que presuntamente se habían tratado cuestiones legales que afectaban a la empresa. La Comisión rechazó la petición de acceso de la empresa alegando intereses superiores de protección de datos ([638]). Bavarian Lager, con arreglo al artículo 32 del Reglamento de protección de datos de las instituciones de la UE, interpuso un recurso contra esa decisión ante el Tribunal de Primera Instancia (el paso previo al Tribunal General). En su resolución (asunto T-194/04, *The Bavarian Lager Co. Ltd contra Comisión de las Comunidades Europeas*), el Tribunal de Primera Instancia anuló la decisión de la Comisión de denegar la solicitud de acceso. La Comisión Europea recurrió esta resolución ante el TJUE.

([636]) Reglamento (CE) n.º 45/2001, artículo 32, apartado 3.

([637]) TJUE, C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd* [GS], 2010.

([638]) Véase un análisis de la argumentación en SEPD (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bruselas, SEPD.

El TJUE dictó sentencia (en la Gran Sala) para anular la sentencia del Tribunal de Primera Instancia y confirmar la denegación por parte de la Comisión Europea de la petición de acceso al acta completa de la reunión, a fin de proteger los datos personales de las personas presentes en dicha reunión. El TJUE consideró que la Comisión había actuado correctamente al negarse a revelar esa información, puesto que los participantes no habían dado su consentimiento para la difusión de sus datos personales. Además, Bavarian Lager no había demostrado la necesidad de obtener acceso a dicha información.

Por último, los interesados, las autoridades de control y los responsables o encargados del tratamiento pueden solicitar al órgano jurisdiccional nacional, en el curso de un procedimiento nacional, que solicite al TJUE aclaración sobre la interpretación y validez de los actos de instituciones, organismos, oficinas o agencias de la UE. Dichas aclaraciones se conocen como decisiones prejudiciales. Estas decisiones no son un recurso directo para el reclamante, pero permiten a los órganos jurisdiccionales nacionales asegurarse de que aplican una interpretación correcta del Derecho de la UE. A través de este mecanismo de las decisiones prejudiciales llegaron al TJUE algunos casos históricos —como *Digital Rights Ireland* y *Kärntner Landesregierung y otros* ([639]) o *Schrems* ([640])— que influyeron enormemente en el desarrollo de la legislación de la UE en materia de protección de datos.

Ejemplo: *Digital Rights Ireland* y *Kärntner Landesregierung y otros* ([641]) fueron asuntos acumulados presentados por la High Court de Irlanda y el Tribunal Constitucional de Austria en relación con la conformidad de la Directiva 2006/24/CE (Directiva sobre conservación de datos) con la legislación de la UE en materia de protección de datos. El Tribunal Constitucional austriaco preguntó al TJUE por la validez de los artículos 3 a 9 de la Directiva 2006/24/CE a la luz de los artículos 7, 9 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea. También preguntaba si determinadas disposiciones de la Ley federal de telecomunicaciones de Austria por la que

([639]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros* y *Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.

([640]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015.

([641]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.

se transponía la Directiva sobre conservación de datos eran incompatibles con algunos aspectos de la antigua Directiva sobre protección de datos y el Reglamento de protección de datos de las instituciones de la UE.

En el asunto de *Kärntner Landesregierung y otros,* el Sr. Seitlinger —uno de los demandantes en el procedimiento ante el Tribunal Constitucional— sostenía que él utilizaba el teléfono, internet y el correo electrónico tanto con fines laborales como en su vida privada. En consecuencia, la información que enviaba y recibía pasaba a través de redes de telecomunicaciones públicas. Con arreglo a lo dispuesto en la Ley austriaca de telecomunicaciones de 2003, su proveedor de servicios de telecomunicaciones estaba obligado legalmente a recoger y conservar datos sobre el uso que él hacía de la red. El Sr. Seitlinger creía que no era necesario recoger y conservar sus datos personales para los fines técnicos del envío y recepción de información a través de la red. Y que tampoco era necesario recoger y conservar dichos datos con fines de facturación. El Sr. Seitlinger declaró que él no había autorizado este uso de sus datos personales, cuya recogida y conservación se efectuaba exclusivamente a raíz de la Ley austriaca de telecomunicaciones de 2003.

Por tanto, el Sr. Seitlinger interpuso un recurso ante el Tribunal Constitucional austriaco en el que alegaba que las obligaciones legales de su proveedor de telecomunicaciones violaban sus derechos fundamentales, con arreglo a lo dispuesto en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Puesto que la legislación austriaca aplicaba el Derecho de la Unión (la Directiva de conservación de datos entonces vigente), el Tribunal Constitucional austriaco remitió la cuestión al TJUE para que resolviese si la Directiva era compatible con los derechos a la privacidad y a la protección de datos consagrados en la Carta de los Derechos Fundamentales de la Unión Europea.

La Gran Sala del TJUE dictó sentencia sobre el asunto, que dio lugar a la anulación de la Directiva de la UE sobre conservación de datos. El TJUE dictaminó que dicha Directiva suponía una injerencia especialmente grave en los derechos fundamentales a la privacidad y a la protección de datos, sin que dicha injerencia se limitase a lo que fuera estrictamente necesario. La Directiva perseguía un fin legítimo, ya que permitía que las autoridades nacionales tuvieran oportunidades adicionales de investigar y perseguir delitos graves y era, por tanto, un instrumento valioso para las investigaciones penales. Sin embargo, el TJUE observó que las limitaciones

de los derechos fundamentales únicamente debían aplicarse cuando fueran estrictamente necesarias y debían ir acompañadas de normas claras y precisas respecto de su ámbito de aplicación, así como de garantías para las personas físicas.

Según el TJUE, la Directiva no cumplía este criterio de necesidad. En primer lugar, no establecía normas claras y precisas que limitasen el alcance de la injerencia. En lugar de exigir una relación entre los datos conservados y un delito grave, la Directiva se aplicaba a todos los metadatos de todos los usuarios de todos los medios de comunicación electrónica. Constituía, por lo tanto, una injerencia en los derechos a la privacidad y a la protección de datos de prácticamente toda la población de la UE, lo cual podía considerarse desproporcionado. No contenía condiciones que limitasen las personas autorizadas para obtener acceso a los datos personales, ni se sometía dicho acceso a condiciones procedimentales, como el requisito de contar con la aprobación de una autoridad administrativa o de un órgano jurisdiccional antes de obtener acceso. Por último, la Directiva no establecía garantías claras para la protección de los datos conservados. Por consiguiente, no garantizaba la protección efectiva de los datos contra el riesgo de abuso ni contra posibles accesos y usos ilícitos de los datos ([642]).

En principio, el TJUE debe contestar a las cuestiones que se le remiten y no puede negarse a adoptar una decisión prejudicial alegando que esta no sería pertinente ni oportuna al respecto del asunto original. Sin embargo, sí puede negarse si la cuestión no entra dentro de su ámbito de competencias ([643]). El TJUE adopta sus resoluciones únicamente en relación con los elementos constitutivos de la petición de decisión prejudicial, mientras que el órgano jurisdiccional nacional sigue siendo el competente para resolver el litigio original ([644]).

En el Derecho del CdE, las Partes Contratantes deben establecer recursos judiciales y no judiciales adecuados en relación con las violaciones de las disposiciones del

([642]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros* [GS], 8 de abril de 2014, apartado 69.

([643]) TJUE, C-244/80, *Pasquale Foglia contra Mariella Novello* (n.º 2), 16 de diciembre de 1981; TJUE, C-467/04, *Procedimiento penal entablado contra Gasparini y otros*, 28 de septiembre de 2006.

([644]) TJUE, C-438/05, *International Transport Workers' Federation y Finnish Seamen's Union contra Viking Line ABP y OÜ Viking Line Eesti* [GS], 11 de diciembre de 2007, apartado 85.

Convenio 108 modernizado ([645]). Además, se pueden presentar ante el TEDH denuncias de violaciones de los derechos de protección de datos que contravengan el artículo 8 del CEDH contra una Parte Contratante del CEDH una vez agotados todos los recursos disponibles en el ámbito nacional. Un alegato de violación del artículo 8 del CEDH ante el TEDH también debe cumplir otros criterios de admisibilidad (artículos 34 y 35 del CEDH) ([646]).

Aunque las demandas al TEDH pueden ir dirigidas únicamente contra las Partes Contratantes, también pueden tratar indirectamente de acciones u omisiones de particulares, en la medida en que la Parte Contratante no haya cumplido con sus obligaciones positivas con arreglo al CEDH y no haya previsto una protección suficiente contra las infracciones de los derechos de protección de datos recogidos en su Derecho nacional.

Ejemplo: En *K.U. contra Finlandia* ([647]), el demandante, menor de edad, denunció que se había publicado un anuncio de carácter sexual sobre su persona en un sitio de citas por internet. El proveedor del servicio no reveló la identidad de la persona que había publicado esa información debido a las obligaciones de confidencialidad que establecía la ley finlandesa. El demandante alegó que la legislación finlandesa no establecía una protección suficiente contra las actuaciones del particular que publicó datos incriminatorios acerca de su persona en internet. El TEDH resolvió que los Estados no solo estaban obligados a abstenerse de injerencias arbitrarias en la vida privada de las personas físicas, sino que además pueden estar sometidos a obligaciones positivas que impliquen «la adopción de medidas diseñadas para garantizar el respeto a la vida privada incluso en el ámbito de las relaciones entre los propios individuos». En el caso del demandante, su protección práctica y efectiva exigía que se adoptaran medidas eficaces para identificar y enjuiciar al autor. Sin embargo, el Estado no había proporcionado dicha protección y el Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

([645]) Convenio 108 modernizado, artículo 12.

([646]) CEDH, artículos 34-37.

([647]) TEDH, *K.U. contra Finlandia*, n.º 2872/02, 2 de diciembre de 2008.

Ejemplo: En *Köpke contra Alemania* ([648]), la demandante había sido sospechosa de hurto en su lugar de trabajo y había sido objeto de videovigilancia encubierta. El TEDH concluyó que «nada indicaba que las autoridades internas no hubieran realizado una ponderación equilibrada, dentro de su margen de apreciación, entre el derecho al respeto a la vida privada de la demandante con arreglo al artículo 8 y el interés de su empleador en proteger sus derechos de propiedad y el interés público en la buena administración de la justicia». La demanda, por tanto, fue declarada inadmisible.

Si el TEDH dictamina que una Parte Contratante ha violado alguno de los derechos protegidos por el CEDH, dicha Parte Contratante estará obligada a ejecutar la sentencia del TEDH (artículo 46 del CEDH). Las medidas de ejecución deberán, en primer lugar, poner fin a la violación y subsanar, en la medida de lo posible, las consecuencias negativas que haya tenido para el demandante. La ejecución de sentencias también puede exigir la adopción de medidas generales que eviten violaciones similares a las observadas por el Tribunal, ya sea a través de cambios en la legislación, de la jurisprudencia o de otras medidas.

Cuando el TEDH considere que ha existido una violación del CEDH, el artículo 41 del CEDH establece que podrá conceder al demandante una «satisfacción equitativa» a expensas de la Parte Contratante.

Derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro

El RGPD autoriza a las personas físicas que presenten una reclamación ante una autoridad de control o que ejerciten una acción judicial ante un órgano jurisdiccional a dar mandato a una entidad, organización o asociación sin ánimo de lucro para que les represente ([649]). Estas entidades sin ánimo de lucro deben tener objetivos estatutarios que entren en la esfera del interés público y tener actividad en el ámbito de la protección de datos. Dichas entidades podrán presentar la reclamación o ejercitar el derecho al recurso judicial en nombre de los interesados. El Reglamento ofrece a los Estados miembros la opción de decidir —de acuerdo con su Derecho nacional— si una entidad puede presentar reclamaciones en nombre de los interesados sin haber recibido el mandato de dichos interesados.

([648]) TEDH, *Köpke contra Alemania* (dic.), n.º 420/07, 5 de octubre de 2010.

([649]) Reglamento general de protección de datos, artículo 80.

Este derecho de representación permite a las personas físicas beneficiarse de los conocimientos y la capacidad organizativa y financiera de dichas entidades sin ánimo de lucro, con lo que se les facilita enormemente el ejercicio de sus derechos. El RGPD permite que estas entidades presenten demandas colectivas en nombres de multitud de interesados. Esto también es beneficioso para el funcionamiento y la eficiencia del sistema judicial, ya que las demandas similares se agrupan y se examinan de forma conjunta.

6.2.3. Responsabilidad y derecho a indemnización

El derecho a la tutela judicial efectiva debe facultar a las personas físicas para reclamar indemnizaciones por los daños y perjuicios que hayan sufrido a consecuencia del tratamiento de sus datos personales de manera que se infrinja la legislación aplicable. La responsabilidad de los responsables y de los encargados por un tratamiento ilícito está expresamente reconocida en el RGPD ([650]). El Reglamente reconoce a las personas físicas el derecho a recibir una indemnización del responsable o del encargado del tratamiento por daños y perjuicios materiales o inmateriales, mientras que en sus considerandos se establece que «[e]l concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento» ([651]). Los responsables del tratamiento deben responder y pueden tener que hacer frente a reclamaciones de indemnización por los daños y perjuicios causados si no cumplen sus obligaciones de conformidad con el Reglamento. Los encargados del tratamiento de datos personales deben responder de los daños y perjuicios causados por el tratamiento únicamente cuando no hayan cumplido las obligaciones del Reglamento dirigidas específicamente a los encargados, o cuando hayan actuado al margen o en contra de las instrucciones legales del responsable. Cuando un responsable o encargado haya pagado una indemnización en su integridad, el RGPD establece que el responsable o encargado podrá reclamar a los demás responsables o encargados que hayan participado en la misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados ([652]). Al mismo tiempo, las excepciones de la responsabilidad son muy estrictas y requieren que se aporten pruebas de que el responsable o encargado no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

([650]) Ibíd., artículo 82.

([651]) Ibíd., considerando 146.

([652]) Ibíd., artículo 82, apartados 2 y 5.

La indemnización debe ser «total y efectiva» en relación con los daños y perjuicios sufridos. Cuando los daños sean causados por operaciones de tratamiento realizadas por varios responsables y encargados, cada responsable o encargado deberá responder de la totalidad de los daños. Esta disposición tiene por objeto garantizar que los interesados obtengan una indemnización efectiva y que los responsables y encargados participantes en actividades de tratamiento actúen de forma coordinada.

Ejemplo: Los interesados no están obligados a ejercitar acciones legales para reclamar una indemnización a todas las entidades responsables de los daños y perjuicios, ya que esto podría dar lugar a un procedimiento costoso y prolongado. Basta con ejercitar la acción contra uno de los corresponsables, que podrá entonces tener que responder de la totalidad de los daños. En estos casos, el responsable o encargado que pague los daños tendrá después derecho a reclamar al resto de entidades que hayan participado en el tratamiento y sean responsables de la violación la parte de la cuantía pagada correspondiente a su grado de responsabilidad en los daños. Estos procedimientos entre los distintos corresponsables y encargados del tratamiento tienen lugar después de que el interesado ha recibido la indemnización y el interesado no participa en ellos.

En el marco jurídico del CdE, el artículo 12 del Convenio 108 modernizado exige que las Partes Contratantes establezcan recursos apropiados para las violaciones de la legislación nacional que aplique los requisitos del Convenio. El Informe explicativo del Convenio 108 modernizado indica que estos recursos deben incluir la posibilidad de impugnar judicialmente una decisión o práctica, aunque también deben existir recursos extrajudiciales ([653]). Las modalidades de estos recursos y las diferentes normas relativas al acceso a ellos, junto con el procedimiento que se ha de seguir, quedan a criterio de cada Parte Contratante. Las Partes Contratantes y los órganos jurisdiccionales nacionales también deben tener en cuenta las disposiciones relativas a la indemnización económica por los daños y perjuicios materiales o inmateriales ocasionados por el tratamiento, así como la posibilidad de habilitar acciones colectivas ([654]).

([653]) Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108), apartado 100.

([654]) Ibíd.

6.2.4. Sanciones

En el Derecho del CdE, el artículo 10 del Convenio 108 estipula que cada Parte Contratante deberá establecer sanciones y recursos adecuados para las violaciones de las disposiciones de Derecho nacional que apliquen los principios básicos de la protección de datos recogidos en el Convenio 108. El Convenio no establece o impone un conjunto de sanciones concretas. Por el contrario, indica claramente que cada Parte Contratante tiene discrecionalidad para determinar la naturaleza de las sanciones judiciales o no judiciales, que pueden ser penales, administrativas o civiles. El Informe explicativo del Convenio 108 modernizado establece que las sanciones deben ser efectivas, proporcionadas y disuasorias ([655]). Las Partes Contratantes deben respetar este principio cuando determinen la naturaleza y gravedad de las sanciones disponibles en su ordenamiento jurídico nacional.

En el Derecho de la UE, el artículo 83 del RGPD faculta a las autoridades de control de los Estados miembros para imponer multas por infracciones del Reglamento. En el mismo artículo 83 se establecen los niveles de las multas y las circunstancias que las autoridades nacionales han de tener en cuenta para decidir si imponen una multa, así como los límites máximos totales de dicha multa. El régimen sancionador está, por tanto, armonizado para toda la UE.

El RGPD establece multas de distintos niveles. Las autoridades de control están facultadas para imponer multas administrativas por infracciones del Reglamento de hasta 20 000 000 EUR o, tratándose de una empresa, del 4 % de su volumen de negocio total anual global, optándose por la de mayor cuantía. Entre las infracciones que pueden dar lugar a multas de este nivel están las violaciones de los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento, las violaciones de los derechos de los interesados y las violaciones de las disposiciones del Reglamento que regulan la transferencia de datos personales a destinatarios de terceros países. Por otras infracciones, las autoridades de control pueden imponer multas de hasta 10 000 000 EUR o, tratándose de una empresa, del 2 % de su volumen de negocio total anual global, optándose por la de mayor cuantía.

A la hora de determinar el tipo y nivel de la multa impuesta, las autoridades de control deben tener en cuenta una serie de factores ([656]). Por ejemplo, deben tomar en la debida consideración la naturaleza, gravedad y duración de la infracción, las categorías de datos personales afectadas y si existía intencionalidad o negligencia.

([655]) Ibíd.

([656]) Reglamento general de protección de datos, artículo 83, apartado 2.

Cuando un responsable o encargado haya tomado medidas para paliar los daños y perjuicios sufridos por los interesados, esto también deberá tenerse en cuenta. Del mismo modo, el grado de cooperación con la autoridad de control tras la infracción y la forma en que la autoridad de control tuviera conocimiento de la misma (por ejemplo, si fue notificada por la entidad responsable del tratamiento o por un interesado cuyos derechos fueron vulnerados) son otros factores importantes que las autoridades de control deben tener en cuenta en su decisión ([657]).

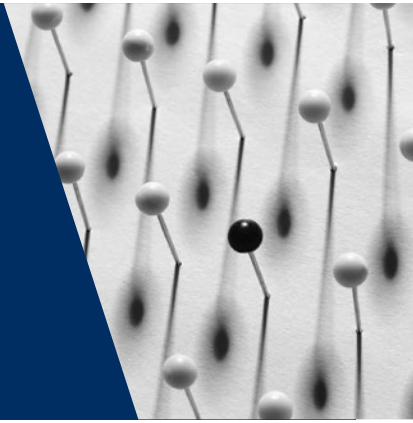
Además de la capacidad de imponer multas administrativas, las autoridades de control tienen a su disposición una gran variedad de poderes correctivos adicionales. Los denominados poderes «correctivos» de las autoridades de control están recogidos en el artículo 58 del RGPD. Estos van desde órdenes, advertencias y apercibimientos a responsables y encargados hasta la imposición de prohibiciones temporales o definitivas de las actividades de tratamiento.

En lo que atañe a las sanciones contra infracciones de la legislación de la Unión por parte de instituciones y organismos de la UE, debido al mandato especial del Reglamento de protección de datos de las instituciones de la UE, solo se pueden prever sanciones en forma de acciones disciplinarias. Según el artículo 49 del Reglamento, «[e]l incumplimiento, ya sea intencionado o por negligencia, de las obligaciones a que está sujeto en virtud del presente Reglamento un funcionario u otro agente de las Comunidades Europeas dará lugar a la apertura de un expediente disciplinario [...]».

([657]) Grupo de Trabajo del Artículo 29 (2017), Directrices sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679,, WP 253, 3 de octubre de 2017.

7

Transferencias y flujos internacionales de datos personales



UE	Materias tratadas	CdE
Transferencias de datos personales		
Reglamento general de protección de datos, artículo 44	Concepto	Convenio 108 modernizado, artículo 14, apartados 1 y 2
Libre circulación de los datos personales		
Reglamento general de protección de datos, artículo 1, apartado 3 y considerando 170.	Entre los Estados miembros de la UE	
	Entre las Partes Contratantes del Convenio 108	Convenio 108 modernizado, artículo 14, apartado 1
Transferencias de datos personales a terceros países o a organizaciones internacionales		
Reglamento general de protección de datos, artículo 45 C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 2015	Decisión de adecuación/ terceros países u organizaciones internacionales con niveles de protección adecuados	Convenio 108 modernizado, artículo 14, apartado 2
Reglamento general de protección de datos, artículo 46, apartados 1 y 2	Garantías adecuadas, que incluyan derechos exigibles y acciones legales efectivas para los interesados, que se establezcan a través de cláusulas contractuales tipo, normas corporativas vinculantes, códigos de conducta y mecanismos de certificación	Convenio 108 modernizado, artículo 14, apartados 2, 3, 5 y 6

UE	Materias tratadas	CdE
Reglamento general de protección de datos, artículo 46, apartado 3	**Sujetas a la autorización de la autoridad de control competente: cláusulas contractuales y disposiciones incluidas en acuerdos administrativos entre autoridades públicas**	
Reglamento general de protección de datos, artículo 46, apartado 5	**Autorizaciones existentes con arreglo a la Directiva 95/46**	
Reglamento general de protección de datos, artículo 47	**Normas corporativas vinculantes**	
Reglamento general de protección de datos, artículo 49	**Excepciones para situaciones específicas**	Convenio 108 modernizado, artículo 14, apartado 4
Ejemplos: Acuerdo sobre PNR entre la UE y los EE. UU. Acuerdo sobre SWIFT entre la UE y los EE. UU.	**Acuerdos internacionales**	Convenio 108 modernizado, artículo 14, apartado 3, letra a)

En el Derecho de la UE, el Reglamento general de protección de datos establece la libre circulación de datos en la Unión Europea. Sin embargo, contiene requisitos específicos para las transferencias de datos personales a terceros países externos a la Unión Europea y a organizaciones internacionales. El Reglamento reconoce la importancia de este tipo de transferencias, especialmente con miras al comercio y la cooperación internacionales, pero también reconoce el incremento del riesgo para los datos personales. Por tanto, el Reglamento trata de ofrecer a los datos personales transferidos a terceros países el mismo nivel de protección del que gozan en la UE ([658]). El Derecho del CdE también reconoce la importancia de establecer normas que regulen los flujos de datos transfronterizos, basadas en la libre circulación entre las partes y requisitos específicos para las transferencias a Estados no partes.

([658]) Reglamento general de protección de datos, considerandos 101 y 116.

7.1. Naturaleza de las transferencias de datos personales

Puntos clave

- El Derecho de la UE y el Derecho del CdE incorporan normas que regulan las transferencias de datos personales a destinatarios de terceros países o a organizaciones internacionales.
- El hecho de garantizar que los derechos del interesado estén protegidos cuando se transfieran sus datos fuera de la UE permite que la protección que le confiere el Derecho de la UE siga a los datos personales originados en la UE.

En el **Derecho del CdE**, los flujos de datos transfronterizos se definen como transferencias de datos personales a destinatarios sujetos a una jurisdicción extranjera ([659]). Los flujos de datos transfronterizos a destinatarios no sujetos a la jurisdicción de una Parte Contratante solo se permiten si existe un nivel de protección adecuado ([660]).

El **Derecho de la UE** regula las transferencias «de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional [...]» ([661]). Estos flujos de datos solo están permitidos si cumplen las disposiciones del capítulo V del RGPD.

Se permiten flujos transfronterizos de datos personales a destinatarios que estén sujetos a la jurisdicción de una Parte Contratante o Estado miembro conforme al Derecho del CdE o al Derecho de la UE, respectivamente. Ambos ordenamientos jurídicos permiten también las transferencias de datos a países que no sean Partes Contratantes o Estados miembros, siempre que se cumplan determinadas condiciones.

([659]) Informe explicativo del Convenio 108 modernizado, párrafo 102.

([660]) Convenio 108 modernizado, artículo 12, apartado 2.

([661]) Reglamento general de protección de datos, artículo 44.

7.2. Libre circulación de datos personales entre Estados miembros o Partes Contratantes

Puntos clave

- La circulación de datos personales por el territorio de la UE, así como las transferencias de datos personales entre las Partes Contratantes del Convenio 108 modernizado, no deben tener limitaciones. Sin embargo, dado que no todas las Partes Contratantes del Convenio 108 modernizado son Estados miembros de la UE, no es posible realizar transferencias de datos desde un Estado miembro a un tercer país que, no obstante, sea Parte Contratante del Convenio 108, a menos que se cumplan las condiciones establecidas en el RGPD.

En el Derecho del CdE, debe existir libre circulación de datos personales entre las Partes Contratantes del Convenio 108 modernizado. Sin embargo, se puede prohibir la transferencia si «existe un riego real y grave de que la transferencia a otra de las Partes pudiera conducir a evitar las disposiciones de la Convención» o si una de las partes «está obligada a ello por normas armonizadas de protección comunes a los Estados pertenecientes a una organización internacional regional» ([662]).

En el Derecho de la UE, están prohibidas las limitaciones o prohibiciones de la libre circulación de datos personales entre Estados miembros de la UE por razones relacionadas con la protección de las personas físicas en relación con el tratamiento de datos personales ([663]). El alcance de la libre circulación de datos ha sido ampliado por el Acuerdo sobre el Espacio Económico Europeo (EEE) ([664]), que incorpora a Islandia, Liechtenstein y Noruega al mercado interior.

([662]) Convenio 108 modernizado, artículo 14, apartado 1.

([663]) Reglamento general de protección de datos, artículo 1, apartado 3.

([664]) Decisión del Consejo y de la Comisión de 13 de diciembre de 1993 relativa a la celebración del Acuerdo sobre el Espacio Económico Europeo entre las Comunidades Europeas y sus Estados miembros, por una parte, y la República de Austria, la República de Finlandia, la República de Islandia, el Principado de Liechtenstein, el Reino de Noruega, el Reino de Suecia y la Confederación Suiza, por otra parte, DO 1994 L 1.

Ejemplo: Si una filial de un grupo internacional de empresas, que tiene establecimientos en varios Estados miembros de la UE, entre ellos Eslovenia y Francia, envía datos personales de Eslovenia a Francia, este flujo de datos no debe quedar limitado ni prohibido por la legislación nacional eslovena por razones relacionadas con la protección de datos personales.

No obstante, si la misma filial eslovena quiere transferir los mismos datos personales a la sociedad matriz en Malasia, la exportadora de datos eslovenos deberá tener en cuenta las disposiciones del capítulo V del RGPD. Estas disposiciones tienen por objeto salvaguardar los datos personales de los interesados que están sujetos a la jurisdicción de la UE.

En el Derecho de la UE, los flujos de datos personales a los Estados miembros del EEE con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales están sujetos a la Directiva 2016/680 ([665]). De este modo se garantiza además que el intercambio de datos personales entre autoridades competentes de la Unión no quede limitado o prohibido por razones de protección de datos. En el Derecho del CdE, todos los tratamientos de datos personales (incluidos los flujos transfronterizos con otras partes del Convenio 108), sin excepción alguna en virtud de sus fines o ámbitos de acción, están incluidos en el ámbito de aplicación del Convenio 108, aunque las Partes Contratantes pueden establecer exenciones. Todos los miembros del EEE son también Partes del Convenio 108.

([665]) 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 2016 L 119.

7.3. Transferencias de datos personales a terceros países o Estados no partes o a organizaciones internacionales

Puntos clave

- Tanto el **CdE** como la **UE** permiten las transferencias de datos personales a terceros países o a organizaciones internacionales, siempre que se cumplan determinadas condiciones para la protección de los datos personales.
  - **En el Derecho del CdE**, se puede conseguir un nivel de protección adecuado por medio de la legislación del Estado u organización internacional o adoptando normas apropiadas.
  - **En el Derecho de la UE**, se pueden realizar transferencias si el país tercero garantiza un nivel adecuado de protección o si el responsable o encargado del tratamiento establece garantías adecuadas, por ejemplo que los interesados cuenten con derechos exigibles y acciones legales efectivas, por ejemplo a través de cláusulas tipo de protección de datos o normas corporativas vinculantes.
- **Tanto el Derecho del CdE como el Derecho de la UE** establecen cláusulas de excepción que permiten la transferencia de datos personales en circunstancias concretas, aunque no exista ni un nivel de protección adecuado ni garantías apropiadas.

Aunque tanto el Derecho del CdE como el Derecho de la UE permiten los flujos de datos a terceros países o a organizaciones internacionales, establece diferentes condiciones. Cada conjunto de condiciones tiene en cuenta las diferencias entre las organizaciones respectivas en cuanto a estructura y fines.

En el **Derecho de la UE** existen, en principio, dos maneras de permitir la transferencia de datos personales a terceros países o a organizaciones internacionales. Las transferencias de datos personales pueden realizarse en virtud de una decisión de adecuación tomada por la Comisión Europea ([666]) o bien, en ausencia de dicha decisión de adecuación, cuando el responsable o encargado del tratamiento ofrezca garantías adecuadas, por ejemplo que los interesados cuenten con derechos exigibles y acciones legales efectivas ([667]). En ausencia de una decisión de adecuación o de garantías adecuadas, existen ciertas excepciones.

([666]) Reglamento general de protección de datos, artículo 45.

([667]) Ibíd., artículo 46.

En el **Derecho del CdE**, sin embargo, solo es posible realizar transferencias de datos a Estados no partes del Convenio conforme a lo siguiente:

- el Derecho de ese Estado u organización internacional, incluidos los tratados o acuerdos internacionales aplicables que garanticen salvaguardas apropiadas;

- salvaguardas específicas o estándar aprobadas que estén recogidas en instrumentos legalmente vinculantes y de cumplimiento exigible, adoptados y aplicados por las personas que participen en la transferencia de los datos y en su tratamiento ulterior ([668]).

Al igual que en el Derecho de la UE, en ausencia de un nivel adecuado de protección de datos, existen distintas excepciones.

7.3.1. Transferencias basadas en una decisión de adecuación

En el Derecho de la UE, el artículo 45 del RGPD establece la libre circulación de datos personales a terceros países con un nivel adecuado de protección de datos. El TJUE ha aclarado que la expresión «nivel de protección adecuado» exige que el tercer país garantice un nivel de protección de los derechos y libertades fundamentales que sea «sustancialmente equivalente» ([669]) a las garantías establecidas por la ley en la UE. Al mismo tiempo, los medios de los que se sirva un tercer país para los fines de garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión: el criterio de adecuación no requiere que se reproduzcan las normas de la UE punto por punto ([670]).

La Comisión Europea evalúa el nivel de protección de datos en países terceros analizando su Derecho nacional y sus obligaciones internacionales aplicables. También ha de tenerse en cuenta la participación de un país en sistemas multilaterales o regionales, en particular con respecto a la protección de datos personales. Si la Comisión Europea determina que el tercer país u organización internacional garantiza

([668]) Convenio 108 modernizado, artículo 14, apartado 3, letras a) y b).

([669]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015, apartado 96.

([670]) Ibíd., apartado 74. Véase también Comisión Europea (2017), Comunicación de la Comisión al Parlamento Europeo y al Consejo «Intercambio y protección de los datos personales en un mundo globalizado», COM(2017) 7 final, de 10 de enero de 2017, p. 6.

un nivel adecuado de protección, puede adoptar una decisión de adecuación que tiene efectos vinculantes ([671]). No obstante, el TJUE ha declarado que las autoridades de control nacionales siguen siendo competentes para examinar la reclamación de una persona física en relación con la protección de sus datos personales que hayan sido transferidos a un país tercero que la Comisión haya considerado que garantiza un nivel de protección adecuado, cuando esa persona alegue que la legislación y las prácticas vigentes en el tercer país no garantizan un nivel de protección adecuado ([672]).

La Comisión Europea también puede evaluar la adecuación de un territorio de un tercer país o limitarse a sectores concretos, como en el caso de la legislación comercial privada de Canadá, por ejemplo ([673]). También existen decisiones de adecuación relativas a transferencias basadas en acuerdos entre la UE y terceros países. Estas decisiones se refieren exclusivamente a un único tipo de transferencias de datos, como la transmisión de registros de nombres de los pasajeros (PNR) por parte de una compañía aérea a las autoridades extranjeras de control fronterizo cuando dicha compañía aérea vuela desde la UE a determinados destinos en el exterior (véase la sección 7.3.4).

Las decisiones de adecuación están sujetas a un control continuo. La Comisión Europea revisa periódicamente estas decisiones para tener en cuenta acontecimientos que puedan afectar a su estatus. De este modo, si la Comisión determina que un tercer país u organización internacional ha dejado de cumplir las condiciones que justificaban la decisión de adecuación, puede modificar, suspender o derogar dicha decisión. La Comisión también puede entablar negociaciones con el tercer país u organización internacional en cuestión con vistas a poner remedio a la situación en la que se base su decisión.

Las decisiones de adecuación adoptadas por la Comisión Europea en virtud de la Directiva 95/46/CE permanecen vigentes hasta que sean modificadas, sustituidas o derogadas por una Decisión de la Comisión adoptada de conformidad con las disposiciones del artículo 45 del RGPD.

([671]) Se puede consultar una lista de países objeto de una decisión de adecuación, que se actualiza constantemente, en la página de inicio de la Comisión Europea, Dirección General de Justicia.

([672]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015, apartados 63 y 65-66.

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

Hasta la fecha, la Comisión Europea ha reconocido que Andorra, Argentina, Canadá (organizaciones comerciales comprendidas en el ámbito de aplicación de la *Personal Information and Electronic Documents Act* o PIPEDA), Islas Feroe, Guernesey, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay garantizan una protección adecuada. Con respecto a las transferencias de datos a EE. UU., la Comisión Europea adoptó en 2000 una decisión de adecuación que permitía dichas transferencias a empresas que autocertificasen su protección de los datos personales transferidos desde la Unión Europea y cumplimiento de los llamados «principios de puerto seguro» ([674]). El TJUE invalidó esta decisión en 2015 y adoptó una nueva decisión de adecuación en 2016, que permitía que las empresas se incorporasen a partir del 1 de agosto de 2016.

Ejemplo: En *Schrems* ([675]), Maximilian Schrems, un ciudadano austriaco, había sido usuario de Facebook durante varios años. Parte o la totalidad de los datos facilitados por el Sr. Schrems a Facebook fueron transferidos por la filial irlandesa de Facebook a servidores radicados en los Estados Unidos, donde fueron objeto de tratamiento. El Sr. Schrems presentó una reclamación a la autoridad de protección de datos irlandesa, alegando que, a la luz de las revelaciones efectuadas por el estadounidense Edward Snowden en relación con las actividades de vigilancia de los servicios de inteligencia de los Estados Unidos, ni la legislación ni las prácticas estadounidenses ofrecen protección suficiente para los datos transferidos a ese país. La autoridad irlandesa rechazó la reclamación basándose en que, en su decisión de 26 de julio de 2000, la Comisión había considerado que, en virtud del sistema de «puerto seguro», los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos. El asunto llegó a la *High Court* irlandesa, que lo remitió al TJUE para que adoptase una decisión prejudicial.

El TJUE dictaminó que la decisión de la Comisión sobre la adecuación del marco de puerto seguro era inválida. El TJUE señaló en primer lugar que la decisión permitía que la aplicabilidad de los principios de protección de datos de puerto seguro se limitase por razones de seguridad nacional, interés

([674]) Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, DO L 215. Esta Decisión fue declarada inválida por el TJUE en el asunto C-362/14 *Maximillian Schrems contra Data Protection Commissioner* [GS].

([675]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015.

público o cumplimiento de la ley o en virtud de la legislación nacional de los EE. UU. Por tanto, la Decisión permitía la injerencia en los derechos fundamentales de las personas cuyos datos personales fueran o pudieran ser transferidos a los EE. UU. ([676]). Señaló además que la decisión no contenía ninguna conclusión sobre la existencia de normas en los EE. UU. destinadas a limitar dicha injerencia, ni sobre la existencia de ningún tipo de protección jurídica efectiva contra esta ([677]). El TJUE puso de relieve que el nivel de protección de los derechos y libertades fundamentales garantizados en la UE requiere que la legislación que suponga una injerencia en los artículos 7 y 8 debe establecer normas claras y precisas que definan el alcance y la aplicación de una medida e imponer garantías mínimas, excepciones y limitaciones con respecto a la protección de los datos personales ([678]). Puesto que la decisión de la Comisión no declaraba que los Estados Unidos de hecho garantizasen tal nivel de protección en virtud de su legislación nacional o sus compromisos internacionales, el TJUE concluyó que no cumplía los requisitos de lo dispuesto en materia de transferencias en la Directiva sobre protección de datos y, por tanto, era inválida ([679]).

Por tanto, el nivel de protección de los Estados Unidos no era «sustancialmente equivalente» a los derechos y libertades fundamentales garantizados por la Unión Europea ([680]). El TJUE argumentó que se habían violado varios artículos de la Carta de Derechos Fundamentales de la Unión Europea. En primer lugar, el contenido esencial del artículo 7 quedaba comprometido, ya que la legislación estadounidense «permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas». En segundo lugar, también se vulneraba el contenido esencial del artículo 47, ya que la legislación no ofrecía a las personas físicas recursos jurídicos en relación con el acceso a los datos personales o la rectificación o supresión de dichos datos. Por último, dado que el acuerdo de puerto seguro violaba los artículos citados, el tratamiento de los datos personales dejaba de ser lícito y por tanto existía una violación del artículo 8.

([676]) Ibíd., apartado 84.

([677]) Ibíd., apartados 88-89.

([678]) Ibíd., apartados 91-92.

([679]) Ibíd., apartados 96-97.

([680]) Ibíd., apartados 73-74 y 96.

Cuando el TJUE declaró inválido el acuerdo de puerto seguro, la Comisión y los Estados Unidos acordaron un nuevo marco: el Escudo de la privacidad UE-EE. UU. El 12 de julio de 2016, la Comisión adoptó una decisión por la que declaraba que los Estados Unidos garantizan un nivel adecuado de protección para los datos personales transferidos desde la Unión hasta organizaciones de los EE. UU. conforme al Escudo de la privacidad ([681]).

Al igual que el acuerdo de puerto seguro, el Escudo de la privacidad UE-EE. UU. tiene por objeto proteger los datos personales transferidos desde la UE hasta los EE. UU. con fines comerciales ([682]). Las empresas estadounidenses pueden autocertificar voluntariamente su adhesión a la lista del Escudo de la privacidad comprometiéndose a cumplir las normas de protección de datos del marco. Las autoridades competentes de los EE. UU. supervisan y verifican el cumplimiento de estas normas por parte de las empresas certificadas.

En particular, el régimen del Escudo de la privacidad establece:

- obligaciones de protección de datos para las empresas que reciben datos personales desde la UE;

- mecanismos de protección y recurso para las personas físicas, en particular la creación de un Defensor del Pueblo independiente de los servicios de inteligencia de los EE. UU. que atiende las reclamaciones de las personas físicas que creen que sus datos personales han sido utilizados de manera ilícita por las autoridades estadounidenses en el ámbito de la seguridad nacional;

([681]) Decisión de ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., DO L 207. El Grupo de Trabajo del Artículo 29 acogió favorablemente las mejoras incorporadas por el mecanismo del Escudo de la privacidad en comparación con la decisión de puerto seguro y elogió a la Comisión y a las autoridades de los EE. UU. por haber tenido en cuenta en la versión definitiva de los documentos del Escudo de la privacidad las inquietudes expresadas en su dictamen WP 238 relativo al proyecto de decisión de adecuación sobre el Escudo de la privacidad UE-EE. UU. No obstante, puso de relieve una serie de inquietudes todavía por resolver. Para más detalles, véase Grupo de Trabajo del Artículo 29, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, adoptado el 13 de abril de 2016, 16/EN, WP 238.

([682]) Para más información, véase EU-U.S. Privacy Shield factsheet.

- una revisión conjunta anual para controlar la aplicación del marco ([683]); la primera revisión se realizó en septiembre de 2017 ([684]).

El Gobierno de los Estados Unidos ha ofrecido determinados compromisos y garantías por escrito que acompañan a la decisión del Escudo de la privacidad y establecen limitaciones y salvaguardas en relación con el acceso por parte del Gobierno de los EE. UU. a los datos de carácter personal con fines policiales y de seguridad nacional.

7.3.2. Transferencias mediante garantías adecuadas

Tanto en el **Derecho del CdE** como en el **Derecho de la UE** se reconocen las garantías adecuadas entre el responsable exportador de datos y el destinatario en el país tercero u organización internacional como un medio posible para que el destinatario garantice un nivel de protección de datos suficiente.

En el **Derecho de la UE**, las transferencias de datos personales a un tercer país o a una organización internacional están permitidas si el responsable o encargado del tratamiento ofrece garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas ([685]). La lista de «garantías adecuadas» aceptables está recogida exclusivamente en la legislación de protección de datos de la UE. Se pueden establecer garantías adecuadas por medio de:

- un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;
- normas corporativas vinculantes;
- cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control;
- códigos de conducta;

([683]) Para más información, véase la página web de la Comisión Europea sobre el Escudo de la privacidad UE-EE. UU..

([684]) Comisión Europea, Informe de la Comisión al Parlamento Europeo y al Consejo sobre la primera revisión anual del funcionamiento del Escudo de la privacidad UE-EE. UU., COM(2017) 611 final, 18 de octubre de 2017.

([685]) Reglamento general de protección de datos, artículo 46.

- mecanismos de certificación ([686]).

Las cláusulas contractuales tipo entre el responsable o encargado radicado en la UE y el destinatario de los datos radicado en un país tercero son otro medio de establecer garantías adecuadas. Sin embargo, las cláusulas contractuales de esta índole deben ser autorizadas por la autoridad de control competente para que puedan servir como herramienta en la transferencia de datos personales. Del mismo modo, las autoridades públicas pueden hacer uso de las disposiciones de protección de datos incluidas en sus acuerdos administrativos, siempre que sean autorizadas por la autoridad de control ([687]).

En el Derecho del CdE, los flujos de datos a un Estado u organización internacional que no sea parte del Convenio 108 modernizado están permitidos, siempre que se garantice un nivel de protección adecuado. Esto se puede conseguir por medio de:

- las normas del Estado u organización internacional; o bien

- garantías específicas o estándar incorporadas a un documento jurídicamente vinculante ([688]).

Transferencias sujetas a cláusulas contractuales

Tanto en el **Derecho del CdE** como en el **Derecho de la UE** se reconocen las cláusulas contractuales entre el responsable exportador de datos y el destinatario en el país tercero u organización internacional como un medio posible para que el destinatario garantice un nivel de protección de datos suficiente ([689]).

En el **ámbito de la UE**, la Comisión Europea, con la ayuda del Grupo de Trabajo del Artículo 29, elaboró cláusulas contractuales tipo que fueron certificadas oficialmente por una Decisión de la Comisión como prueba de una protección de datos adecuada ([690]). Dado que las decisiones de la Comisión son vinculantes en su totalidad en los Estados miembros, las autoridades nacionales encargadas de la supervisión

([686]) Reglamento general de protección de datos, artículo 46, apartado 1, letras c) y d), apartado 2, letras a), b), e) y f), y artículo 47.

([687]) Ibíd., art. 46 apartado 3.

([688]) Convenio 108 modernizado, artículo 14, apartado 3, letra b).

([689]) Reglamento general de protección de datos, artículo 46, apartado 3; Protocolo adicional al Convenio 108 modernizado, artículo 14, apartado 3, letra b).

([690]) Ibíd., artículo 46, apartado 2, letra b) y artículo 46, apartado 5.

de las transferencias de datos deberán reconocer dichas cláusulas contractuales tipo en sus procedimientos ([691]). Por tanto, si el responsable exportador de datos y el destinatario en el país tercero acuerdan y firman dichas cláusulas, esto debería ser suficiente demostración para la autoridad de control de que se existen garantías adecuadas. Pero en el asunto *Schrems*, el TJUE resolvió que la Comisión Europea no tiene competencia para limitar el poder de las autoridades de control nacionales para supervisar la transferencia de datos personales a un tercer país que haya sido objeto de una decisión de adecuación de la Comisión ([692]). Por tanto, nada impide que las autoridades de control nacionales ejerzan sus poderes, incluido el poder de suspender o prohibir una transferencia de datos personales cuando esta suponga una violación de la legislación de protección de datos nacional o de la UE, como por ejemplo cuando el importador de los datos no respete las cláusulas contractuales tipo ([693]).

La existencia de cláusulas tipo de protección de datos en el marco jurídico de la UE no impide que los responsables formulen otras cláusulas contractuales específicas e individuales, siempre que sean autorizadas por la autoridad de control ([694]). Sin embargo, tendrían que garantizar el mismo nivel de protección que las cláusulas tipo de protección de datos. Para autorizar cláusulas específicas, las autoridades de control deben aplicar el mecanismo de coherencia, a fin de garantizar que exista un criterio normativo coherente en toda la UE ([695]). Esto significa que la autoridad de control competente debe comunicar su proyecto de decisión sobre las cláusulas al CEPD. El CEPD adoptará un dictamen sobre la materia, y la autoridad de control debe tener en cuenta este dictamen en la mayor medida posible cuando tome su decisión. Si no tiene intención de atenerse al dictamen del CEPD, se activará el mecanismo de resolución de conflictos del CEPD y el Comité adoptará una decisión vinculante ([696]).

([691]) Ibíd., artículo 46, apartado 3; Comité Ad hoc sobre Protección de Datos (CAHDATA), Informe explicativo del Convenio modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, apartado 105.

([692]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015, apartados 96-98 y 102-105.

([693]) A fin de tener en cuenta la posición del TJUE en el asunto *Schrems*, la Comisión modificó su Decisión sobre las cláusulas contractuales tipo. Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016, por la que se modifican las Decisiones 2001/497/CE y 2010/87/UE relativas a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, DO 2016 L 344.

([694]) Reglamento general de protección de datos, artículo 46, apartado 3, letra a).

([695]) Ibíd., artículo 63 y artículo 64, apartado 1, letra e).

([696]) Ibíd., artículos 64 y 65.

Las características más importantes de una cláusula contractual tipo son las siguientes:

- se trata de una cláusula que beneficia a un tercero, es decir, permite al interesado ejercer derechos contractuales, aunque no sea parte del contrato;

- en caso de litigio, el destinatario o importador de los datos accede a someterse a la autoridad de control o a los órganos jurisdiccionales del territorio nacional del responsable exportador de datos.

Actualmente existen dos conjuntos de cláusulas tipo para las transferencias de datos de responsable a responsable, entre los cuales puede elegir el responsable exportador de datos ([697]). Para las transferencias de responsable a encargado, solo hay un conjunto de cláusulas contractuales tipo ([698]). Sin embargo, estas cláusulas contractuales tipo son actualmente objeto de un proceso legal.

Ejemplo: Cuando el TJUE declaró inválida la Decisión de puerto seguro ([699]), las transferencias de datos personales a los Estados Unidos ya no podían basarse en aquella decisión de adecuación. Mientras las negociaciones con las autoridades estadounidenses seguían su curso, y pendiente la adopción de una nueva decisión de adecuación (que finalmente se adoptó el 12 de julio de 2016) ([700]), solo podían realizarse transferencias conforme a otras bases jurídicas, como cláusulas contractuales tipo o normas corporativas vinculantes. Varias empresas, como Facebook Ireland (que era la parte

([697]) El primer conjunto está incluido en el anexo de la Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, DO 2001, L 181; el segundo conjunto está incluido en el anexo de la Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países, DO 2004 L 385.

([698]) Comisión Europea (2010), Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, DO 2010 L 39. En el momento de redactarse el presente manual, el uso de cláusulas contractuales tipo como base para las transferencias de datos personales a los Estados Unidos era objeto de un proceso legal ante la High Court de Irlanda.

([699]) TJUE, C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS]70/10, 6 de octubre de 2015.

([700]) Decisión de ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU., DO L 207.

demandada en el asunto que dio lugar a la invalidación de la Decisión de puerto seguro), comenzaron a utilizar cláusulas contractuales tipo para continuar realizando transferencias de datos desde la UE hasta los EE. UU.

El Sr. Schrems presentó una reclamación ante la autoridad de control irlandesa, por la cual solicitaba la suspensión de las transferencias de datos a los Estados Unidos en virtud de cláusulas contractuales tipo. En esencia, alegó que cuando sus datos personales eran transferidos por la filial irlandesa de Facebook a Facebook Inc., y a servidores radicados en los EE. UU., no existían garantías de que estuvieran protegidos. Facebook Inc. está sujeta a leyes estadounidenses que podrían obligarla a revelar datos personales a los cuerpos de seguridad de EE. UU. y no existe ningún recurso judicial que permita impugnar esta práctica a los ciudadanos europeos ([701]). Por estas razones, el TJUE concluyó que la Decisión de puerto seguro era inválida, y si bien la sentencia del Tribunal se limitó al examen de esa decisión, el demandante consideró que las razones planteadas son igual de pertinentes cuando la transferencia se basa en cláusulas contractuales. En el momento de redactarse el presente documento, el asunto estaba siendo examinado por la *High Court* de Irlanda. El demandante aparentemente tiene intención de llevar el asunto al TJUE, donde pretende impugnar la validez de la decisión de la Comisión Europea sobre las cláusulas contractuales tipo. Como se ha explicado en el capítulo 5, solo el TJUE tiene competencia para declarar un instrumento de la UE inválido.

Transferencias sujetas a normas corporativas vinculantes

El **Derecho de la UE** también permite realizar transferencias de datos personales basadas en normas corporativas vinculantes en el caso de transferencias internacionales que tengan lugar dentro del mismo grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta ([702]). Antes de que las normas corporativas vinculantes puedan servir como herramienta en la transferencia de datos personales, la autoridad de control competente debe aprobarlas de conformidad con el mecanismo de coherencia.

([701]) Para más información, véase la demanda revisada presentada por Maximilian Schrems al Data Protection Commissioner irlandés contra Facebook Ireland Ltd con fecha 1 de diciembre de 2015.

([702]) Reglamento general de protección de datos, artículo 47.

Para que se aprueben, las normas corporativas vinculantes deben ser jurídicamente vinculantes, comprender todos los principios esenciales de protección de datos y ser aplicadas —y cumplidas— por todos los miembros del grupo. Deben conferir expresamente a los interesados derechos exigibles, incluir todos los principios esenciales de protección de datos y cumplir determinados requisitos formales, como por ejemplo especificar la estructura del grupo empresarial, describir las transferencias y concretar cómo se aplicarán los principios de protección de datos. Esto incluye proporcionar dicha información a los interesados. Las normas corporativas vinculantes deben especificar, entre otras cosas, los derechos de los interesados y disposiciones sobre responsabilidad en caso de incumplimiento de las normas ([703]). Cuando se aprueben normas corporativas vinculantes, se activará el mecanismo de coherencia para la cooperación entre autoridades de control (descrito en el capítulo 5).

En el marco del mecanismo de coherencia, la autoridad de control principal revisa las normas corporativas vinculantes propuestas, adopta un proyecto de decisión y lo comunica al CEPD. El Comité emite un dictamen sobre la materia y la autoridad de control principal puede aprobar formalmente las normas corporativas vinculantes al tiempo que «tiene en cuenta en la mayor medida posible» el dictamen del Comité. Este dictamen no es jurídicamente vinculante, pero si la autoridad de control tiene intención de no atenerse al dictamen, se activa el mecanismo de resolución de conflictos y el Comité ha de adoptar una decisión jurídicamente vinculante por mayoría de dos terceras partes de sus miembros ([704]).

En el **Derecho del CdE**, las garantías específicas o estándar incorporadas a un documento jurídicamente vinculante ([705]) también incluyen normas corporativas vinculantes.

7.3.3. Excepciones para situaciones específicas

En el Derecho de la UE, las transferencias de datos personales a un tercer país pueden estar justificadas, incluso en ausencia de una decisión de adecuación o de garantías adecuadas, como cláusulas contractuales tipo o normas corporativas vinculantes, en cualquiera de las circunstancias siguientes:

([703]) Véase una descripción más detallada en el Reglamento general de protección de datos, artículo 47.

([704]) Ibíd., artículo 57, apartado 1, letra s), artículo 58, apartado 1, letra j), artículo 64, apartado 1, letra f), artículo 65, apartados 1 y 2.

([705]) Convenio 108 modernizado, artículo 14, apartado 3, letra b).

- que el interesado dé su consentimiento explícito a la transferencia de los datos;
- que el interesado formalice —o esté dispuesto a formalizar— una relación contractual cuando la transferencia de datos al exterior sea necesaria;
- para celebrar un contrato entre el responsable del tratamiento y un tercero en interés del interesado;
- por razones importantes de interés público;
- para la formulación, el ejercicio o la defensa de reclamaciones;
- para proteger los intereses vitales del interesado;
- para la transferencia de datos desde registros públicos (este es un caso en el que prevalecen los intereses del público en general de poder acceder a información que se conserve en registros públicos) ([706]).

Cuando ninguna de estas condiciones sea de aplicación y las transferencias no se puedan basar en una decisión de adecuación o en garantías adecuadas, solo se podrá realizar una transferencia cuando no sea repetitiva, afecte a un número limitado de interesados y sea necesaria para los fines de los intereses legítimos imperiosos del responsable del tratamiento, siempre que sobre ellos no prevalezcan los derechos del interesado ([707]). En estos casos, el responsable ha de valorar las circunstancias que rodean a la transferencia y establecer garantías. También deberá informar a la autoridad de control y a los interesados afectados acerca de la transferencia y del interés legítimo que la justifica.

El hecho de que las excepciones sean el último recurso para realizar transferencias lícitas ([708]) (aplicables únicamente en ausencia de una decisión de adecuación y cuando no existan otras garantías) resalta su carácter excepcional, lo cual queda todavía más de manifiesto en los considerandos del RGPD ([709]). En este sentido, las excepciones se aceptan como una posibilidad «de realizar transferencias en

([706]) Reglamento general de protección de datos, artículo 49.

([707]) Ibíd.

([708]) Ibíd., artículo. 49 apartado 1.

([709]) Reglamento general de protección de datos, artículo 49, apartado 1, letras a), b) and e) y considerando 113.

determinadas circunstancias» y si «la transferencia es ocasional y necesaria» ([710]) en relación con un contrato o una reclamación.

Además, de acuerdo con las directrices del Grupo de Trabajo del Artículo 29, el recurso a las excepciones para situaciones concretas debe ser excepcional, basado en casos concretos y no se puede utilizar para transferencias masivas o repetitivas ([711]). El Supervisor Europeo de Protección de Datos también ha subrayado el carácter excepcional de las derogaciones utilizadas como base jurídica para las transferencias en virtud del Reglamento 45/2001, señalando que esta solución debe utilizarse en «casos limitados» y «para transferencias ocasionales» ([712]).

Ejemplo: Una empresa de servicios que opera un sistema de distribución global (SDG), con domicilio social en los Estados Unidos, gestiona el sistema de reservas en línea de numerosas compañías aéreas, hoteles y cruceros de todo el mundo, que implica el tratamiento de datos de decenas de millones de personas en la UE. La empresa SDG utiliza una excepción como base jurídica para transferir inicialmente los datos a sus servidores en los Estados Unidos, ya que esto es necesario para celebrar un contrato. Es decir, no aporta ninguna otra garantía para los datos personales originarios de Europa, transferidos a los EE. UU. y redistribuidos a continuación a hoteles de todo el mundo (lo que implica que tampoco existen garantías para las transferencias ulteriores). La empresa SDG no está cumpliendo los requisitos del RGPD para la licitud de las transferencias de datos internacionales, porque se basa en una excepción como fundamento lícito para realizar transferencias masivas.

Si no existe una decisión de adecuación, la UE o sus Estados miembros están facultadas para limitar la transferencia de determinadas categorías de datos personales a terceros países, aunque se cumplan otras condiciones para realizar este tipo de transferencias, por razones importantes de interés público. Estos límites deben

([710]) Ibíd., artículo. 49 apartado 1.

([711]) Grupo de Trabajo del Artículo 29 (2005), Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, WP 114, Bruselas, 25 de noviembre de 2005.

([712]) Supervisor Europeo de Protección de Datos, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, Documento de posición, Bruselas, 14 de julio de 2014, p. 15.

ser percibidos como excepcionales y los Estados miembros tienen la obligación de comunicar las disposiciones pertinentes a la Comisión ([713]).

El **Derecho del CdE** permite los flujos de datos a territorios que carecen de una protección de datos adecuada cuando:

- el interesado ha dado su consentimiento,
- los intereses del interesado requieren la transferencia;
- prevalecen intereses legítimos, en particular importantes intereses públicos, establecidos por la ley;
- constituye una medida necesaria y proporcionada en una sociedad democrática ([714]).

7.3.4. Transferencias basadas en acuerdos internacionales

La UE puede celebrar acuerdos internacionales con terceros países que regulen la transferencia de datos personales con fines concretos. Dichos acuerdos deben incluir garantías adecuadas para proteger los datos personales de las personas físicas afectadas. El RGPD existe sin perjuicio de estos acuerdos internacionales ([715]).

Los Estados miembros también pueden celebrar acuerdos internacionales con terceros países u organizaciones internacionales que garanticen un nivel adecuado de protección de los derechos y libertades fundamentales de las personas físicas, en la medida en que dichos acuerdos no afecten a la aplicación del RGPD.

El artículo 12, apartado 3, letra a) del Convenio 108 modernizado recoge una disposición similar.

([713]) Véase, en particular, Grupo de Trabajo del Artículo 29 (2005), Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, WP 114, Bruselas, 25 de noviembre de 2005.

([714]) Convenio 108 modernizado, artículo 14, apartado 4.

([715]) Reglamento general de protección de datos, considerando 102.

Un ejemplo de acuerdo internacional que implica la transferencia de datos personales son los acuerdos sobre registros de nombres de pasajeros (PNR, por sus siglas en inglés).

Registros de nombres de pasajeros

Los datos de los PNR son recogidos por las compañías aéreas durante el procedimiento de reserva del vuelo e incluyen, entre otras cosas, el nombre, la dirección, la información de la tarjeta de crédito y el número de asiento de los pasajeros por vía aérea. Las compañías aéreas también recogen esta información para sus propios fines comerciales. La UE ha alcanzado acuerdos con determinados terceros países (Australia, Canadá y los EE. UU.) en relación con la transferencia de datos de PNR con fines de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo o delitos graves transnacionales. Además, en 2016 la Unión adoptó la Directiva (UE) 2016/861, conocida como la Directiva PNR ([716]). Esta directiva establece un marco jurídico para que los Estados miembros de la UE transfieran los datos de los PNR a las autoridades competentes de otros terceros países, con fines similares de prevención, detección, investigación o enjuiciamiento de delitos de terrorismo y delitos graves. Las transferencias de PNR a autoridades de terceros países se autorizan caso por caso y están sujetas a una evaluación individual de la necesidad de la transferencia para los fines especificados en la Directiva y siempre que se respeten los derechos fundamentales.

En relación con los acuerdos sobre PNR entre la UE y terceros países, se ha cuestionado su compatibilidad con los derechos fundamentales a la privacidad y la protección de datos personales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea. Cuando —después de las negociaciones con Canadá— la UE firmó un acuerdo sobre la transferencia y el tratamiento de datos de PNR en 2014, el Parlamento Europeo decidió remitir el asunto al TJUE para que evaluase la legalidad del acuerdo conforme al Derecho de la UE y, en particular, conforme a los artículos 7 y 8 de la Carta.

([716]) 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, DO 2016 L 119.

Ejemplo: En su Dictamen sobre la legalidad del Acuerdo entre la UE y Canadá sobre los PNR ([717]), el TJUE dictaminó que, en su formato actual, el Acuerdo previsto era incompatible con los derechos fundamentales reconocidos por la Carta y, por tanto, no podía celebrarse. Dado que comprendía el tratamiento de datos personales, constituía una injerencia en el derecho a la protección de los datos personales protegido por el artículo 8 de la Carta. Al mismo tiempo, también representa una limitación del derecho al respeto de la vida privada, consagrado en el artículo 7, puesto que, conjuntamente considerados, los datos del PNR pueden agregarse y analizarse para revelar hábitos de viaje, relaciones entre distintas personas, información acerca de su situación financiera, hábitos alimentarios o estado de salud, con lo que se produce una intromisión en su vida privada.

La injerencia en los derechos fundamentales que suponía el Acuerdo previsto perseguía un objetivo de interés general, concretamente la seguridad pública y la lucha contra el terrorismo y la delincuencia transnacional grave. Sin embargo, el TJUE recordó que, para estar justificada, una injerencia debe limitarse a lo estrictamente necesario para alcanzar el fin que persigue. Después de analizar sus disposiciones, el TJUE concluyó que el Acuerdo previsto no cumplía el criterio de «necesidad estricta». Para llegar a esa conclusión, el TJUE tuvo en cuenta, entre otros, los siguientes factores:

- El hecho de que el Acuerdo previsto implicaba la transferencia de datos sensibles. El PNR recogido en virtud del Acuerdo previsto podía incluir datos sensibles, como información reveladora del origen racial o étnico, las creencias religiosas o el estado de salud de un pasajero. La transferencia y el tratamiento de datos sensibles por las autoridades canadienses podía acarrear un riesgo para el principio de no discriminación y, por tanto, requería una justificación precisa y sólida, basada en razones distintas de la seguridad pública y la lucha contra la delincuencia grave. El Acuerdo previsto no aportaba tal justificación ([718]).

- También se consideró que el almacenamiento continuado de los datos del PNR de la totalidad de los pasajeros durante un periodo superior a cinco años, incluso después de su partida de Canadá, excedía los límites de la necesidad estricta. El TJUE consideró que sería admisible que las

([717]) TJUE, *Dictamen 1/15 del Tribunal* [GS], 26 de julio de 2017.

([718]) Ibíd., apartado 165.

> autoridades canadienses conservaran los datos de pasajeros respecto de los que existieran elementos objetivos que indicasen que podrían presentar un riesgo en materia de seguridad pública, incluso después de que esas personas hubieran salido de Canadá. Por el contrario, no está justificada la conservación de datos personales de la *totalidad* de los pasajeros, respeto de quienes no existan pruebas, ni siquiera indirectas, de que presentan un riesgo para la seguridad pública ([719]).

El Comité Consultivo del Convenio 108 ha emitido un dictamen relativo al impacto en materia de protección de datos de los acuerdos sobre el PNR en virtud del Derecho del CdE ([720]).

Datos de mensajería

La Sociedad de las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT, por sus siglas en inglés), con sede en Bélgica, que es la encargada del tratamiento de la mayoría de transferencias monetarias mundiales desde bancos europeos, operaba con un centro «espejo» en los Estados Unidos y recibió una solicitud de revelación de datos al Departamento del Tesoro de los Estados Unidos por razones de investigación del terrorismo de conformidad con su Programa de Seguimiento de la Financiación del Terrorismo ([721]).

Desde la perspectiva de la UE, no existía suficiente base jurídica para revelar estos datos a los EE. UU. —principalmente acerca de ciudadanos de la UE— simplemente porque uno de los centros de proceso de datos de SWIFT estuviera radicado allí.

([719]) Ibíd., apartados 204-207.

([720]) Consejo de Europa, *Dictamen sobre las implicaciones para la protección de datos del tratamiento de los registros de nombres de pasajeros*, T-PD(2016)18rev, 19 de agosto de 2016.

([721]) Véase, en este contexto, Grupo de Trabajo del Artículo 29 (2011), Dictamen 14/2011 sobre los aspectos de la protección de datos relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo, WP 186, Bruselas, 13 de junio de 2011; Grupo de Trabajo del Artículo 29 (2006), Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT), WP 128, Bruselas, 22 de noviembre de 2006; Comisión de Bélgica para la protección de la vida privada (*Commission de la protection de la vie privée*) (2008), «Procedimiento de control y recomendación iniciado con respecto a la compañía SWIFT scrl», Decisión de 9 de diciembre de 2008.

En 2010 se celebró un acuerdo especial entre la UE y los Estados Unidos, conocido como Acuerdo SWIFT, para establecer la base jurídica necesaria y garantizar normas de protección de datos adecuadas ([722]).

En virtud de este acuerdo, los datos financieros almacenados por SWIFT se facilitan al Departamento del Tesoro de los Estados Unidos con fines de prevención, investigación, detección o represión del terrorismo o de su financiación. El Departamento del Tesoro de los Estados Unidos podrá solicitar datos financieros a SWIFT, siempre que la solicitud:

- identifique de la forma más clara posible los datos financieros;
- motive claramente la necesidad de los datos;
- se circunscriba en la mayor medida posible a los datos que resulten necesarios, con objeto de reducir al mínimo la cantidad de datos requeridos;
- no pida ningún dato sobre la zona única de pagos en euros (SEPA) ([723]).

Europol deberá recibir una copia de cada solicitud realizada por el Departamento del Tesoro de los Estados Unidos y comprobar si se están cumpliendo los principios del Acuerdo SWIFT ([724]). Si se confirma que se cumplen, SWIFT debe proporcionar los datos financieros directamente al Departamento del Tesoro de los EE. UU. El departamento deberá almacenar los datos financieros en un entorno físico seguro al que puedan acceder únicamente analistas dedicados a la investigación del terrorismo o de su financiación, y los datos no deberán interconectarse con otras bases de datos. En general, los datos financieros recibidos por SWIFT deberán ser suprimidos a más tardar cinco años después de su recepción. Los datos financieros que sean relevantes para investigaciones o acciones judiciales concretas podrán ser conservados únicamente durante el tiempo que resulte necesario para dichas investigaciones o acciones judiciales.

([722]) Decisión 2010/412/UE del Consejo, de 13 de julio de 2010, relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo, DO 2010 L 195, pp. 3 y 4. El texto del Acuerdo se adjunta a esta Decisión, DO 2010 L 195, pp. 5-14.

([723]) Ibíd., artículo 4, apartado 2.

([724]) La Autoridad Común de Control de Europol ha realizado auditorías sobre las actividades de Europol en este ámbito.

El Departamento del Tesoro de los Estados Unidos podrá transferir la información de los datos recibidos de SWIFT a las fuerzas y cuerpos de seguridad y a las autoridades responsables del mantenimiento del orden público o de lucha contra el terrorismo de dentro o de fuera de los Estados Unidos, exclusivamente a efectos de prevención, detección, investigación o represión del terrorismo o de su financiación. Cuando la transferencia ulterior de los datos financieros implique a un ciudadano o residente de un Estado miembro de la UE, el intercambio de información con las autoridades de un tercer país estará supeditado al consentimiento previo de las autoridades competentes del Estado miembro en cuestión. Pueden establecerse excepciones si el intercambio de datos es esencial para la prevención de una amenaza grave e inmediata contra la seguridad pública.

El cumplimiento de los principios del Acuerdo SWIFT será controlado por supervisores independientes, incluida una persona designada por la Comisión Europea. Estos supervisores tendrán la posibilidad de efectuar un examen retrospectivo y en tiempo real de todas las búsquedas de los datos facilitados, solicitar información adicional para justificar la relación de estas búsquedas con el terrorismo y la facultad de suspender alguna o la totalidad de las búsquedas que parezca que infringen las salvaguardas establecidas en el acuerdo.

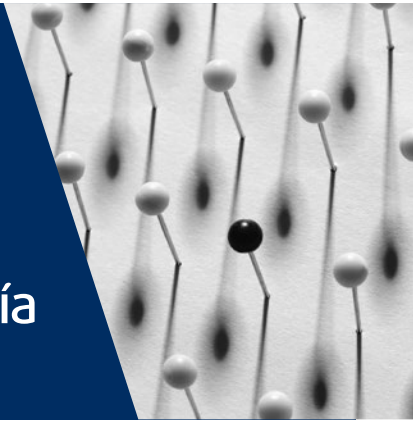
Los interesados tienen derecho a que la autoridad de control competente de la UE les confirme que se han respetado sus derechos en materia de protección de datos. Los interesados también tienen derecho de rectificación, supresión o bloqueo de aquellos de sus datos personales que hayan sido obtenidos y almacenados por el Departamento del Tesoro de los Estados Unidos con arreglo a lo dispuesto en el Acuerdo SWIFT. Sin embargo, los derechos de acceso de los interesados podrán estar sujetos a determinadas limitaciones legales. En el caso de que se deniegue el acceso, deberá informarse al interesado por escrito de la denegación y de su derecho a interponer los recursos administrativos o judiciales disponibles en los Estados Unidos.

El Acuerdo SWIFT tiene una validez de cinco años y su primer periodo de validez finalizó en agosto de 2015. Se prorroga automáticamente por periodos sucesivos de un año, a menos que una de las partes notifique a la otra por escrito, con seis meses de antelación, su intención de no prorrogar el acuerdo. La prórroga automática se aplicó en agosto de 2015, 2016 y 2017 y garantiza la validez del Acuerdo SWIFT como mínimo hasta agosto de 2018 ([725]).

([725]) Ibíd., artículo 23, apartado 2.

8

Protección de datos en el contexto de la policía y la justicia penal



UE	Materias tratadas	CdE
Directiva sobre protección de datos para las autoridades policiales y de justicia penal	**En general**	Convenio 108 modernizado
	Policía	Recomendación sobre la policía Guía práctica sobre el uso de datos personales en el ámbito policial.
	Vigilancia	TEDH, *B.B. contra Francia*, n.º 5335/06, 2009 TEDH, *S. y Marper contra Reino Unido* [GS], números 30562/04 y 30566/04, 2008 TEDH, *Allan contra Reino Unido*, n.º 48539/99, 2002. TEDH, *Malone contra Reino Unido*, n.º 8691/79, 1984. TEDH, *Klass y otros contra Alemania*, n.º 5029/71, 1978 TEDH, *Szabó y Vissy contra Hungría*, n.º 37138/14, 2016 TEDH, *Vetter contra Francia*, n.º 59842/00, 2005
	Ciberdelincuencia	Convenio sobre la ciberdelincuencia

UE	Materias tratadas	CdE
Otros instrumentos jurídicos específicos		
Decisión Prüm	**Para datos especiales: impresiones dactilares, ADN, gamberrismo, información sobre pasajeros aéreos, datos de telecomunicaciones, etc.**	Convenio 108 modernizado, artículo 6 Recomendación sobre la policía. Guía práctica sobre el uso de datos personales en el ámbito policial.
Iniciativa Sueca (Decisión marco 2006/960/JAI)	**Simplificación del intercambio de información e inteligencia entre los servicios de seguridad**	TEDH, *S. y Marper contra Reino Unido* [GS], números 30562/04 y 30566/04, 2008
Directiva (UE) 2016/681 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 TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Kärntner Landesregierung y otros* [GS], 2014 TJUE, asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige y Home Department contra Tom Watson y otros* [GC], 2016	**Conservación de datos personales**	TEDH, *B.B. contra Francia*, n.º 5335/06, 2009
Reglamento de Europol Decisión de Eurojust	**Por las agencias especiales**	Recomendación sobre la policía
Decisión Schengen II Reglamento VIS Reglamento Eurodac Decisión del SIA	**Por los sistemas comunes de información especiales**	Recomendación sobre la policía TEDH, Dalea contra Francia, n.º 964/07, 2010

Para ponderar los intereses de las personas físicas en la protección de datos y los intereses de la sociedad en la obtención de datos con el fin de combatir la delincuencia y garantizar la seguridad nacional y pública, el CdE y la UE han adoptado instrumentos jurídicos específicos. Esta sección ofrece un resumen del Derecho del CdE (véase la sección 8.1) y del Derecho de la UE (véase la sección 8.2) en relación con la protección de datos en asuntos de la policía y la justicia penal.

8.1. Derecho del CdE sobre la protección de datos en asuntos de seguridad nacional, policía y justicia penal

Puntos clave

- El Convenio 108 modernizado y la Recomendación sobre la policía del CdE se aplican a la protección de datos en todos los ámbitos de la labor policial.
- El Convenio sobre la ciberdelincuencia (Convenio de Budapest) es un instrumento jurídico internacional vinculante que trata sobre los delitos cometidos contra y con ayuda de las redes electrónicas. También es pertinente para la investigación de delitos que no se pueden considerar ciberdelitos pero que generan pruebas electrónicas.

Una distinción importante entre el **Derecho del CdE** y el Derecho de la UE es que el primero, a diferencia del segundo, también se aplica al ámbito de la seguridad nacional. Esto significa que las Partes Contratantes deben atenerse al mandato del artículo 8 del CEDH incluso en el caso de las actividades relacionadas con la seguridad nacional. Algunas sentencias del TEDH se refieren a actividades del Estado en las áreas sensibles de la legislación y la práctica de la seguridad nacional ([726]).

A escala europea, en lo que respecta a la policía y la justicia penal, el Convenio 108 modernizado abarca todos los ámbitos del tratamiento de datos personales, y sus disposiciones pretenden regular el tratamiento de datos personales en general. En consecuencia, el Convenio 108 modernizado se aplica a la protección de datos en el ámbito de la policía y la justicia penal. Solo está permitido el tratamiento de datos genéticos, datos personales relativos a delitos, procesos penales y condenas y posibles medidas de seguridad relacionadas, datos biométricos que identifiquen a una persona de forma inequívoca, así como cualquier dato sensible de carácter personal, cuando existan garantías adecuadas contra los riesgos que el tratamiento de tales datos pueda generar para los intereses, derechos y libertades fundamentales del interesado, y en particular el riesgo de discriminación ([727]).

([726]) Véase, por ejemplo, TEDH, *Klass y otros contra Alemania*, n.º 5029/71, 6 de septiembre de 1978; TEDH, *Rotaru contra Rumanía* [GS], n.º 28341/95, 4 de mayo de 2000; y TEDH, *Szabó y Vissy contra Hungría*, n.º 37138/14, 12 de enero de 2016.

([727]) Convenio 108 modernizado, artículo 6.

Las funciones legales de las autoridades policiales y de justicia penal requieren con frecuencia el tratamiento de datos personales, que puede acarrear graves consecuencias para las personas físicas afectadas. La Recomendación sobre la policía adoptada por el CdE en 1987 tiene por objeto orientar a las Partes Contratantes sobre la manera de aplicar los principios del Convenio 108 en el contexto del tratamiento de datos personales por parte de las autoridades policiales ([728]). La recomendación ha sido complementada con una Guía práctica sobre el uso de datos personales en el ámbito policial adoptada por el Consejo consultivo del Convenio 108 ([729]).

Ejemplo: En *D.L. contra Bulgaria* ([730]), los servicios sociales internaron a la demandante en un centro educativo de seguridad por orden judicial. Toda la correspondencia escrita y las conversaciones telefónicas fueron sometidas por el centro a una vigilancia general e indiscriminada. El TEDH resolvió que había existido violación del artículo 8, dado que la medida en cuestión no era necesaria en una sociedad democrática. El Tribunal declaró que había que hacer todo lo necesario para que los menores internados en un centro tuvieran contacto suficiente con el mundo exterior, ya que esto era parte integral de su derecho a ser tratados con dignidad y era absolutamente esencial para preparar su reinserción en la sociedad. Esto era igualmente aplicable a la correspondencia escrita y a las conversaciones telefónicas. Además, la vigilancia no hacía distinción alguna entre las comunicaciones con familiares y miembros de las ONG que representaban los derechos de los menores o sus abogados. Más aún, la decisión de interceptar las comunicaciones no estaba fundamentada en un análisis individualizado del riesgo existente en cada caso concreto.

Ejemplo: En *Dragojević contra Croacia* ([731]), el demandante era sospechoso de tráfico de drogas. Fue declarado culpable a raíz de que el juez instructor autorizase medidas de vigilancia encubierta para interceptar las llamadas telefónicas del demandante. El TEDH dictaminó que la medida, contra la que se había interpuesto demanda, constituía una injerencia en el derecho al respeto de la vida privada y la correspondencia. La autorización otorgada

([728]) Consejo de Europa, Comité de Ministros (1987), *Recommendation Rec(87)15 to Member States regulating the use of personal data in the police sector*, 17 de septiembre de 1987.

([729]) Consejo de Europa (2018), Consultative Committee of Convention 108, Practical Guide on the use of personal data in the police sector, T-PD(2018)1.

([730]) TEDH, *D.L. contra Bulgaria*, n.º 7472/14, 19 de mayo de 2016.

([731]) TEDH, *Dragojević contra Croacia*, n.º 68955/11, 15 de enero de 2015.

por el juez instructor se basaba únicamente en la declaración de la Fiscalía de que «no era posible realizar la investigación por otros medios». El TEDH señaló además que los órganos jurisdiccionales penales habían limitado su evaluación con respecto al uso de las medidas de vigilancia y que el Gobierno no había aportado información alguna sobre los recursos disponibles. En consecuencia, había existido violación del artículo 8.

8.1.1. La Recomendación sobre la policía

El TEDH ha sostenido sistemáticamente que el almacenamiento y conservación de datos personales por parte de la policía o de las autoridades nacionales de seguridad constituye una injerencia en el artículo 8, apartado 1, del CEDH. Muchas de las sentencias del TEDH tratan sobre la justificación de dichas injerencias ([732]).

Ejemplo: En *B.B. contra Francia* ([733]), el demandante fue condenado por cometer delitos sexuales contra menores de 15 años aprovechándose de su posición de confianza. Cumplió su condena de privación de libertad en 2000. Un año después, solicitó que se eliminase la mención de esta sentencia de sus antecedentes penales, pero su petición fue denegada. En 2004, una ley francesa creó una base de datos nacional de delincuentes sexuales para uso judicial y se comunicó al demandante que había sido incluido en ella. El TEDH resolvió que el artículo 8 del CEDH era aplicable a la inclusión de un delincuente sexual convicto en una base de datos nacional de uso judicial. Sin embargo, dado que se habían aplicado garantías suficientes en materia de protección de datos, como el derecho del interesado a solicitar la supresión de los datos, la conservación de los datos por tiempo limitado y la limitación del acceso a dichos datos, se había alcanzado un justo equilibrio entre los intereses públicos y privados enfrentados. El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH.

([732]) Véase, por ejemplo, TEDH, *Leander contra Suecia*, n.º 9248/81, 26 de marzo de 1987; TEDH, *M.M.* contra Reino Unido, n.º 24029/07, 13 de noviembre de 2012; TEDH, *M.K. contra Francia*, n.º 19522/09, 18 de abril de 2013; o TEDH, *Aycaguer contra Francia*, n.º 8806/12, 22 de junio de 2017.

([733]) TEDH, *B.B. contra Francia*, n.º 5335/06, 17 de diciembre de 2009.

Ejemplo: En *S. y Marper contra Reino Unido* ([734]), ambos demandantes habían sido acusados de delitos, aunque no habían sido condenados. Sin embargo, la policía conservó y almacenó sus impresiones dactilares, perfiles de ADN y muestras celulares. La ley permitía la conservación ilimitada de los datos biométricos mencionados cuando una persona había sido sospechosa de un delito, aunque posteriormente hubiera sido absuelta o se hubiera retirado la acusación. El TEDH sostuvo que la conservación generalizada e indiscriminada de datos personales, sin limitación en el tiempo y con opciones limitadas de que las personas físicas absueltas solicitasen su supresión, constituía una injerencia desproporcionada en el derecho de los demandantes al respeto de su vida privada. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

Un aspecto crucial en el contexto de las comunicaciones electrónicas es la injerencia por parte de las autoridades públicas en los derechos a la privacidad y a la protección de datos. Los medios de vigilancia o intervención de las comunicaciones, como los dispositivos de escucha o grabación, solo son admisibles si están previstos por la ley y constituyen una medida necesaria en una sociedad democrática en interés de:

- la protección de la seguridad nacional;
- la seguridad pública;
- los intereses monetarios del Estado;
- la supresión de los delitos; o
- la protección del interesado o de los derechos y libertades de los demás.

Muchas otras sentencias del TEDH tratan de la justificación de la injerencia en el derecho a la privacidad mediante la vigilancia.

([734]) TEDH, *S. y Marper contra el Reino Unido* [GS], números 30562/04 y 30566/04, 4 de diciembre de 2008, apartados 119 y 125.

Ejemplo: En *Allan contra Reino Unido* ([735]), las autoridades grabaron en secreto conversaciones privadas entre un preso y una amiga en el área de visitas del centro penitenciario y con otro acusado en una celda. El TEDH dictaminó que el uso de dispositivos de grabación de audio y vídeo en la celda del demandante, en el área de visitas del centro penitenciario y en la propia persona de un compañero de prisión suponía una injerencia en el derecho a la vida privada del demandante. Como no existía un régimen jurídico que regulase el uso de dispositivos de grabación ocultos por parte de la policía en aquel momento, dicha injerencia no había sido realizada de conformidad con la ley. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

Ejemplo: En *Roman Zakharov contra Rusia* [GS] ([736]), el demandante entabló un proceso judicial contra tres operadores de redes móviles. Alegó que se había violado el derecho a la privacidad de sus comunicaciones telefónicas, ya que estos operadores habían instalado equipos que permitían al Servicio de Seguridad Federal intervenir sus comunicaciones telefónicas sin autorización judicial previa. El TEDH resolvió que las disposiciones legales nacionales que regulaban la intervención de las comunicaciones no contemplaban garantías adecuadas y efectivas contra la arbitrariedad y el riesgo de abuso. En particular, la legislación nacional no exigía que se eliminasen los datos almacenados una vez conseguido el fin de tal almacenamiento. Además, aunque se requería autorización judicial, el examen judicial era limitado.

Ejemplo: En *Szabó y Vissy contra Hungría* ([737]), los demandantes denunciaron que la legislación húngara violaba el artículo 8 del CEDH, ya que no era suficientemente detallada ni precisa. Además, alegaban que la legislación no ofrecía garantías suficientes contra el abuso y la arbitrariedad. El TEDH dictaminó que la legislación húngara no exigía que la vigilancia estuviera sujeta a la autorización de un órgano jurisdiccional. No obstante, el Tribunal señaló que, si bien estaba sujeta a la aprobación del Ministerio de Justicia, esta supervisión era eminentemente política y no podía garantizar el criterio exigido de «necesidad estricta». Además, la legislación nacional no contemplaba la revisión judicial, dado que no se enviaría notificación alguna a los interesados. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

([735]) TEDH, *Allan contra Reino Unido*, n.º 48539/99, 5 de noviembre de 2002.

([736]) TEDH, *Roman Zakharov contra Rusia* [GS], n.º 47143/06, 4 de diciembre de 2015.

([737]) TEDH, *Szabó y Vissy contra Hungría*, n.º 37138/14, 12 de enero de 2016.

Dado que el tratamiento de datos por parte de las autoridades policiales puede afectar de forma significativa a los interesados, el tratamiento de datos personales en este ámbito requiere especialmente la existencia de normas detalladas de protección de datos. La Recomendación del CdE sobre la policía trataba de resolver este problema ofreciendo orientaciones sobre cómo debía efectuarse la recogida de datos de carácter personal con fines policiales; cómo debían conservarse los ficheros de datos en este ámbito, incluidas las condiciones para transferir datos personales a autoridades personales extranjeras; cómo debían poder los interesados ejercitar sus derechos de protección de datos; y cómo debía llevarse a cabo el control por autoridades independientes. También se tuvo en cuenta la obligación de garantizar la seguridad de los datos de forma adecuada.

La Recomendación no contempla que las autoridades policiales puedan recoger datos de carácter personal de manera abierta e indiscriminada. La recogida de datos personales por parte de las autoridades policiales se limita a lo que sea necesario para la prevención de un peligro real o la supresión de un delito específico. La recogida de datos adicionales ha de estar basada en legislación nacional específica. El tratamiento de datos sensibles debe limitarse a lo que sea absolutamente necesario en el contexto de una investigación concreta.

Cuando se recogen datos personales sin el conocimiento del interesado, este debe ser informado de ello en el momento en que esa comunicación ya no sea perjudicial para la investigación. La recogida de datos mediante vigilancia técnica u otros medios automatizados también debe tener una base jurídica específica.

Ejemplo: En *Versini-Campinchi y Crasnianski contra Francia* ([738]), la demandante, una abogada, mantuvo una conversación telefónica con un cliente cuya línea telefónica había sido intervenida a petición de un juez instructor. La transcripción de la información demostró que había revelado información protegida por el privilegio de la profesión jurídica. El fiscal envió esta información al Colegio de Abogados, que sancionó a la demandante. El TEDH reconoció la existencia de una injerencia en el derecho al respeto de la vida privada y la correspondencia, no solo de la persona cuyo teléfono había sido intervenido, sino también de la demandante, cuya comunicación había sido interceptada y transcrita. La injerencia se había realizado con arreglo a la ley y perseguía el fin legítimo de la prevención del desorden. La demandante

([738]) TEDH, *Versini-Campinchi y Crasnianski contra Francia*, n.º 49176/11, 16 de junio de 2016.

había obtenido una revisión de la licitud de la entrega de la transcripción de los registros de la intervención telefónica en el contexto del procedimiento disciplinario iniciado contra ella. Aunque ella no había podido solicitar que se anulase la transcripción de la conversación telefónica, el TEDH consideró que había existido un examen efectivo capaz de limitar la injerencia denunciada a lo que fuera necesario en una sociedad democrática. El TEDH resolvió que el argumento de que la posibilidad de un procedimiento penal contra un abogado basado en la transcripción podía tener un efecto alarmante sobre la libertad de comunicación entre un abogado y su cliente y, por tanto, en el derecho de defensa de este último, no era creíble cuando la revelación realizada por la propia abogada podía suponer una conducta ilegal por su parte. En consecuencia, no se reconoció violación del artículo 8.

La Recomendación del CdE sobre la policía establece que, cuando se conservan datos personales, deben establecerse claras distinciones entre: datos administrativos y datos policiales; los datos personales de diferentes tipos de interesados, como sospechosos, condenados, víctimas y testigos; y datos considerados hechos irrefutables y otros basados en sospechas o especulaciones.

Los fines para los que pueden utilizarse los datos policiales deben tener limitaciones estrictas. Esto tiene consecuencias para la revelación de datos policiales a terceros: la transferencia o comunicación de dichos datos en el sector policial debe regirse por la existencia (o no) de un interés legítimo en la información. La transferencia o la comunicación de dichos datos fuera del sector policial solo deberá permitirse cuando exista una obligación o autorización legal clara.

Ejemplo: En *Karabeyoğlu contra Turquía* ([739]), el demandante, un juez, tenía sus líneas telefónicas intervenidas en el contexto de una investigación criminal sobre una organización ilegal a la que era sospechoso de pertenecer o a la que se creía que prestaba ayuda y asistencia. A raíz de la decisión de no enjuiciarle, el fiscal encargado de la investigación destruyó las grabaciones en cuestión. Sin embargo, una copia permanecía en posesión de los investigadores judiciales, que utilizaron el material relevante en el contexto de una investigación disciplinaria contra el demandante. El TEDH dictaminó que se había vulnerado la legislación pertinente, ya que la información se había utilizado con fines distintos de aquellos para los que se había obtenido

([739]) TEDH, *Karabeyoğlu contra Turquía*, n.º 30083/10, 7 de junio de 2016.

y no se había destruido en el plazo legal establecido. La injerencia en el derecho del demandante al respeto de su vida privada no se había realizado conforme a la ley en lo que respectaba al procedimiento disciplinario seguido contra él.

La transferencia o comunicación internacional debe quedar limitada a las autoridades policiales extranjeras y estar basada en disposiciones jurídicas especiales —posiblemente acuerdos internacionales—, salvo que resulte necesaria para evitar un peligro grave e inminente.

El tratamiento de datos por parte de la policía debe estar sujeto a un control independiente para garantizar el cumplimiento de la legislación nacional en materia de protección de datos. Los interesados deben disponer de todos los derechos de acceso reconocidos en el Convenio 108 modernizado. Cuando los derechos de acceso de los interesados hayan sido limitados con arreglo a lo dispuesto en el artículo 9 del Convenio 108, en interés de la eficacia de las investigaciones policiales y la aplicación de sanciones penales, el interesado debe tener derecho, con arreglo a la legislación nacional, a recurrir a la autoridad nacional de control en materia de protección de datos o a otro órgano independiente.

8.1.2. El Convenio de Budapest sobre la Ciberdelincuencia

Dado que las actividades delictivas utilizan y afectan de forma creciente a los sistemas electrónicos de tratamiento de datos, son necesarias nuevas disposiciones jurídicas penales para afrontar este reto. Por este motivo, el CdE adoptó un instrumento jurídico internacional —el Convenio sobre la Ciberdelincuencia, también conocido como Convenio de Budapest— para tratar la cuestión de los delitos cometidos contra y a través de redes electrónicas ([740]). Este Convenio también está abierto a la adhesión de países que no sean miembros del CdE. A comienzos del año 2018, catorce Estados no miembros del CdE ([741]) eran partes del Convenio y otros siete lo habían firmado o habían sido invitados a adherirse.

([740]) Consejo de Europa, Comité de Ministros (2001), Convenio sobre la Ciberdelincuencia, STE n.º 185, Budapest, 23 de noviembre de 2001, que entró en vigor el 1 de julio de 2004.

([741]) Australia, Canadá, Chile, los Estados Unidos, Israel, Japón, Mauricio, Panamá, República Dominicana, Senegal, Sri Lanka y Tonga. Véase la Lista de firmas y ratificaciones del Tratado 185 a fecha de julio de 2017.

El Convenio sobre la Ciberdelincuencia sigue siendo el tratado internacional más influyente en relación con los incumplimientos de la legislación sobre internet u otras redes de información. Exige a las partes que actualicen y armonicen sus legislaciones penales contra la piratería y otras infracciones de la seguridad incluidas las infracciones de los derechos de autor, fraudes informáticos, pornografía infantil y otras ciberactividades ilícitas. El Convenio también establece competencias de procedimiento que comprenden el registro de redes informáticas y la intervención de comunicaciones en el contexto de la lucha contra la ciberdelincuencia. Por último, permite una cooperación internacional eficaz. Un protocolo adicional al Convenio trata de la tipificación de la propaganda racista y xenófoba en redes informáticas.

Aunque el Convenio no es un instrumento destinado a fomentar la protección de datos, tipifica actividades que pueden violar el derecho del interesado a la protección de sus datos. Además, exige que las Partes Contratantes adopten medidas legislativas que permitan a sus autoridades nacionales interceptar datos relativos al tráfico y al contenido ([742]). También obliga a las Partes Contratantes, a la hora de aplicar el Convenio, a prever una protección adecuada de los derechos y libertades humanos y, en particular, de los derechos garantizados por el CEDH, como el derecho a la protección de datos ([743]). Las Partes Contratantes no están obligadas a adherirse también al Convenio 108 para poder incorporarse al Convenio de Budapest sobre la ciberdelincuencia.

8.2. Derecho del CdE sobre la protección de datos en asuntos de la policía y la justicia penal

Puntos clave

- En la UE, la protección de datos en el sector de la policía y la justicia penal está regulado en el contexto del tratamiento tanto nacional como transfronterizo por las autoridades policiales y de justicia penal de los Estados miembros y de la UE.
- A escala de los Estados miembros, se requiere la transposición de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal.

([742]) Consejo de Europa, Comité de Ministros (2001), Convenio sobre la Ciberdelincuencia, STE n.º 185, Budapest, 23 de noviembre de 2001, artículos 20 y 21.

([743]) Ibíd., artículo 15, apartado 1.

- La protección de datos en la cooperación transfronteriza entre cuerpos policiales y servicios de seguridad, especialmente para combatir el terrorismo y la delincuencia transfronteriza, se rige por instrumentos jurídicos específicos.
- Existen normas de protección de datos especiales para la Oficina Europea de Policía (Europol) y la unidad de cooperación judicial de la UE (Eurojust), así como la Fiscalía Europea de reciente creación, que son organismos de la UE que prestan asistencia y promueven la aplicación transfronteriza de la ley.
- También existen normas especiales de protección de datos para los sistemas comunes de información que se han establecido a escala de la UE para el intercambio transfronterizo de información entre las autoridades policiales y judiciales competentes. Como ejemplos importantes cabe mencionar el Sistema de Información de Schengen II (SIS II), el Sistema de Información de Visados (VIS) y Eurodac, un sistema centralizado que contiene los datos de impresiones dactilares de nacionales de terceros países y apátridas que solicitan asilo en uno de los Estados miembros.
- La UE está en proceso de actualización de los sistemas de protección de datos mencionados, para que se ajusten a las disposiciones de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal.

8.2.1. La Directiva sobre protección de datos para las autoridades policiales y de justicia penal

La Directiva 2016/680/UE 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 (Directiva sobre protección de datos para las autoridades policiales y de justicia penal) ([744]), tiene por objeto la protección de los datos personales recogidos y tratados para los fines de la justicia penal, como son:

- la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública;
- la ejecución de una sanción penal; y

([744]) Directiva 2016/680/UE 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 2016 L 119, p. 89 (Directiva sobre protección de datos para las autoridades policiales y de justicia penal).

- en los casos en que la policía u otras fuerzas y cuerpos de seguridad actúen en defensa de la ley y como protección y prevención frente a las amenazas para la seguridad pública y para los derechos fundamentales de la sociedad que puedan ser constitutivas de infracciones penales.

La Directiva sobre protección de datos para las autoridades policiales y de justicia penal protege los datos personales de diferentes categorías de personas físicas implicadas en procesos penales, como testigos, informadores, víctimas, sospechosos y cómplices. Las autoridades policiales y de justicia penal están obligadas a cumplir las disposiciones de la Directiva siempre que lleven a cabo el tratamiento de este tipo de datos personales con fines de aplicación de la ley, tanto en el ámbito personal como material de la Directiva ([745]).

Sin embargo, en determinadas circunstancias se admite el uso de los datos con un fin diferente. El tratamiento de datos con un fin de aplicación de la ley diferente a aquel para el que han sido recogidos solo está permitido si es lícito, necesario y proporcionado conforme al Derecho del Estado miembro o de la Unión ([746]). Para otros fines, se aplican las disposiciones del Reglamento general de protección de datos. El registro y la documentación de los intercambios de datos constituyen uno de los deberes específicos de las autoridades competentes para contribuir a aclarar las responsabilidades derivadas de las reclamaciones.

Las autoridades competentes en el área de la policía y la justicia penal son autoridades públicas o autoridades facultadas por la legislación nacional y los poderes públicos para desempeñar las funciones de una autoridad pública ([747]), por ejemplo, los centros penitenciarios de gestión privada ([748]). La aplicabilidad de la Directiva se extiende tanto al tratamiento de datos de ámbito nacional como al de ámbito transfronterizo entre las autoridades policiales y de justicia penal de los Estados

([745]) Directiva sobre protección de datos para las autoridades policiales y de justicia penal, artículo 2, apartado 1.

([746]) Ibíd., artículo 4, apartado 2.

([747]) Ibíd., artículo 3, apartado 7.

([748]) Comisión Europea (2016), Comunicación de la Comisión al Parlamento Europeo con arreglo al artículo 294, apartado 6, del Tratado de Funcionamiento de la Unión Europea sobre la posición del Consejo acerca de la adopción de una Directiva del Parlamento Europeo y del Consejo 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, COM(2016) 213 final, Bruselas, 11 de abril de 2016.

miembros, así como a las transferencias internacionales realizadas por las autoridades competentes a terceros países y organizaciones internacionales ([749]). No comprende la seguridad nacional ni el tratamiento de datos personales por instituciones, organismos, oficinas y agencias de la UE ([750]).

La Directiva se basa, en gran medida, en los principios y definiciones que contiene el Reglamento general de protección de datos, teniendo en cuenta la naturaleza específica de los ámbitos de la policía y la justicia penal. El control puede ser ejercido por las mismas autoridades de los Estados miembros que lo ejercen también en virtud del Reglamento general de protección de datos. El nombramiento de delegados de protección de datos y las evaluaciones de impacto de la protección de datos se han introducido en la Directiva como nuevas obligaciones de las autoridades policiales y de justicia penal ([751]). Aunque estos conceptos se inspiran en el Reglamento general de protección de datos, la Directiva trata de la naturaleza específica de las autoridades policiales y de justicia penal. En comparación con el tratamiento de datos con fines comerciales, que está regulado por el Reglamento, el tratamiento relacionado con la seguridad puede requerir cierto grado de flexibilidad. Por ejemplo, el hecho de conferir a los interesados el mismo nivel de protección en términos de derecho de información, acceso o supresión de sus datos personales de que gozan en virtud del Reglamento general de protección de datos podría implicar que una operación de vigilancia realizada con fines de aplicación de la ley fuera ineficaz en el contexto de estos fines. Por consiguiente, la Directiva no contiene el principio de transparencia. Del mismo modo, los principios de minimización de datos y de limitación a una finalidad específica, que exigen que los datos personales se limiten únicamente a lo que sea necesario en relación con los fines para los que sean tratados y que se traten con objetivos específicos y explícitos, también deben aplicarse con flexibilidad en el tratamiento relacionado con la seguridad. La información recogida y conservada por las autoridades competentes para un caso concreto puede resultar muy útil para resolver casos futuros.

Principios relativos al tratamiento

La Directiva sobre protección de datos para las autoridades policiales y de justicia penal establece algunas garantías clave en relación con el uso de datos personales.

([749]) Directiva sobre protección de datos para las autoridades policiales y de justicia penal, capítulo V.

([750]) Ibíd., artículo 2, apartado 3.

([751]) Ibíd., en los artículos 32 y 27, respectivamente.

También explica con detalle los principios por los que se rige el tratamiento de estos datos. Los Estados miembros deben asegurarse de que los datos personales sean:

- tratados de manera lícita y leal;
- recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines;
- adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados;
- exactos y, si fuera necesario, actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados;
- conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados;
- tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas ([752]).

De acuerdo con la Directiva, el tratamiento solo es lícito en la medida en que sea necesario para la ejecución de una función pertinente. Además, debe ser realizado por una autoridad competente para lograr los fines especificados en la Directiva y estar basado en el Derecho de la Unión o del Estado miembro ([753]). Los datos no deben ser conservados durante más tiempo del necesario y deben ser eliminados o revisados periódicamente dentro de determinados plazos. Solo deben ser utilizados por una autoridad competente y para los fines para los que se hayan recogido, transmitido o puestos a disposición.

Derechos del interesado

La Directiva también establece los derechos del interesado. Entre estos cabe incluir los siguientes:

([752]) Ibíd., artículo. 4 apartado 1.

([753]) Ibíd., artículo 8.

- El derecho a recibir información. Los Estados miembros deben obligar al responsable del tratamiento a poner a disposición del interesado: 1) la identidad y los datos de contacto del responsable del tratamiento; 2) los datos de contacto del delegado de protección de datos; 3) los fines del tratamiento previsto; 4) el derecho a presentar una reclamación ante la autoridad de control y sus datos de contacto; y 5) el derecho de acceso a los datos personales y su rectificación o supresión, así como la limitación de su tratamiento ([754]). Además de estos requisitos de información general, la Directiva establece que, en determinados casos y a fin de permitir el ejercicio de sus derechos, el responsable del tratamiento debe facilitar al interesado información acerca de la base jurídica del tratamiento y del plazo durante el cual se conservarán los datos. Si los datos personales van a ser transmitidos a otros destinatarios, en particular en terceros países u organizaciones internacionales, se deberán comunicar a los interesados las categorías de dichos destinatarios. Por último, los responsables del tratamiento deben facilitar cualquier otra información, teniendo en cuenta las circunstancias concretas en las que se hayan recogido los datos: por ejemplo, cuando se hayan recogido durante una operación de vigilancia encubierta, es decir, sin conocimiento del interesado. De este modo se garantiza el leal tratamiento respecto del interesado ([755]).

- El derecho de acceso a los datos personales. Los Estados miembros deben garantizar que el interesado goce del derecho a saber si sus datos personales están siendo objeto de tratamiento. De ser así, el interesado deberá tener acceso a determinada información, como las categorías de datos objeto de tratamiento ([756]). Sin embargo, este derecho puede ser limitado: por ejemplo, para evitar que se obstaculicen investigaciones o que se cause perjuicio a la persecución de un delito o para proteger la seguridad pública y los derechos y libertades de otras personas ([757]).

- El derecho de rectificación de los datos personales. Los Estados miembros están obligados a garantizar que el interesado pueda obtener, sin dilación indebida, la rectificación de datos personales incorrectos. Además, el interesado tiene derecho a que se completen los datos personales que sean incompletos ([758]).

([754]) Ibíd., artículo 13, apartado 1.

([755]) Ibíd., artículo 13, apartado 2.

([756]) Ibíd., artículo 14.

([757]) Ibíd., artículo 15.

([758]) Ibíd., artículo 16, apartado 1.

- El derecho de supresión de los datos personales y limitación de su tratamiento. En algunos casos, el responsable del tratamiento necesita suprimir los datos personales. Además, el interesado puede obtener la supresión de sus datos personales, pero solo cuando sean objeto de un tratamiento ilícito ([759]). En algunas situaciones, en lugar de suprimir los datos, se puede limitar su tratamiento. Esto puede ocurrir cuando 1) se haya puesto en duda la exactitud de los datos personales, pero no pueda determinarse la exactitud o inexactitud o 2) cuando los datos personales hayan de conservarse a efectos probatorios ([760]).

Cuando el responsable del tratamiento se niegue a rectificar o suprimir datos personales o a limitar su tratamiento, deberá comunicar este hecho al interesado por escrito. Los Estados miembros podrán limitar este derecho a la información para, entre otras cosas, proteger la seguridad pública o los derechos y libertades de otras personas, por las mismas razones que para limitar el derecho de acceso ([761]).

Normalmente, el interesado tiene derecho a recibir información acerca del tratamiento de sus datos personales y los derechos de acceso, rectificación y supresión de los datos o limitación de su tratamiento, que puede ejercer directamente ante el responsable del tratamiento. La Directiva sobre protección de datos para las autoridades policiales y de justicia penal contempla que estos derechos también se puedan ejercer de manera indirecta a través de la autoridad de control competente cuando el responsable del tratamiento limite los derechos del interesado ([762]). El artículo 17 de la Directiva establece que los Estados miembros deberán adoptar medidas que garanticen que los interesados también puedan ejercer sus derechos a través de su autoridad de control. Por esta razón, el responsable del tratamiento debe informar al interesado de la posibilidad de acceso indirecto.

Obligaciones del responsable y del encargado del tratamiento

En el contexto de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal, los responsables del tratamiento son autoridades públicas competentes, u otros organismos con los poderes públicos y la autoridad pública pertinentes, que determinan los fines y los medios del tratamiento de los datos personales. La Directiva establece varias obligaciones para los responsables del

([759]) Ibíd., artículo 16, apartado 2.

([760]) Ibíd., artículo 16, apartado 3.

([761]) Ibíd., artículo 16, apartado 4.

([762]) Ibíd., artículo 17.

tratamiento con el fin de garantizar un alto nivel de protección de los datos personales tratados con fines de aplicación de la ley.

Las autoridades competentes deben conservar registros de las operaciones de tratamiento que realicen en sistemas de tratamiento automatizados. Deben registrase al menos las operaciones de recogida, alteración, consulta, comunicación incluidas las transferencias, combinación o supresión de los datos personales ([763]). La Directiva establece que los registros de consulta y comunicación deben hacer posible que se determine la fecha y la hora de las operaciones, su justificación y, en la medida de lo posible, la identificación de la persona que haya consultado el sistema o comunicado los datos personales, y los destinatarios de dichos datos personales. Los registros deberán utilizarse únicamente a efectos de verificar la legalidad del tratamiento, autocontrol, garantizar la integridad y la seguridad de los datos personales y en el ámbito de los procesos penales ([764]). A petición de la autoridad de control, el responsable y el encargado del tratamiento deberán poner los registros a su disposición.

En particular, los responsables del tratamiento tienen la obligación general de aplicar las medidas técnicas y organizativas apropiadas para garantizar que el tratamiento se lleve a cabo de conformidad con la Directiva y estar en condiciones de demostrar la licitud de dicho tratamiento ([765]). En el momento de formular dichas medidas, deben tener en cuenta la naturaleza, el ámbito y el contexto del tratamiento y, de manera especialmente importante, cualquier posible riesgo existente para los derechos y libertades de las personas físicas. Los responsables del tratamiento deben adoptar políticas internas y aplicar medidas que faciliten el cumplimiento de los principios de la protección de datos, en particular el principio de protección de datos desde el diseño y por defecto ([766]). Cuando el tratamiento pueda entrañar un alto riesgo para los derechos de las personas físicas —debido al uso de nuevas tecnologías, por ejemplo—, los responsables del tratamiento deberán realizar una evaluación de impacto de la protección de datos antes de iniciar el tratamiento ([767]). La Directiva también recoge las medidas que deben aplicar los responsables para garantizar la seguridad del tratamiento, como por ejemplo medidas para prevenir accesos no autorizados a los datos personales que tratan, garantizar que las personas autorizadas solo tengan acceso a los datos personales para los que hayan sido

([763]) Ibíd., artículo 25 apartado 1.

([764]) Ibíd., artículo 25, apartado 2.

([765]) Ibíd., artículo 19.

([766]) Ibíd., artículo 20.

([767]) Ibíd., artículo 27.

autorizados, que las funciones del sistema de tratamiento no presenten defectos, y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema ([768]). En el caso de que se produzca una violación de la seguridad de los datos personales, los responsables del tratamiento deben notificar este hecho a la autoridad de control en un plazo de tres días, con una descripción de la naturaleza de la violación, sus posibles consecuencias, las categorías de datos personales a que afecte y el número aproximado de interesados respectivos que hayan resultado afectados. La violación de la seguridad de los datos personales también debe comunicarse al interesado «sin dilación indebida» cuando dicha violación pueda entrañar un alto riesgo para sus derechos y libertades ([769]).

La Directiva contiene el principio de rendición de cuentas, que obliga a los responsables del tratamiento a aplicar medidas que garanticen el cumplimiento de ese principio. Los responsables deben conservar registros de todas las categorías de actividades de tratamiento bajo su responsabilidad: en el artículo 24 de la Directiva se especifica con detalle el contenido de esos registros. Los registros deben ponerse a disposición de la autoridad de control cuando lo solicite, para que puedan supervisar las operaciones de tratamiento realizadas por el responsable. Otra medida importante para reforzar la rendición de cuentas es la designación de un delegado de protección de datos (DPD). Los responsables deben designar un DPD, aunque la Directiva permite que los Estados miembros eximan de tal obligación a los tribunales y demás autoridades judiciales independientes ([770]). Las obligaciones del DPD son parecidas a las recogidas en el Reglamento general de protección de datos. Supervisa el cumplimiento de la Directiva, informa y asesora a los empleados que llevan a cabo labores de tratamiento de datos acerca de sus obligaciones conforme a la legislación en materia de protección de datos. El DPD también ofrece asesoramiento acerca de la necesidad de llevar a cabo una evaluación de impacto relativa a la protección de datos y actúa como punto de contacto de la autoridad de control.

Transferencias a terceros países u organizaciones internacionales

De manera similar a lo que ocurre con el Reglamento general de protección de datos, la Directiva establece condiciones para la transferencia de datos personales a terceros países u organizaciones internacionales. Si se transmitieran datos personales libremente fuera de la jurisdicción de la UE, las garantías y el alto nivel de protección

([768]) Ibíd., artículo 29.

([769]) Ibíd., artículos 30 y 31.

([770]) Ibíd., artículo 32.

que confiere el Derecho de la UE podrían verse menoscabados. Sin embargo, las condiciones propiamente dichas son bastante diferentes de las establecidas en el Reglamento general de protección de datos. La transferencia de datos personales a terceros países u organizaciones internacionales se permite en los siguientes casos ([771]):

- cuando la transferencia es necesaria para los objetivos de la Directiva;
- cuando los datos personales se transfieren a una autoridad competente, en el sentido de la Directiva, del país tercero u organización internacional (aunque existe una excepción a esta norma en casos particulares y específicos) ([772]);
- cuando la transferencia a terceros países u organizaciones internacionales de datos personales recibidos en virtud de una cooperación transfronteriza requiere la autorización del Estado miembro de origen de los datos (aunque existen excepciones para casos de urgencia);
- cuando la Comisión Europea ha adoptado una decisión de adecuación, cuando se han establecido garantías apropiadas o cuando se aplican excepciones para situaciones específicas;
- cuando las transferencias ulteriores de datos personales a otro tercer país u organización internacional requieren la autorización previa de la autoridad competente de origen, que tendrá en cuenta, entre otras cosas, la gravedad de la infracción y el nivel de protección de datos existente en el país de destino de la segunda transferencia internacional ([773]).

De acuerdo con la Directiva, pueden realizarse transferencias de datos personales si se cumple una de las tres condiciones que se indican a continuación. La primera es cuando la Comisión Europea ha adoptado una decisión de adecuación conforme a la Directiva. Esta decisión puede aplicarse a todo el territorio de un tercer país o a sectores específicos de ese tercer país o a una organización internacional. Sin embargo, esto solo puede hacerse si se garantiza un nivel de protección adecuado y se cumplen las condiciones definidas en la Directiva ([774]). En estos casos, la transfe-

([771]) Ibíd., artículo 35.

([772]) Ibíd., artículo 39.

([773]) Ibíd., artículo 35, apartado 1.

([774]) Ibíd., artículo 36.

rencia de datos personales no está sujeta a la autorización del Estado miembro ([775]). La Comisión Europea ha de supervisar los acontecimientos que puedan afectar al funcionamiento de las decisiones de adecuación. Además, la decisión debe incluir un mecanismo de revisión periódica. La Comisión también puede derogar, modificar o suspender una decisión cuando la información disponible revele que las circunstancias existentes en el tercer país u organización internacional ya no garantizan un nivel adecuado de protección. En ese caso, la Comisión ha celebrar consultas con el país tercero u organización internacional para tratar de corregir la situación.

En ausencia de una decisión de adecuación, las transferencias pueden basarse en garantías adecuadas, que pueden estar recogidas en un instrumento jurídicamente vinculante, o bien el responsable del tratamiento puede llevar a cabo su propia evaluación de las circunstancias que rodean a la transferencia de los datos personales y llegar a la conclusión de que existen garantías adecuadas. En su evaluación, debe tener en cuenta los acuerdos de cooperación que puedan haberse celebrado entre Europol o Eurojust y el tercer país u organización internacional, la existencia de obligaciones de confidencialidad y la limitación de la finalidad, así como las garantías que se ofrezcan de que los datos no se utilizarán para ninguna forma de trato cruel o inhumano, incluida la pena de muerte ([776]). En este último caso, el responsable del tratamiento debe comunicar las categorías de transferencias comprendidas en esta categoría a la autoridad de control competente ([777]).

Cuando no se haya adoptado una decisión de adecuación o no se hayan establecido garantías adecuadas, todavía podrán autorizarse transferencias en situaciones específicas descritas en la Directiva, que incluyen, entre otras, la protección de los intereses vitales del interesado o de otra persona y la prevención de una amenaza grave e inmediata para la seguridad del Estado miembro o del tercer país ([778]).

En casos particulares y específicos, las autoridades competentes podrán realizar transferencias a destinatarios establecidos en terceros países que no sean autoridades competentes si, además de cumplirse una de las tres condiciones antes descritas, se cumplen también las condiciones adicionales recogidas en el artículo 39 de la Directiva. En particular, la transferencia debe ser estrictamente necesaria para la realización de una función de la autoridad competente de la transferencia, que

([775]) Ibíd., artículo 36, apartado 1.

([776]) Ibíd., considerando 71.

([777]) Ibíd., artículo 37, apartado 1.

([778]) Ibíd., artículo. 38 apartado 1.

también debe determinar que ninguno de los derechos y libertades fundamentales de los interesados sea superior al interés público que justifique la transferencia. Estas transferencias deben documentarse y la autoridad competente de la transferencia ha de informar a la autoridad de control competente ([779]).

Por último, y en relación con los terceros países y las organizaciones internacionales, la Directiva obliga además a crear mecanismos de cooperación internacional que faciliten la aplicación efectiva de la legislación y que ayuden así a las autoridades de control de la protección de datos a cooperar con sus homólogos extranjeros ([780]).

Control independiente y tutela judicial de los interesados

Cada Estado miembro debe garantizar que una o más autoridades nacionales de control independientes se encarguen de asesorar y supervisar la aplicación de las disposiciones adoptadas con arreglo a la Directiva ([781]). La autoridad de control constituida para los fines de la Directiva debe ser la misma autoridad de control constituida con arreglo al Reglamento general de protección de datos, pero los Estados miembros tienen libertad para designar una autoridad diferente, siempre que cumpla los criterios de independencia. Las autoridades de control también entenderán de las reclamaciones presentadas por cualquier persona en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales por parte de las autoridades competentes.

Cuando el ejercicio de los derechos del interesado sea denegado por motivos imperiosos, el interesado deberá tener derecho a recurrir ante la autoridad nacional de control o ante un órgano jurisdiccional. Si una persona sufre daños y perjuicios como consecuencia de una vulneración de las disposiciones nacionales de transposición de la Directiva, tendrá derecho a recibir una indemnización del responsable o de cualquier otra autoridad competente en virtud del Derecho del Estado miembro ([782]). En general, los interesados tendrán derecho a la tutela judicial efectiva en caso de violación de los derechos que les garanticen las disposiciones de Derecho nacional de transposición de la Directiva ([783]).

([779]) Ibíd., artículo 37, apartado 3.

([780]) Ibíd., artículo 40.

([781]) Ibíd., artículo 41.

([782]) Ibíd., artículo 56.

([783]) Ibíd., artículo 54.

8.3. Otros instrumentos jurídicos específicos sobre protección de datos en materia de aplicación de la ley

Además de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal, el intercambio de la información que poseen los Estados miembros en ámbitos concretos se rige por distintos instrumentos jurídicos, como la Decisión marco 2009/315/JAI del Consejo relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros, la Decisión 2000/642/JAI del Consejo relativa a las disposiciones de cooperación entre las unidades de información financiera de los Estados miembros para el intercambio de información, y la Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea ([784]).

Un aspecto importante es que, en la cooperación transfronteriza ([785]) entre las autoridades competentes, es cada vez más necesario el intercambio de datos de inmigración. Este ámbito del Derecho no se considera parte de los asuntos de la policía y justicia penal, aunque, en muchos aspectos, es relevante para el trabajo de las autoridades policiales y judiciales. Lo mismo puede decirse de los datos sobre las mercancías que se importan o se exportan en la UE. La eliminación de los controles fronterizos interiores en el espacio Schengen ha aumentado el riesgo de fraude y ha hecho necesario que los Estados miembros intensifiquen su cooperación, en especial mejorando el intercambio transfronterizo de información, para detectar y perseguir de un modo más eficaz las violaciones de las legislaciones aduaneras nacionales y de la UE. Además, en los últimos años el mundo ha sido testigo de un incremento de la delincuencia grave y organizada y del terrorismo, que puede afectar a los desplazamientos internacionales, y ha puesto de manifiesto la necesidad de reforzar la

([784]) Consejo de la Unión Europea (2009), Decisión marco 2009/315/JAI del Consejo, de 26 de febrero de 2009, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros, DO 2009 L 93; Consejo de la Unión Europea (2000), Decisión 2000/642/JAI del Consejo, de 17 de octubre de 2000, relativa a las disposiciones de cooperación entre las unidades de información financiera de los Estados miembros para el intercambio de información DO 2000 L 271; Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, DO L 386.

([785]) Comisión Europea (2012), Comunicación de la Comisión al Parlamento Europeo y al Consejo, Refuerzo de la cooperación en materia de aplicación de la ley en la UE: el Modelo Europeo para el intercambio de información (EIXM), COM (2012) 735 final, Bruselas, 7 de diciembre de 2012.

cooperación transfronteriza en materia policial y de aplicación de la ley en muchos casos ([786]).

La decisión Prüm

Un importante ejemplo de cooperación transfronteriza institucionalizada mediante el intercambio de los datos que se conservan en el ámbito nacional es la Decisión 2008/615/JAI del Consejo, junto con sus disposiciones de ejecución sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (Decisión Prüm), que incorporaba, en 2008, el Tratado de Prüm a la legislación de la Unión Europea ([787]). El Tratado de Prüm fue un acuerdo internacional de cooperación policial firmado en 2005 por Alemania, Austria, Bélgica, España, Francia, Luxemburgo y los Países Bajos ([788]).

La Decisión Prüm tiene por objeto ayudar a los Estados miembros signatarios a mejorar el intercambio de información con fines de prevención de la delincuencia en tres ámbitos: el terrorismo, la delincuencia transfronteriza y la migración ilegal. Para ello, la Decisión establece disposiciones relativas a:

- el acceso automatizado a perfiles de ADN, datos de dactiloscópicos y ciertos datos de los registros nacionales de matriculación de vehículos;
- el suministro de datos relacionados con acontecimientos importantes que tengan una dimensión transfronteriza;
- el suministro de información con el fin de prevenir atentados terroristas;
- otras medidas de intensificación de la cooperación policial transfronteriza.

([786]) Véase Comisión Europea (2011), Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, COM(2011) 32 final, Bruselas, 2 de febrero de 2011, p. 1.

([787]) Consejo de la Unión Europea (2008), Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, DO 2008 L 210.

([788]) Convenio entre el Reino de Bélgica, la República Federal de Alemania, el Reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal.

Las bases de datos que se ponen a disposición en virtud de la Decisión Prüm se rigen enteramente por el Derecho nacional, pero el intercambio de datos se rige además por esta Decisión, cuya compatibilidad con la Directiva sobre protección de datos para las autoridades policiales y de justicia penal tendrá que ser evaluada. Los órganos competentes de control de dichos flujos de datos son las autoridades nacionales de control de la protección de datos.

Decisión marco 2006/960/JAI: la Iniciativa Sueca

La Decisión marco 2006/960/JAI (iniciativa sueca) ([789]) representa otro ejemplo de cooperación transfronteriza con respecto al intercambio de los datos que poseen los cuerpos de seguridad de ámbito nacional. La Iniciativa Sueca se centra específicamente en el intercambio de información e inteligencia y establece normas concretas de protección de datos en su artículo 8.

De acuerdo con este instrumento, la utilización de la información e inteligencia que se intercambien debe estar sujeta a las disposiciones nacionales sobre protección de datos del Estado miembro receptor, con arreglo a las mismas normas que si hubieran sido recabadas en ese Estado miembro. El artículo 8 va más lejos y establece que, cuando se proporcione información e inteligencia, los servicios de seguridad competentes podrán imponer condiciones que se ajusten a lo dispuesto en su legislación nacional sobre su utilización por los servicios de seguridad receptores. Dichas condiciones también podrán aplicarse a la comunicación del resultado de la investigación penal o a las operaciones de investigación penal en cuyo contexto haya sido necesario el intercambio de información e inteligencia. Sin embargo, cuando la legislación nacional establezca excepciones a las limitaciones de uso (p.ej. para autoridades judiciales, órganos legislativos, etc.), la información e inteligencia solo podrá utilizarse previa consulta con el Estado miembro transmisor.

La información e inteligencia proporcionada podrá utilizarse:

- para los fines para los que haya sido suministrada; o bien
- para la prevención de amenazas inmediatas y graves a la seguridad pública.

([789]) Consejo de la Unión Europea (2006), Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea, DO L 386/89, de 29 de diciembre de 2006.

Es admisible el tratamiento con otros fines, pero únicamente previa autorización del Estado miembro transmisor.

La Iniciativa Sueca establece además que los datos personales tratados deben ser protegidos con arreglo a instrumentos internacionales como los siguientes:

- Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal ([790]).

- Protocolo adicional de 8 de noviembre de 2001 al citado Convenio, en lo que respecta a las autoridades de control y los flujos de datos transfronterizos ([791]).

- Recomendación n.º R(87)15 del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía ([792]).

La Directiva PNR

Los datos de los registros de nombres de pasajeros (PNR, por sus siglas en inglés) contienen información acerca de los pasajeros aéreos que son recogidos y conservados en los sistemas de control de reservas y salidas gestionados por las compañías aéreas para sus propios fines comerciales. Estos datos contienen distintos tipos de información, como las fechas de viaje, el itinerario, información sobre el billete, datos de contacto, la agencia de viajes con la que se reservó el vuelo, el medio de pago utilizado, el número de asiento e información sobre el equipaje ([793]). El tratamiento de los datos del PNR puede ayudar a los servicios de seguridad a identificar a los sospechosos conocidos o potenciales y realizar análisis basados en los patrones de viaje y otros indicadores típicamente asociados a las actividades delictivas. El análisis de los datos del PNR también permite vigilar de forma

([790]) Consejo de Europa (1981), Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, STE n.º 108.

([791]) Consejo de Europa (2001), Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en lo que respecta a las autoridades de control y los flujos de datos transfronterizos, STE n.º 108.

([792]) Consejo de Europa (1987), Recomendación n.º R (87)15 del Comité de Ministros a los Estados miembros dirigida a regular la utilización de datos de carácter personal en el sector de la policía (adoptada por el Comité de Ministros el 17 de septiembre de 1987 en la 410.ª reunión de los Delegados de los Ministros).

([793]) Comisión Europea (2011), Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos terroristas y delitos graves, COM (2011) 32 final, Bruselas, 2 de febrero de 2011, p. 1.

retrospectiva los itinerarios de viaje y los contactos de las personas sospechosas de haber participado en actividades delictivas, que pueden ayudar a los servicios de seguridad a identificar las redes criminales ([794]). La UE ha celebrado algunos acuerdos con terceros países para el intercambio de datos PNR, como se explica en el capítulo 7. Además, ha introducido el tratamiento de los datos PNR en la UE por medio de la Directiva 2016/681/UE 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 (Directiva PNR) ([795]). Esta Directiva obliga a las compañías aéreas a transmitir los datos PNR a las autoridades competentes y establece rigurosas garantías de protección de datos en relación con el tratamiento y la obtención de dichos datos. La PNR se aplica a los vuelos internacionales con origen y destino en la UE, pero también a los vuelos interiores de la UE si un Estado miembro así lo decide ([796]).

Los datos PNR obtenidos deben contener únicamente la información que permite la Directiva PNR. Deben conservarse en una única unidad de información, en un lugar seguro en cada Estado miembro. Los datos PNR deben ser despersonalizados al cabo de seis meses de su transmisión por parte de la compañía aérea y conservados durante un plazo máximo de cinco años ([797]). Los datos PNR se intercambian entre Estados miembros; entre los Estados miembros y Europol; y con terceros países, pero caso por caso.

La transmisión y el tratamiento de los datos PNR y los derechos garantizados a los interesados deben ajustarse a lo dispuesto en la Directiva sobre protección de datos para las autoridades policiales y de justicia penal, y deben garantizar el alto nivel de protección de la privacidad y los datos personales que exigen la Carta, el Convenio 108 modernizado y el CEDH.

Las autoridades nacionales de control independiente competentes en virtud de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal también tienen la responsabilidad de asesorar sobre y vigilar la aplicación de las

([794]) Comisión Europea (2015), Hoja informativa sobre la lucha contra el terrorismo en el ámbito de la UE: panorámica de las acciones, medidas e iniciativas de la Comisión, Bruselas, 11 de enero de 2015.

([795]) 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, DO 2016 L 119, p. 132.

([796]) Directiva PNR, L 119, p. 132, artículo 1, apartado 1 y artículo 2, apartado 1.

([797]) Ibíd., artículo 12, apartados 1 y 2.

disposiciones adoptadas por los Estados miembros de conformidad con la Directiva PNR.

Conservación de datos de telecomunicaciones

La Directiva sobre la conservación de datos ([798]) —declarada inválida el 8 de abril de 2014 en el asunto *Digital Rights Ireland*— obligaba a los proveedores de servicios de comunicaciones a mantener los metadatos disponibles, con el fin específico de combatir la delincuencia grave, durante un mínimo de seis y un máximo de veinticuatro meses, al margen de que el proveedor necesitara o no dichos datos con fines de facturación o de prestación técnica del servicio.

La conservación de los datos de telecomunicaciones constituye una clara injerencia en el derecho a la protección de los datos ([799]). En los Estados miembros se han llevado a cabo varios procedimientos judiciales para determinar si esta injerencia está justificada o no ([800]).

Ejemplo: En *Digital Rights Ireland* y *Kärntner Landesregierung y otros* ([801]), el grupo Digital Rights y el Sr. Seitlinger interpusieron una demanda ante la High Court de Irlanda y el Tribunal Constitucional de Austria, respectivamente, impugnando la legalidad de las medidas nacionales que permitían la conservación de datos de telecomunicaciones electrónicas. Digital Rights solicitó al órgano jurisdiccional irlandés que declarase inválida la Directiva 2006/24 y la parte del Derecho penal nacional relativa a los delitos de terrorismo. Del mismo modo, el Sr. Seitlinger, junto con otros

([798]) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios en comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DO 2006 L 105.

([799]) SEPD (2011), Dictamen de 31 de mayo de 2011 relativo al Informe de evaluación de la Comisión al Consejo y al Parlamento Europeo sobre la Directiva sobre la conservación de datos (Directiva 2006/24/CE), 31 de mayo de 2011.

([800]) Alemania, Tribunal Constitucional Federal (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 de marzo de 2010; Rumanía, Tribunal Constitucional Federal (*Curtea Constituțională a României*), No. 1258, 8 de octubre de 2009; República Checa, Tribunal Constitucional (*Ústavní soud České republiky*), 94/2011 Coll., 22 de marzo de 2011.

([801]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros* [GS], 8 de abril de 2014, apartado 65.

más de 11 000 demandantes, impugnaron y solicitaron la anulación de una disposición de la legislación austriaca de telecomunicaciones de transposición de la Directiva 2006/24.

En respuesta a estas peticiones de decisión prejudicial, el TJUE invalidó la Directiva sobre conservación de datos. De acuerdo con el TJUE, los datos que se podían conservar en virtud de esta Directiva contenían información precisa acerca de las personas físicas cuando se consideraban en su conjunto. Además, el TJUE examinó la gravedad de la injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales. Determinó que la conservación responde a un objetivo de interés general, concretamente la lucha contra la delincuencia y grave y, por tanto, la seguridad pública. No obstante, el TJUE declaró que el legislador de la UE había violado el principio de proporcionalidad al adoptar esta Directiva. Aunque la Directiva pueda ser adecuada para alcanzar el fin perseguido, «esta Directiva constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario».

En ausencia de legislación específica sobre conservación de datos, se permite conservar datos como excepción a la confidencialidad de los datos de las telecomunicaciones en virtud de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) ([802]), como medida preventiva, pero únicamente con el fin de combatir la delincuencia grave. Dicha conservación debe limitarse a lo que sea estrictamente necesario con respecto a las categorías de datos conservados, los medios de comunicación afectados, las personas afectadas y el periodo de conservación elegido. Las autoridades nacionales pueden tener acceso a los datos conservados en condiciones estrictas, incluida su revisión previa por una autoridad independiente. Los datos deben conservarse en el territorio de la UE.

([802]) 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 2002 L 201.

Ejemplo: Tras la sentencia *Digital Rights Ireland* y *Kärntner Landesregierung y otros* ([803]), el TJUE vio dos asuntos más en relación con la obligación general de conservación de datos de telecomunicaciones impuesta en Suecia y Reino Unido a los proveedores de servicios de comunicaciones electrónicas por la Directiva sobre conservación de datos invalidada. En *Tele2 Sverige* y *Home Department contra Tom Watson y otros* ([804]), el TJUE dictaminó que la legislación nacional que prescribe la conservación de datos de forma general e indiscriminada sin necesidad de que exista relación alguna entre los datos que deben ser conservados y una amenaza para la seguridad pública y sin especificar condición alguna —p.ej. periodo de retención, área geográfica o grupo de personas que puedan estar involucradas en un delito grave— excede los límites de lo estrictamente necesario y no se puede considerar justificado en una sociedad democrática, como exige la Directiva 2002/58/CE, interpretada a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

Perspectivas

En enero de 2017, la Comisión Europea publicó una propuesta de Reglamento sobre el respeto de la vida privada y la protección de los datos personales en las comunicaciones electrónicas, con el fin de derogar y sustituir a la Directiva 2002/58/CE ([805]). Esta propuesta no incluye ninguna disposición específica sobre conservación de datos. Sin embargo, establece que los Estados miembros pueden limitar por ley determinadas obligaciones y derechos, siempre que tal limitación constituya una medida necesaria y proporcionada para proteger determinados intereses públicos como la seguridad nacional, la defensa, la seguridad pública y la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la sanción de infracciones penales ([806]). Por tanto, los Estados miembros podrían mantener o crear marcos nacionales de conservación de datos que previeran medidas de

([803]) TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.

([804]) TJUE, asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB contra Post- och telestyrelsen y Secretary of State for the Home Department contra Tom Watson y otros* [GS], 21 de diciembre de 2016.

([805]) Comisión Europea (2017), 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) 10 final, Bruselas, 10 de enero de 2017.

([806]) Ibíd., considerando 26.

conservación específicas, siempre que dichos marcos fueran conformes al Derecho de la Unión, habida cuenta de la jurisprudencia del TJUE sobre la interpretación de la Directiva sobre privacidad y comunicaciones electrónicas y de la Carta de los Derechos Fundamentales de la Unión Europea ([807]). En el momento de redactarse el presente manual, continuaban las negociaciones sobre la adopción del Reglamento.

Acuerdo marco entre la UE y los EE. UU. sobre la protección de los datos personales intercambiados con fines de aplicación de la ley

El 1 de febrero de 2017 entró en vigor el Acuerdo marco entre la UE y los EE. UU. para el tratamiento de datos personales con fines de prevención, investigación, detección y enjuiciamiento de infracciones penales ([808]). El Acuerdo marco entre la UE y los EE. UU. tiene por objeto garantizar un alto nivel de protección de datos a los ciudadanos de la UE, así como reforzar la cooperación entre los servicios de seguridad de la UE y los EE. UU. Es complementario a los acuerdos ya existentes entre los servicios de seguridad de la UE y los EE. UU. y de los Estados miembros y los EE. UU., al tiempo que contribuye a establecer normas claras y armonizadas de protección de datos para futuros acuerdos en este terreno. En ese sentido, el acuerdo pretende establecer un marco jurídico duradero para facilitar el intercambio de información.

El Acuerdo no establece por sí solo una base jurídica adecuada para el intercambio de datos personales, sino que ofrece garantías de protección de datos adecuadas para los interesados. Comprende todo tratamiento de datos personales necesario para la prevención, investigación, detección y enjuiciamiento de infracciones penales, incluido el terrorismo ([809]).

El Acuerdo establece múltiples salvaguardias para garantizar que los datos personales se utilicen únicamente con los fines especificados en él. En particular, contempla la siguiente protección para los ciudadanos de la UE:

([807]) Véase la exposición de motivos de la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, COM(2017) 10 final, punto 1.3.

([808]) Véase Consejo de la UE (2016), «Refuerzo de los derechos de protección de datos para los ciudadanos de la UE en la cooperación policial: la UE y los EE. UU. firman un "Acuerdo marco"», nota de prensa 305/16, 2 de junio de 2016.

([809]) Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales, de 18 de mayo de 2016 (OR. en) 8557/16, artículo 3, apartado 1. Véase también la notificación de la Comisión sobre las negociaciones del acuerdo de protección de datos entre la UE y los EE. UU. de 26 de mayo de 2010, MEMO/10/216 y la nota de prensa de la Comisión Europea (2010) sobre los altos niveles de privacidad en el acuerdo de protección de datos entre la UE y los EE. UU. de 26 de mayo de 2010, IP/10/609.

- limitaciones sobre el uso de los datos: los datos de carácter personal solo podrán utilizarse para los fines de prevención, investigación, detección o enjuiciamiento de infracciones penales;

- protección contra la discriminación arbitraria e injustificable;

- transferencias ulteriores: cualquier transferencia ulterior a una organización internacional o a un país que no sean los Estados Unidos o un Estado miembro deberá estar sujeta al consentimiento previo de la autoridad competente del país que envió inicialmente los datos;

- calidad de los datos: los datos personales deberán conservarse teniendo en cuenta su exactitud, pertinencia, puntualidad y exhaustividad;

- seguridad del tratamiento, incluida la notificación de incidentes de seguridad de los datos personales;

- el tratamiento de datos sensibles solo está permitido con garantías adecuadas conforme a la ley;

- periodos de conservación: los datos personales no pueden conservarse durante más tiempo del necesario o apropiado;

- derechos de acceso y rectificación: todos los interesados tienen derecho a obtener acceso a sus datos personales, siempre que se cumplan determinadas condiciones, y podrán solicitar que se corrijan los datos si son inexactos;

- las decisiones automatizadas requieren salvaguardias adecuadas, incluida la posibilidad de obtener la intervención humana;

- supervisión efectiva, incluida la cooperación entre las autoridades de control de la UE y de los EE. UU; y

- recurso judicial y cumplimiento de la ley: los ciudadanos de la UE tienen derecho ([810]) a interponer recurso judicial ante los órganos jurisdiccionales de los Estados Unidos cuando las autoridades de este país denieguen el acceso o rectificación o revelen sus datos personales de forma ilícita.

([810]) El Presidente Obama firmó la Ley estadounidense de reparación judicial el 24 de febrero de 2016.

En virtud de este «Acuerdo marco», también se ha creado un sistema de notificación a las autoridades de control competentes de los Estados miembros de las personas físicas afectadas en relación con posibles violaciones de la protección de datos, cuando sea necesario. Las salvaguardias legales que establece el Acuerdo garantizan la igualdad de trato de los ciudadanos de la UE en los Estados Unidos cuando se produzca una violación de la privacidad ([811]).

8.3.1. Protección de datos en los órganos judiciales y cuerpos y fuerzas de seguridad de la UE

Europol

Europol, la agencia policial de la UE, tiene su sede en La Haya y cuenta con unidades nacionales (UNE) en cada Estado miembro. Europol se constituyó en 1998; su actual estatuto jurídico como institución europea se basa en el Reglamento relativo a la Agencia de la Unión Europea para la Cooperación Policial (Reglamento de Europol) ([812]). Europol tiene por objeto colaborar en la prevención e investigación de la delincuencia organizada, el terrorismo y otras formas de delincuencia grave, que se enumeran en el anexo I del Reglamento de Europol, que afecten a dos o más Estados miembros. Con este fin actúa como centro de intercambio de información en la UE y realiza análisis de inteligencia y evaluaciones de amenazas.

Para lograr sus objetivos, Europol ha creado el Sistema de Información de Europol, que dispone de una base de datos para el intercambio de información e inteligencia criminal entre los Estados miembros a través de sus UNE. El Sistema de información de Europol puede utilizarse para facilitar datos relativos a personas que sean sospechosas de haber participado en delitos penales que sean competencia de Europol o que hayan sido condenadas por tales delitos o a personas respecto de las cuales

([811]) El Supervisor Europeo de Protección de Datos emitió un Dictamen sobre el Acuerdo entre la UE y los EE. UU. en el que recomendaba, entre otras, las siguientes adaptaciones: 1) añadir «para los fines específicos para los que fueron transferidos» en el artículo que trata de que la conservación de los datos no dure más tiempo del necesario y apropiado y 2) excluir que pueda ser posible realizar transferencias de gran volumen de datos sensibles. Véase Supervisor Europeo de Protección de Datos, Dictamen 1/2016, *Preliminary Opinion on the agreement between the United State of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, apartado 35.

([812]) 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) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, DO 2016 L 135, p. 53.

existan indicios concretos o motivos razonables para pensar que cometerán tales delitos. Europol y las UNE pueden introducir datos directamente en el Sistema de Información de Europol y extraer datos del mismo. Únicamente la parte que haya introducido los datos en el sistema podrá modificarlos, corregirlos o suprimirlos. Los organismos de la UE, terceros países y organizaciones internacionales también pueden proporcionar información a Europol.

Europol también puede obtener información, incluidos datos personales, de fuentes públicamente disponibles como internet. Las transferencias de datos personales a organismos de la UE solo se permiten si son necesarias para que Europol o el organismo receptor desempeñen sus funciones. Las transferencias de datos personales a terceros países u organizaciones internacionales solo se permiten si la Comisión Europea decide que el país u organización internacional en cuestión garantiza un nivel adecuado de protección de datos («decisión de adecuación») o si existe un acuerdo internacional o de cooperación. Europol puede recibir y tratar datos personales procedentes de entidades privadas y de particulares única y exclusivamente cuando se cumplan unas estrictas condiciones: que dichos datos sean transferidos por una UNE de conformidad con su legislación nacional, por un punto de contacto de un país tercero o una organización nacional con la que exista una cooperación consolidada a través de un acuerdo de cooperación, o por una autoridad de un país tercero o una organización internacional que estén sujetos a una decisión de adecuación o con los que la UE haya celebrado un acuerdo internacional. Todos los intercambios de información se efectúan por medio de la Aplicación de la Red de Intercambio Seguro de Información (SIENA, por sus siglas en inglés).

En vista de los últimos acontecimientos, se han creado centros especializados en Europol. El Centro Europeo de Ciberdelincuencia se creó como parte de Europol en 2013 ([813]). Este centro actúa como centro de información de la UE sobre la ciberdelincuencia, contribuye a acelerar las reacciones ante los delitos cometidos en línea, desarrolla y despliega capacidades forenses digitales e imparte buenas prácticas de investigación de la ciberdelincuencia. El centro está orientado a los ciberdelitos que:

- sean cometidos por grupos organizados para generar grandes ganancias delictivas, como el fraude en línea;

([813]) Véase, asimismo, SEPD (2012), *Opinion of the Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre*, Bruselas, 29 de junio de 2012.

- provoquen graves perjuicios a las víctimas, como en el caso de la explotación sexual infantil en línea;

- afecten a infraestructuras o servicios de información indispensables de la UE.

El Centro Europeo Contra el Terrorismo (ECTC, por sus siglas en inglés) se creó en enero de 2016 para prestar asistencia operativa a los Estados miembros en las investigaciones relacionadas con delitos de terrorismo. Se encarga de cotejar datos operativos en vivo con los datos que Europol ya posee, sacando rápidamente a la luz pistas financieras, y analiza todos los datos de las investigaciones disponibles para ayudar a que se obtenga una imagen estructurada de una red terrorista ([814]).

El Centro europeo sobre el tráfico ilícito de migrantes (EMSC, por sus siglas en inglés) se creó en febrero de 2016, a raíz de una reunión del Consejo celebrada en noviembre de 2015, con el fin de ayudar a los Estados miembros a localizar y desmantelar redes criminales de tráfico de migrantes. Actúa como centro de información en apoyo de las oficinas del grupo operativo regional de la UE en Catania (Italia) y El Pireo (Grecia), que colaboran con las autoridades nacionales en varios ámbitos, como el intercambio de inteligencia, las investigaciones criminales y la persecución de redes criminales de tráfico de personas ([815]).

Se refuerza el régimen de protección de datos por el que se rigen las actividades de Europol, que se basa en los principios del Reglamento de protección de datos de las instituciones de la UE ([816]) y es además coherente con la Directiva sobre protección de datos para las autoridades policiales y de justicia penal, el Convenio 108 modernizado y la Recomendación sobre la policía.

El tratamiento de datos personales de las víctimas de delitos, los testigos u otras personas que pudieran facilitar información sobre delitos y de los menores de dieciocho años estará permitido si es estrictamente necesario y proporcionado para la prevención o la lucha contra los delitos enunciados en los objetivos de Europol ([817]). Está prohibido el tratamiento de datos personales sensibles, a menos que sea estrictamente necesario y proporcionado para prevenir o combatir los delitos enunciados

([814]) Véase la página web de Europol sobre el ECTC.

([815]) Véase la página web de Europol sobre el EMSC.

([816]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO 2001 L 8.

([817]) Reglamento de Europol, artículo 30, apartado 1.

en los objetivos de Europol y si esos datos son complementarios de otros datos personales tratados por Europol ([818]). En ambos casos, solo Europol podrá acceder a los datos pertinentes ([819]).

Solo se permite conservar datos durante un periodo de tiempo necesario y proporcionado y su prolongación está sujeta a revisión cada tres años, sin la cual los datos se cancelarán automáticamente ([820]).

En determinadas circunstancias, Europol puede transferir datos personales a un organismo de la Unión o a una autoridad de un país tercero o a una organización internacional directamente ([821]). Las violaciones de la seguridad de los datos, si pueden afectar de forma severa y negativa a los derechos y libertades de los interesados afectados, deben serles comunicadas sin demora ([822]). En el ámbito del Estado miembro, se creará una autoridad nacional de control para supervisar las actividades de tratamiento de datos personales realizadas por Europol ([823]).

El SEPD tiene la responsabilidad de vigilar y garantizar la protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos personales por Europol, y de asesorar a Europol y a los interesados sobre cualquier cuestión relativa al tratamiento de los datos personales. Para tal fin, el SEPD actúa como organismo de investigación y atención de reclamaciones, en estrecha colaboración con las autoridades de control nacionales ([824]). El SEPD y las autoridades de control nacionales se reúnen al menos dos veces al año en el Consejo de Cooperación, que tiene funciones consultivas ([825]). Los Estados miembros están obligados a crear una autoridad de control por ley, encargada de vigilar la licitud de la transferencia, extracción y comunicación de datos personales a Europol por parte del Estado miembro de que se trate ([826]). Los Estados miembros también tienen la obligación de garantizar que la autoridad de control nacional pueda actuar con total independencia en el desempeño de sus funciones con arreglo al Reglamento de

([818]) Ibíd., artículo 30, apartado 2.
([819]) Ibíd., artículo 30, apartado 3.
([820]) Ibíd., artículo 31.
([821]) Ibíd., artículos 24 y 25, respectivamente.
([822]) Ibíd., artículo 35.
([823]) Reglamento de Europol, artículo 42.
([824]) Ibíd., artículos 43 y 44.
([825]) Ibíd., artículo 45.
([826]) Ibíd., artículo 42, apartado 1.

Europol ([827]). Para verificar la licitud del tratamiento de datos, realizar un autocontrol de sus actividades, y garantizar la integridad y seguridad de los datos, Europol lleva anotaciones o documentación de sus actividades de tratamiento de datos. Estas anotaciones contienen información sobre las operaciones de recogida, modificación, consulta, comunicación, combinación y supresión de datos en sistemas de tratamiento automatizados ([828]).

Las decisiones del SEPD pueden recurrirse ante el TJUE ([829]). Cualquier persona física que haya sufrido un daño como consecuencia de una operación de tratamiento ilícita tendrá derecho a recibir una indemnización por el daño sufrido, bien de Europol, bien del Estado miembro, para lo cual deberá interponer una acción ante el TJUE, en el primer caso, o ante el tribunal nacional competente, en el segundo ([830]). Además, las actividades de Europol pueden ser objeto de control por parte de un órgano especializado: un Grupo de Control Parlamentario Conjunto creado conjuntamente por los parlamentos nacionales y la comisión competente del Parlamento Europeo ([831]). Todas las personas físicas tienen derecho a acceder a los datos que Europol pueda conservar sobre ellas, además del derecho a solicitar la comprobación, rectificación o supresión de dichos datos. Pueden aplicarse exenciones y limitaciones.

Eurojust

Eurojust, constituido en 2002, es un órgano de la UE con sede en La Haya. Su misión es promover la cooperación judicial en investigaciones y actuaciones judiciales relativas a delitos graves que afecten al menos a dos Estados miembros ([832]). Eurojust tiene competencias para:

([827]) Ibíd., artículo 42, apartado 1.

([828]) Ibíd., artículo 40.

([829]) Ibíd., artículo 48.

([830]) Ibíd., artículo 50.

([831]) Ibíd., artículo 51.

([832]) Consejo de la Unión Europea (2002), Decisión 2002/187/JAI del Consejo, de 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO 2002 L 63; Consejo de la Unión Europea (2003), Decisión 2003/659/JAI del Consejo, de 18 de junio de 2003, por la que se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO 2003 L 44; Consejo de la Unión Europea (2009), Decisión 2009/426/JAI del Consejo, de 16 de diciembre de 2008, por la que se refuerza Eurojust y se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO 2009 L 138 (Decisiones de Eurojust).

- fomentar y mejorar la coordinación de las investigaciones y de las actuaciones judiciales entre las autoridades competentes de los distintos Estados miembros;

- facilitar la ejecución de solicitudes y resoluciones relacionadas con la cooperación judicial.

Las funciones de Eurojust son desempeñadas por los miembros nacionales. Cada Estado miembro delega un juez o fiscal a Eurojust, cuyo estatuto está sujeto al Derecho nacional y que tiene atribuidas las competencias necesarias para desempeñar las funciones que resulten necesarias para fomentar y mejorar la cooperación judicial. Además, los miembros nacionales actúan conjuntamente de forma colegiada para desempeñar las funciones especiales de Eurojust.

Eurojust puede tratar datos personales en la medida en que sea necesario para lograr sus objetivos. Esto queda limitado, sin embargo, a la información específica relativa a las personas que sean sospechosas de haber cometido una infracción penal respecto de la cual tenga competencias Eurojust, o de haber participado en ella, o que hayan sido condenadas por una infracción de este tipo. Eurojust también puede tratar determinada información relacionada con testigos o víctimas de delitos que sean de su competencia ([833]). En circunstancias excepcionales, Eurojust podrá, durante un periodo de tiempo limitado, tratar datos personales más amplios relativos a las circunstancias de una infracción, cuando dichos datos sean de interés inmediato para una investigación en curso. Dentro de su ámbito de competencias, Eurojust podrá cooperar con otras instituciones, organismos y agencias de la UE e intercambiar con ellas datos personales. Eurojust podrá, asimismo, cooperar e intercambiar datos personales con terceros países y organizaciones.

En relación con la protección de datos, Eurojust deberá garantizar un nivel de protección al menos equivalente al de los principios del Convenio 108 modernizado y sus modificaciones posteriores. En los casos de intercambio de datos, deberán observarse normas y limitaciones específicas que se establecerán mediante un acuerdo de cooperación o un acuerdo de trabajo, de conformidad con lo dispuesto en las Decisiones de Eurojust del Consejo y las Normas de Eurojust relativas a la protección de datos ([834]).

([833]) Versión consolidada de la Decisión 2002/187/JAI del Consejo, modificada por la Decisión 2003/659/JAI del Consejo y por la Decisión 2009/426/JAI del Consejo, artículo 15, apartado 2.

([834]) Normas del Reglamento interno de Eurojust relativas al tratamiento y a la protección de datos personales, DO 2005 C 68/01, 19 de marzo de 2005, p. 1.

En Eurojust se ha creado una Autoridad Común de Control (ACC) independiente cuya misión es controlar el tratamiento de datos personales realizado por Eurojust. Los interesados pueden recurrir a la ACC si no están satisfechos con una decisión adoptada por Eurojust con respecto a una solicitud de acceso, rectificación, bloqueo o supresión de datos personales. Cuando Eurojust realice un tratamiento ilícito de datos personales, será responsable, con arreglo al Derecho nacional del Estado donde se encuentra su sede, los Países Bajos, de los daños y perjuicios que se puedan causar al interesado.

Perspectivas

La Comisión Europea presentó una propuesta de Reglamento de reforma de Eurojust en julio de 2013. Esta propuesta iba acompañada de una propuesta de creación de una Fiscalía Europea (véase el apartado siguiente). Este Reglamento tiene por objeto racionalizar sus funciones y estructura para que se correspondan con el Tratado de Lisboa. Además, el objetivo de la reforma es establecer una clara división entre las funciones operativas de Eurojust, desempeñadas por el Colegio de Eurojust, y sus funciones administrativas. De este modo, los Estados miembros también podrían centrarse más en las funciones operativas. Se creará un nuevo Consejo Ejecutivo que ayude al Colegio en el desempeño de las funciones administrativas ([835]).

Fiscalía Europea

La incoación de procedimientos penales por delitos de fraude y por la aplicación indebida del presupuesto de la UE, que pueden tener implicaciones transfronterizas, es competencia exclusiva de los Estados miembros. La importancia de investigar, perseguir y poner a disposición de la justicia a los autores de este tipo de delitos ha aumentado, sobre todo dada la actual crisis económica ([836]). La Comisión Europea ha propuesto un Reglamento relativo a la creación de la Fiscalía Europea (FE) ([837]) con el objetivo de combatir los delitos penales que afectan a los intereses financieros de la Unión. La FE se creará por el procedimiento de cooperación reforzada, que permite que un mínimo de nueve Estados miembros establezcan una cooperación avanzada en el marco de las estructuras de la UE, sin la participación del resto

([835]) Véase la página web de la Comisión Europea sobre Eurojust.

([836]) Véase Comisión Europea (2013), Propuesta de Reglamento del Consejo relativo a la creación de la Fiscalía Europea, COM(2013) 534 final, Bruselas, 17 de julio de 2013, p. 1 y la página web de la Comisión sobre la FE.

([837]) Comisión Europea (2013), Propuesta de Reglamento del Consejo relativo a la creación de la Fiscalía Europea, COM(2013) 534 final, Bruselas, 17 de julio de 2013.

de Estados miembros ([838]). Alemania, Bélgica, Bulgaria, Chipre, Croacia, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Letonia, Lituania, Luxemburgo, Portugal, Chequia y Rumanía se han adherido a la cooperación reforzada, mientras que Austria e Italia han expresado su intención de hacerlo ([839]).

La FE será competente para investigar y procesar los fraudes a la UE y otros delitos que afecten a los intereses financieros de la Unión, con el fin de coordinar eficientemente las investigaciones y los procedimientos en los distintos ordenamientos jurídicos nacionales y mejorar el uso de los recursos y el intercambio de información a escala europea ([840]).

La FE estará encabezada por un Fiscal Europeo, que contará al menos con un fiscal europeo delegado en cada Estado miembro, encargado de llevar a cabo las investigaciones y los procesos penales en ese Estado miembro.

La propuesta contiene sólidas garantías de protección de los derechos que tienen las personas implicadas en las investigaciones de la FE en virtud de la legislación nacional, la legislación de la UE y la Carta de los Derechos Fundamentales de la Unión Europea. Las medidas de investigación que más afecten a los derechos fundamentales necesitarán la autorización previa de un tribunal nacional ([841]). Las investigaciones de la FE estarán sujetas a la revisión judicial de los tribunales nacionales ([842]).

El Reglamento de protección de datos para las instituciones de la UE ([843]) será de aplicación a las actividades de tratamiento de datos personales administrativos que lleve a cabo la FE. Para el tratamiento de datos personales relacionados con cuestiones operativas, al igual que Europol, la FE contará con un régimen de protección de datos autónomo, parecido al que regula las actividades de Europol y Eurojust, dado que el desempeño delas funciones de la FE implicará el tratamiento de datos

([838]) Tratado de Funcionamiento de la Unión Europea, artículo 86, apartado 1 y artículo 329, apartado 1.

([839]) Véase Consejo de la Unión Europea (2017), «*Veinte Estados miembros alcanzan un acuerdo sobre los detalles relativos a la creación de la Fiscalía Europea (FE)*», nota de prensa, 8 de junio de 2017.

([840]) Comisión Europea (2013), Propuesta de Reglamento del Consejo relativo a la creación de la Fiscalía Europea, COM(2013) 534 final, Bruselas, 17 de julio de 2013, p. 1 y p. 51. Véase también la página web de la Comisión sobre la FE.

([841]) Comisión Europea (2013), Propuesta de Reglamento del Consejo relativo a la creación de la Fiscalía Europea, COM(2013) 534 final, Bruselas, 17 de julio de 2013, artículo 26, apartado 4.

([842]) Ibíd., artículo 36.

([843]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO 2001 L 8.

personales con las autoridades policiales y judiciales de los Estados miembros. Por tanto, las normas de protección de datos de la FE son casi idénticas a las normas de la Directiva sobre protección de datos para las autoridades policiales y de justicia penal. De acuerdo con la propuesta de creación de la FE, el tratamiento de datos personales debe atenerse a los principios de lealtad y licitud, limitación a una finalidad específica, minimización de datos, exactitud, integridad y confidencialidad. La FE deberá establecer una distinción lo más clara posible entre los datos personales de distintos tipos de interesados, como personas condenadas por delitos, personas que solo sean sospechosas, víctimas y testigos. También debe procurar verificar la calidad de los datos personales tratados y distinguir, en la medida de lo posible, los datos personales basados en hechos de los datos personales basados en valoraciones personales.

La propuesta contiene disposiciones sobre los derechos de los interesados, concretamente los derechos de información, acceso a sus datos personales, rectificación, supresión y limitación del tratamiento, y establece que estos derechos también se pueden ejercer de forma indirecta, a través del SEPD. También incorpora los principios de seguridad del tratamiento y responsabilidad proactiva, que obligan a la FE a aplicar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado a los riesgos que entraña el tratamiento, a llevar registros de todas las actividades de tratamiento y a realizar una evaluación de impacto de la protección de datos antes del tratamiento, cuando un tipo de tratamiento (por ejemplo, que conlleve el uso de nuevas tecnologías) pueda entrañar un alto riesgo para los derechos de los interesados. Por último, la propuesta contempla la designación de un delegado de protección de datos por el Colegio, que debe participar debidamente en todas las cuestiones relativas a la protección de datos personales y debe velar por que la FE cumpla la normativa de protección de datos aplicable.

8.3.2. La protección de datos en los sistemas comunes de información en el ámbito de la UE

Además del intercambio de datos entre los Estados miembros y la creación de autoridades de la UE especializadas en la lucha de la delincuencia transfronteriza, como Europol, Eurojust y la FE, se han creado varios sistemas comunes de información a escala de la UE que facilitan el intercambio de datos entre las autoridades competentes nacionales y de la UE, para fines específicos en el ámbito de la protección de fronteras, la inmigración y el asilo y las aduanas. Dado que el espacio Schengen se creó por medio de un acuerdo internacional independiente del Derecho de la UE, el

Sistema de Información de Schengen (SIS) evolucionó a partir de acuerdos multilaterales y posteriormente se incorporó al Derecho de la Unión. El Sistema de Información de Visados (VIS), Eurodac, Eurosur y el Sistema de Información Aduanera (SIA) fueron creados como instrumentos que se rigen por el Derecho de la Unión.

Estos sistemas son supervisados conjuntamente por las autoridades de control nacionales y por el SEPD. Para garantizar un alto nivel de protección, estas autoridades colaboran en el seno de los Grupos de Coordinación de la Supervisión (GCS), que se refieren a los siguientes sistemas de TI de gran escala: 1) Eurodac; 2) Sistema de Información de Visados; 3) Sistema de Información de Schengen; 4) Sistema de Información Aduanera; y 5) Sistema de Información del Mercado Interior ([844]). Los GCS suelen reunirse dos veces al año, bajo la autoridad de un presidente electo, para adoptar directrices, analizar casos transfronterizos o adoptar marcos comunes para las inspecciones.

La Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud (eu-LISA) ([845]), creada en 2012, es responsable de la gestión operativa a largo plazo del Sistema de Información de Schengen de segunda generación (SIS II), del Sistema de Información de Visados (VIS) y de Eurodac. La función principal de la Agencia es garantizar el funcionamiento eficaz, seguro y continuo de los sistemas de información de gran magnitud. También tiene la responsabilidad de adoptar las medidas necesarias para garantizar la seguridad de los sistemas y la seguridad de los datos.

El Sistema de Información de Schengen

En 1985, varios Estados miembros de las antiguas Comunidades Europeas celebraron un Acuerdo entre los Estados de la Unión Económica Benelux, Alemania y Francia relativo a la supresión gradual de los controles en las fronteras comunes (Acuerdo de Schengen), al objeto de crear un espacio para la libre circulación de las personas, exento de los inconvenientes de los controles fronterizos en el interior del territorio Schengen ([846]). Para contrarrestar la amenaza para la seguridad pública que podría derivarse de la apertura de fronteras, se establecieron controles reforzados

([844]) Véase la página web del SEPD sobre coordinación de la supervisión.

([845]) Reglamento (UE) n.º 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DO 2011 L 286.

([846]) Acuerdo entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa relativo a la supresión gradual de los controles en las fronteras comunes, DO 2000 L 239.

en las fronteras exteriores del espacio Schengen, así como una estrecha cooperación entre las autoridades policiales y judiciales nacionales.

Como consecuencia de la adhesión de otros Estados al Acuerdo de Schengen, el sistema Schengen se integró finalmente en el marco jurídico de la UE a través del Tratado de Ámsterdam ([847]). Esta decisión se llevó a la práctica en 1999. La versión más reciente del Sistema de Información de Schengen, el denominado SIS II, entró en funcionamiento el 9 de abril de 2013. En la actualidad se extiende a la mayoría de los Estados miembros ([848]), más Islandia, Liechtenstein, Noruega y Suiza ([849]). Europol y Eurojust también tienen acceso al SIS II.

El SIS II está compuesto por un sistema central (C-SIS), un sistema nacional (N-SIS) en cada Estado miembro, y una infraestructura de comunicación entre el sistema central y los sistemas nacionales. El sistema C-SIS incluye ciertos datos introducidos por los Estados miembros sobre personas y objetos. El SIS es utilizado por autoridades nacionales de control fronterizo, policiales, aduaneras, de expedición de visados y judiciales en todo el Espacio Schengen. Cada Estado miembro utiliza una copia nacional del C-SIS, que recibe el nombre de Sistema de Información Schengen Nacional (N-SIS). Esta copia se actualiza constantemente y actualiza a su vez el C-SIS. Existen diferentes tipos de descripciones en el SIS:

- la persona no tiene derecho de entrada o de estancia en el territorio Schengen;
- la persona o el objeto es buscado por autoridades policiales o judiciales (p. ej., órdenes europeas de detención y entrega, solicitudes de controles discretos);
- se ha denunciado la desaparición de la persona;
- se ha denunciado el robo o pérdida de bienes, como billetes de banco, automóviles, camionetas, armas de fuego y documentos de identidad.

([847]) Comunidades Europeas (1997), Tratado de Ámsterdam por el que se modifican el Tratado de la Unión Europea, los Tratados constitutivos de las Comunidades Europeas y determinados actos conexos, DO 1997 C 340.

([848]) Croacia, Chipre e Irlanda están realizando preparativos para integrarse en el SIS II, pero todavía no son parte del sistema. Véase la información sobre el Sistema de Información de Schengen disponible en la página web de la Dirección General de Migración y Asuntos de Interior de la Comisión Europea.

([849]) Reglamento (CE) n.º 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO 2006 L 381; y Consejo de la Unión Europea (2007), Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO 2007 L 205.

Cuando se introduce una descripción, deben iniciarse actividades de seguimiento a través de la Oficina SIRENE. SIS II tiene nuevas funcionalidades, como la posibilidad de introducir datos biométricos, como impresiones dactilares y fotografías, o nuevas categorías de descripciones, como robo de barcos, aviones, contenedores o medios de pago, descripciones enriquecidas de personas y objetos; y copias de las órdenes europeas de detención, entrega o extradición.

El SIS II se basa en dos actos complementarios: la Decisión SIS II ([850]) y el Reglamento SIS II ([851]). El legislador de la UE utilizó diferentes bases jurídicas para la adopción de la Decisión y del Reglamento. La Decisión regula el uso del SIS II para los fines de la cooperación policial y judicial en materia penal (el antiguo tercer pilar de la UE). El Reglamento se aplica a los procedimientos relativos a descripciones que se inscriban en el ámbito de las políticas de visados, asilo, inmigración y otras políticas relacionadas con la libre circulación de personas (antiguamente el primer pilar). Los procedimientos sobre descripciones correspondientes a cada pilar debían regularse por medio de actos distintos, dado que los dos actos jurídicos fueron adoptados antes del Tratado de Lisboa y la abolición de la estructura de pilares.

Ambos actos jurídicos contienen disposiciones relativas a la protección de datos. La Decisión SIS II prohíbe el tratamiento de datos sensibles ([852]). El tratamiento de datos personales estará comprendido en el ámbito de aplicación del Convenio 108 modernizado ([853]). Además, los interesados tienen derecho de acceso a los datos personales que se refieran a ellos y que estén introducidos en el SIS II ([854]).

El Reglamento SIS II establece condiciones y procedimientos para introducir y procesar descripciones relativas a la denegación de entrada o estancia de ciudadanos de países terceros. También establece disposiciones sobre el intercambio de información complementaria y datos adicionales a efectos de la entrada o estancia en un Estado miembro ([855]). Este Reglamento también contiene disposiciones relativas

([850]) Decisión 2007/533/JAI del Consejo de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 205, 7 de agosto de 2007).

([851]) Reglamento (CE) n.º 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 381, 28 de diciembre de 2006).

([852]) Decisión SIS II, artículo 56; Reglamento SIS II, artículo 40.

([853]) Decisión SIS II, artículo 57.

([854]) Decisión SIS II, artículo 58; Reglamento SIS II, artículo 41.

([855]) Reglamento SIS II, artículo 2.

a la protección de datos. No está permitido el tratamiento de categorías de datos sensibles, conforme al artículo 9, apartado 1 del Reglamento general de protección de datos ([856]). El Reglamento SIS II también reconoce ciertos derechos para el interesado, como son:

- el derecho de acceso a los datos personales relativos al interesado ([857]);
- el derecho de rectificación de datos que contengan errores de hecho ([858]);
- el derecho de supresión de datos que contengan errores de derecho ([859]); y
- el derecho a ser informado si el interesado es objeto de una descripción. La información se facilitará por escrito, junto con una copia de la decisión nacional que causó la introducción de la descripción, o una referencia a dicha decisión ([860]).

En ningún caso se proporcionará esta información cuando 1) los datos personales no se hayan obtenido del interesado y el hecho de proporcionar la información resulte imposible o requiera un esfuerzo desproporcionado; 2) el interesado ya tenga la información o 3) el Derecho nacional permita la restricción del derecho de información, entre otras razones, para salvaguardar la seguridad nacional o prevenir delitos ([861]).

Tanto en el caso de la Decisión SIS II como del Reglamento SIS II, los derechos de acceso de los interesados en relación con el SIS II se pueden ejercer en cualquier Estado miembro y se aplican de conformidad con la legislación nacional de dicho Estado miembro ([862]).

Ejemplo: En el asunto *Dalea contra Francia* ([863]), se le había denegado al demandante un visado de visita a Francia, ya que las autoridades francesas habían informado al Sistema de Información de Schengen de que debía serle denegada la entrada. El demandante intentó sin éxito obtener acceso

([856]) Ibíd., artículo 40.
([857]) Ibíd., artículo 41, apartado 1.
([858]) Ibíd., artículo 41, apartado 5.
([859]) Ibíd., artículo 41, apartado 5.
([860]) Ibíd., artículo 42, apartado 1.
([861]) Ibíd., artículo 42, apartado 2.
([862]) Reglamento SIS II, artículo 41, apartado 1 y Decisión SIS II, artículo 58.
([863]) TEDH, *Dalea contra Francia*, n.º 964/07, 2 de febrero de 2010.

a los datos para proceder a su rectificación o supresión ante la Comisión francesa de protección de datos y, en última instancia, ante el Consejo de Estado francés. El TEDH resolvió que la comunicación sobre el demandante al Sistema de Información de Schengen se había realizado de conformidad con la ley y había perseguido el fin legítimo de proteger la seguridad nacional. Dado que el demandante no demostró las consecuencias efectivas que había sufrido a consecuencia de la denegación de la entrada en el espacio Schengen, y teniendo en cuenta que se habían aplicado medidas suficientes para protegerle contra decisiones arbitrarias, la injerencia en su derecho al respeto de su vida privada había sido proporcionada. Por tanto, la reclamación del demandante con arreglo al artículo 8 fue declarada inadmisible.

La autoridad de control competente de cada Estado miembro supervisa el sistema nacional N-SIS. La autoridad de control nacional debe velar por que, al menos cada cuatro años, se lleve a cabo una auditoría de las operaciones de tratamiento de datos en los N-SIS nacionales ([864]). Las autoridades de control nacionales y el SEPD cooperan para garantizar una supervisión coordinada del N-SIS, mientras que el SEPD es responsable de la supervisión del C-SIS. En aras de la transparencia, cada dos años se remitirá un informe conjunto sobre las actividades realizadas al Parlamento Europeo, al Consejo y a la agencia eu-LISA. El Grupo de Coordinación de la Supervisión (GCS) de SIS II se ha creado para garantizar la coordinación de la supervisión del SIS y se reúne dos veces al año. Este grupo está formado por el SEPD y por representantes de las autoridades de control de los Estados miembros que han aplicado el SIS II, así como Islandia, Liechtenstein, Noruega y Suiza, dado que también en ellos se aplica el SIS porque son miembros de Schengen ([865]). Chipre, Croacia e Irlanda todavía no forman parte del SIS II y, por tanto, solo participan como observadores del GCS. En el contexto del GCS, el SEPD y las autoridades de control nacionales mantienen una cooperación activa, en el marco de la cual intercambian información, se prestan ayuda mutua en la realización de auditorías e inspecciones, elaboran propuestas armonizadas de soluciones comunes a problemas potenciales y fomentan el conocimiento de los derechos en materia de protección de datos ([866]). El GCS de SIS II también adopta guías de ayuda para los interesados. Un ejemplo es la guía para ayudar a los interesados a ejercer sus derechos de acceso ([867]).

([864]) Reglamento SIS II, artículo 60, apartado 2.

([865]) Véase la página web del SEPD sobre el Sistema de Información de Schengen.

([866]) Reglamento SIS II, artículo 46 y Decisión SIS II, artículo 62.

([867]) Véase GCS SIS II, *El Sistema de Información de Schengen: guía para el ejercicio del derecho de acceso*, disponible en la página web del SEPD.

Perspectivas

En 2016, la Comisión Europea realizó una evaluación del SIS ([868]) que demostró que se han establecido mecanismos nacionales para facilitar que los interesados accedan a sus datos personales en el SIS II para ejercer sus derechos de rectificación y supresión u obtengan una indemnización por la presencia de errores en los datos. Para mejorar la eficiencia y eficacia del SIS II, la Comisión Europea presentó tres propuestas de Reglamentos:

- un Reglamento relativo al establecimiento, funcionamiento y utilización del SIS en el ámbito de los controles fronterizos, por el que se derogará el Reglamento SIS II;

- un Reglamento relativo al establecimiento, funcionamiento y utilización del SIS en el ámbito de la cooperación policial y judicial en materia penal, por el que se derogará, entre otras cosas, la Decisión SIS II; y

- un Reglamento sobre la utilización del SIS para el retorno de nacionales de terceros países en situación ilegal.

Es importante señalar que las propuestas permiten el tratamiento de otras categorías de datos biométricos, además de fotografías e impresiones dactilares, que ya forman parte del régimen SIS II vigente. En la base de datos del SIS también se conservarán imágenes faciales, impresiones palmares y perfiles de ADN. Además, aunque el Reglamento SIS II y la Decisión SIS II contemplaban la posibilidad de realizar una búsqueda de impresiones dactilares para identificar a una persona, las propuestas establecen que esta búsqueda sea obligatoria si no es posible determinar la identidad de la persona de ninguna otra manera. Se realizarán búsquedas de imágenes faciales, fotografías e impresiones palmares en el sistema para identificar a personas cuando esto sea técnicamente posible. Las nuevas disposiciones sobre los atributos biométricos entrañan determinados riesgos para los derechos de las personas físicas. En su dictamen sobre las propuestas de la Comisión ([869]), el SEPD observa que los datos biométricos son muy sensibles y que su introducción en una

([868]) Comisión Europea (2016), Informe de la Comisión al Parlamento Europeo y al Consejo sobre la evaluación del Sistema de Información de Schengen de segunda generación (SIS II) de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3 y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006 y el artículo 59, apartado 3, y el artículo 66, apartado 5 de la Decisión n.º 2007/533/JAI, COM(2016) 880 final, Bruselas, 21 de diciembre de 2016.

([869]) SEPD (2017), EDPS Opinion on the new legal basis of the Schengen Information System, Dictamen 7/2017, 2 de mayo de 2017.

base de datos de tal envergadura debería requerir una evaluación, basada en pruebas, de la necesidad de incorporarlos al SIS. En otras palabras, es preciso demostrar la necesidad del tratamiento de los nuevos atributos. El SEPD también considera que es necesario aclarar en mayor medida qué tipo de información se puede incluir en el perfil de ADN. Dado que el perfil de ADN puede incluir información sensible (el ejemplo más notable sería información que revelase problemas de salud), los perfiles de ADN almacenados en el SIS deben contener: «únicamente la información mínima que sea estrictamente necesaria para identificar a las personas desaparecidas y deberá excluirse expresamente la información de salud, origen racial y cualquier otra información sensible» ([870]). No obstante, las propuestas establecen garantías adicionales para limitar la recogida y el posterior tratamiento de los datos a lo estrictamente necesario e imprescindible a efectos del funcionamiento, y se restringe el acceso a los datos personales a quienes tengan necesidad de tratarlos con fines operativos ([871]). Las propuestas también facultan a eu-LISA para elaborar periódicamente informes de calidad de los datos destinados a los Estados miembros, que permitan revisar periódicamente las descripciones para garantizar la calidad de los datos ([872]).

El Sistema de Información de Visados

El Sistema de Información de Visados (VIS), cuya gestión compete igualmente a eu-LISA, se desarrolló para facilitar la aplicación de la política común de visados de la UE ([873]). El sistema VIS permite que los Estados Schengen intercambien datos relativos a los solicitantes de visados a través de un sistema totalmente centralizado que conecta los consulados y embajadas de los Estados Schengen situados en terceros países con los puntos de paso de las fronteras exteriores de todos los Estados

([870]) Ibíd., apartado 22.

([871]) Comisión Europea (2016), Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y judicial en materia penal, por el que se modifica el Reglamento (UE) n.º 515/2014 y se deroga el Reglamento (CE) n.º 1986/2006, la Decisión 2007/533/JAI del Consejo y la Decisión n.º 2010/261/UE de la Comisión, COM (2016) 883 final, Bruselas, 21 de diciembre de 2016.

([872]) Ibíd., p. 15.

([873]) Consejo de la Unión Europea (2004), Decisión del Consejo 2004/512/CE, de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS), DO 2004 L 213; Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS), DO 2008 L 218; Consejo de la Unión Europea (2008), Decisión del Consejo 2008/633/JAI, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves, DO 2008 L 218.

Schengen. El sistema VIS trata datos relacionados con las solicitudes de visados de corta duración y visados de tránsito en el espacio Schengen. El sistema VIS permite que las autoridades fronterizas verifiquen, por medio de atributos biométricos y en particular impresiones dactilares, si la persona que presenta un visado es su legítimo titular, así como identificar a las personas indocumentadas o con documentos fraudulentos.

El Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS) regula las condiciones y procedimientos para transferir datos personales relativos a solicitudes de visados para estancias de corta duración. También supervisa las decisiones que se toman sobre las solicitudes, incluidas las decisiones de anulación, retirada o prórroga de los visados ([874]). El Reglamento VIS se aplica a los datos relativos al solicitante, sus visados, fotografías, impresiones dactilares, vínculos con solicitudes anteriores, y los expedientes de solicitud de las personas que le acompañen, o los datos relativos a las personas que le inviten ([875]). El acceso al VIS para introducir, modificar o suprimir datos estará reservado exclusivamente a las autoridades competentes en materia de visados, aunque las autoridades responsables de los controles en los puntos de paso de las fronteras exteriores, de los controles de inmigración y del asilo también podrán acceder para realizar consultas.

En determinadas condiciones, las autoridades policiales nacionales competentes y Europol podrán solicitar acceso a los datos introducidos en el VIS con el fin de prevenir, detectar e investigar delitos de terrorismo y otros delitos ([876]). Dado que el VIS se ha diseñado como instrumento de apoyo a la aplicación de la política común de visados, si el VIS se convirtiese en una herramienta de aplicación de la ley, se violaría el principio de limitación de la finalidad, el cual, según se ha explicado en la sección 3.2, exige que los datos personales se traten únicamente con fines determinados, explícitos y legítimos, y que deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan. Por esta razón, los servicios de seguridad nacionales y Europol no están autorizados a acceder

([874]) Reglamento VIS, artículo 1.

([875]) Artículo 5 del Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS), DO 2008 L 218.

([876]) Consejo de la Unión Europea (2008), Decisión 2008/633/JAI del Consejo, de 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembros y por Europol, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves, DO 2008 L 218.

rutinariamente a la base de datos VIS. Solo se podrá otorgar acceso en función del caso concreto y se establecerán garantías estrictas. Las condiciones y garantías de acceso y consulta del VIS por estas autoridades están reguladas por la Decisión 2008/633/JAI del Consejo ([877]).

Además, el Reglamento VIS establece los derechos de los interesados, como son:

- El derecho a ser informado por el Estado miembro responsable de la identidad y los datos de contacto de la autoridad responsable del control sobre la cual recaerá la responsabilidad central del tratamiento de los datos en dicho Estado miembro, de los fines para los cuales se tratarán los datos en el VIS, de las categorías de personas a quienes se podrán transmitir los datos (destinatarios) y del periodo de conservación de los datos. Además, los solicitantes de visados deberán ser informados de la obligatoriedad de la recogida de sus datos personales conforme al VIS para el examen de su solicitud, mientras que los Estados miembros también deberán informarles de la existencia de su derecho a obtener acceso a sus datos, a solicitar su rectificación o supresión y acerca de los procedimientos que les permitan ejercitar tales derechos ([878]).

- El derecho de acceso a los datos personales que se refieran a ellos y que estén introducidos en el VIS ([879]).

- El derecho de solicitar la corrección de datos inexactos ([880]).

- El derecho de solicitar la supresión de datos obtenidos ilegalmente ([881]).

Para garantizar la supervisión del VIS, se creó el GCS del VIS. Está formado por representantes del SEPD y de las autoridades de control nacionales, que se reúnen dos veces al año. Este grupo está formado por representantes de los 28 Estados miembros de la Unión y de Islandia, Liechtenstein, Noruega y Suiza.

([877]) Ibíd.

([878]) Reglamento VIS, artículo 37.

([879]) Ibíd., artículo. 38 apartado 1.

([880]) Ibíd., artículo 38, apartado 2.

([881]) Ibíd., artículo 38, apartado 2.

Eurodac

Eurodac significa «dactiloscopia europea» ([882]). Es un sistema centralizado que contiene datos dactiloscópicos de nacionales de terceros países y apátridas que solicitan asilo en uno de los Estados miembros de la UE ([883]). El sistema lleva en funcionamiento desde enero de 2003, tras la adopción del Reglamento n.º 2725/2000 del Consejo, cuyo texto refundido entró en vigor en 2015. Su principal finalidad es ayudar a determinar qué Estado miembro debe ser el responsable de examinar una determinada solicitud de asilo en virtud del Reglamento (CE) n.º 604/2013. Ese Reglamento establece los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida (Reglamento de Dublín III) ([884]). Los datos personales que contiene Eurodac sirven principalmente para facilitar la aplicación del Reglamento de Dublín III ([885]).

Los servicios de seguridad nacionales y Europol pueden comparar las impresiones dactilares vinculadas a investigaciones criminales con las impresiones dactilares que contiene Eurodac, pero únicamente con fines de prevención, detección o investigación de delitos de terrorismo u otros delitos graves. Dado que Eurodac se ha diseñado como instrumento de apoyo a la aplicación de la política de asilo de la UE, y no como herramienta de aplicación de la ley, los servicios de seguridad tienen acceso

([882]) Véase la página web del SEPD sobre Eurodac.

([883]) Reglamento (CE) n.º 2725/2000 del Consejo, de 11 de diciembre de 2000, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, DO 2000 L 316; Reglamento (CE) n.º 407/2002 del Consejo, de 28 de febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento (CE) n.º 2725/2000 relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, DO 2002 L 62 (Reglamentos Eurodac), Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n.º 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia, DO 2013 L 180, p 1 (Reglamento Eurodac refundido).

([884]) Reglamento (UE) n.º 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida (Texto refundido) (Reglamento de Dublín III), DO 2013 L 180.

([885]) Reglamento Eurodac refundido, DO 2013 L 180, p. 1, artículo 1, apartado 1.

a la base de datos únicamente en casos concretos, siempre que se cumplan circunstancias específicas y con arreglo a condiciones estrictas ([886]). En relación con otros usos de los datos con fines de aplicación de la ley, se aplica la Directiva sobre protección de datos para las autoridades policiales y de justicia penal, mientras que los datos utilizados con la finalidad principal de facilitar el Reglamento de Dublín III están protegidos por el Reglamento general de protección de datos. Están prohibidas las transferencias ulteriores de datos personales obtenidos por un Estado miembro o por Europol con arreglo al Reglamento Eurodac refundido a terceros países, organismos internacionales o particulares ([887]).

Eurodac consta de una unidad central, operada por eu-LISA, que almacena y compara impresiones dactilares, y un sistema de transmisión electrónica de datos entre los Estados miembros y la base de datos central. Los Estados miembros toman y transmiten las impresiones dactilares de todas las personas mayores de catorce años que soliciten asilo en su territorio, y de todas las personas mayores de catorce años que sean nacionales de terceros países o apátridas y que hayan sido interceptadas con ocasión del cruce irregular de sus fronteras exteriores. Los Estados miembros también podrán tomar y transmitir las impresiones dactilares de personas que sean nacionales de terceros países o apátridas que se encuentren en su territorio sin autorización.

Aunque cualquier Estado miembro puede consultar Eurodac y solicitar comparaciones de datos dactiloscópicos, únicamente el Estado miembro que ha recogido esos datos y los ha transmitido a la unidad central tiene derecho a modificarlos, rectificándolos, complementándolos o suprimiéndolos ([888]). La agencia eu-LISA conserva registros de todas las operaciones de tratamiento de datos para controlar la protección de los datos y garantizar su seguridad ([889]). Las autoridades de control nacionales ayudan y asesoran a los interesados en el ejercicio de sus derechos ([890]). La recogida y transmisión de datos dactiloscópicos está sujeta a revisión judicial por los órganos jurisdiccionales nacionales ([891]). El Reglamento de protección de datos de

([886]) Ibíd., artículo 1, apartado 2.
([887]) Ibíd., artículo 35.
([888]) Ibíd., artículo 27.
([889]) Ibíd., artículo 28.
([890]) Ibíd., artículo 29.
([891]) Ibíd., artículo 29.

las instituciones de la UE ([892]) y la supervisión del SEPD se aplican a las actividades de tratamiento del sistema central, que está gestionado por eu-LISA en relación con Eurodac ([893]). Si una persona sufre un perjuicio como consecuencia de una operación de tratamiento ilegal o un acto incompatible con el Reglamento Eurodac, dicha persona tendrá derecho a indemnización por parte del Estado miembro responsable del perjuicio sufrido ([894]). No obstante, cabe señalar que los solicitantes de asilo conforman un grupo de personas especialmente vulnerables que a menudo han realizado viajes muy largos y arriesgados. Debido a su vulnerabilidad y a la precaria situación en la que a menudo se encuentran mientras está pendiente el examen de su solicitud de asilo, el ejercicio de sus derechos —incluido el derecho a indemnización— puede resultar difícil en la práctica.

Si desean utilizar Eurodac con fines de aplicación de la ley, los Estados miembros deben designar a las autoridades que tendrán derecho a solicitar acceso, así como a las autoridades que verificarán que las solicitudes de comparación sean lícitas ([895]). El acceso de las autoridades nacionales, así como de Europol, a los datos dactiloscópicos de Eurodac está sujeto a condiciones muy estrictas. La autoridad solicitante debe presentar una solicitud electrónica motivada únicamente después de comprar los datos con los existentes en otros sistemas de información disponibles, como el VIS o bases de datos dactiloscópicos nacionales. Debe existir un interés superior de seguridad pública que haga que la comparación sea proporcionada. La comparación debe ser verdaderamente necesaria y referirse a un caso concreto y deben existir motivos razonables para considerar que la comparación contribuirá sustancialmente a la prevención, detección o investigación de cualquiera de los delitos en cuestión, en particular cuando exista una sospecha fundada de que el sospechoso, el autor o la víctima de un delito de terrorismo o de otro delito grave están encuadrados en una categoría sujeta a la recogida de impresiones dactilares en el sistema Eurodac. La comparación debe limitarse a la búsqueda de datos dactiloscópicos. Europol también debe obtener autorización del Estado miembro que haya recogido los datos dactiloscópicos.

([892]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO 2001 L 8.

([893]) Reglamento Eurodac refundido, DO 2013 L 180, p. 1, artículo 31.

([894]) Ibíd., artículo 37.

([895]) Roots, L. (2015), «The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination», *Baltic Journal of European Studies Tallinn University of Technology*, Vol. 5, No. 2, pp. 108-129.

Los datos personales almacenados en Eurodac relativos a los solicitantes de asilo se conservan durante un periodo de diez años a partir de la fecha de obtención de las impresiones dactilares, a menos que el interesado obtenga la ciudadanía de un Estado miembro de la UE. En tal caso, los datos deberán suprimirse de inmediato. Los datos relativos a nacionales extranjeros interceptados con ocasión de un cruce irregular de la frontera exterior se conservan durante un periodo de dieciocho meses. Estos datos deberán eliminarse de inmediato si el interesado recibe un permiso de residencia, abandona el territorio de la UE u obtiene la ciudadanía de un Estado miembro. Los datos de las personas a quienes se concede asilo permanecen disponibles durante tres años a efectos de comparación en el contexto de la prevención, detección e investigación de delitos de terrorismo y otros delitos graves.

Además de todos los Estados miembros de la UE, también Islandia, Noruega, Liechtenstein y Suiza aplican el sistema Eurodac en virtud de acuerdos internacionales.

El GCS de Eurodac se ha creado con el fin de supervisar el sistema Eurodac. Está formado por representantes del SEPD y de las autoridades de control nacionales, que se reúnen dos veces al año. Este grupo consta de representantes de los veintiocho Estados miembros de la Unión y de Islandia, Liechtenstein, Noruega y Suiza ([896]).

Perspectivas

En mayo de 2016, la Comisión publicó una propuesta de nuevo Reglamento Eurodac refundido, como parte de una reforma destinada a mejorar el funcionamiento del Sistema Europeo Común de Asilo (SECA) ([897]). La refundición propuesta es importante, puesto que ampliará sustancialmente el ámbito de aplicación de la base de datos original de Eurodac. Eurodac se creó inicialmente para facilitar la aplicación del SECA, proporcionando pruebas dactiloscópicas que permitiesen determinar qué Estado miembro es responsable del examen de una solicitud de asilo presentada en la Unión. El texto refundido propuesto ampliará el ámbito de aplicación de la base de datos para facilitar el retorno de migrantes irregulares ([898]). Las autoridades

([896]) Véase la página web del SEPD sobre Eurodac.

([897]) Comisión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida] y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (refundición), COM(2016) final, 4 de mayo de 2016.

([898]) Véase la exposición de motivos de la propuesta, p. 3.

nacionales podrán consultar la base de datos con el fin de identificar a los nacionales de terceros países que se encuentren en la Unión en situación ilegal o que hayan entrado en la UE de forma irregular, a fin de obtener pruebas que ayuden a los Estados miembros a efectuar el retorno de estas personas. Además, aunque el régimen jurídico actualmente vigente solo exige la recogida y conservación de impresiones dactilares, la propuesta introduce la recogida de imágenes faciales ([899]), que son otro tipo de datos biométricos. Esta propuesta también reduciría la edad mínima de los menores de quienes se pueden obtener datos biométricos a seis años ([900]) en lugar de catorce, que es la edad mínima en virtud del Reglamento de 2013. La ampliación del ámbito de aplicación de la propuesta implica una injerencia en los derechos a la vida privada y a la protección de datos de un mayor número de personas que podrían incluirse en la base de datos. Para compensar esta injerencia, la propuesta y las modificaciones propuestas por la comisión LIBE del Parlamento Europeo ([901]) pretenden reforzar los requisitos de protección de datos. En el momento de redactarse el presente manual, continuaban las negociaciones sobre la propuesta en el Parlamento y el Consejo.

Eurosur

El Sistema Europeo de Vigilancia de Fronteras (Eurosur) ([902]) está diseñado para reforzar el control de las fronteras exteriores de Schengen mediante la detección, prevención y lucha contra la inmigración ilegal y la delincuencia transfronteriza. Sirve para mejorar el intercambio de información y la cooperación operativa entre

([899]) Comisión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida] y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (refundición), COM(2016) final, 4 de mayo de 2016, artículo 2, apartado 1.

([900]) Ibíd., artículo 2, apartado 2.

([901]) Parlamento Europeo, *Informe sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del [Reglamento (UE) n.º 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida y de la identificación de un nacional de un tercer país o un apátrida en situación ilegal, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley (versión refundida),* PE 597.620v03-00, 9 de junio de 2017.

([902]) Reglamento (UE) n.º 1052/2013 del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, por el que se crea un Sistema Europeo de Vigilancia de Fronteras (Eurosur), DO 2013 L 295.

los centros nacionales de coordinación y Frontex, la agencia de la UE encargada de desarrollar y aplicar el nuevo concepto de gestión integrada de las fronteras ([903]). Sus objetivos generales son los siguientes:

- reducir el número de inmigrantes ilegales que consiguen introducirse en la UE sin ser detectados;
- reducir el número de muertes de inmigrantes ilegales, salvando más vidas en el mar;
- incrementar la seguridad interna global de la UE mediante la contribución a la prevención de la delincuencia transfronteriza ([904]).

Eurosur comenzó a funcionar el 2 de diciembre de 2013 en todos los Estados miembros con fronteras exteriores y lo hará a partir del 1 de diciembre de 2014 en el resto de Estados. El Reglamento se aplica a la vigilancia de las fronteras exteriores terrestres, marítimas y aéreas de los Estados miembros. Eurosur intercambia y trata datos personales de forma muy limitada, ya que tanto los Estados miembros como Frontex solo están autorizados a intercambiar números de identificación de buques. Eurosur intercambia información operativa, como la localización de patrullas e incidentes y, por regla general, la información intercambiada no puede incluir datos personales ([905]). En los casos excepcionales en que se intercambien datos personales en el marco de Eurosur, el Reglamento establece que se aplicará en su totalidad el marco jurídico general de la EU sobre protección de datos ([906]).

([903]) Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo, de 14 de septiembre de 2016, sobre la Guardia Europea de Fronteras y Costas, por el que se modifica el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo y por el que se derogan el Reglamento (CE) n.º 863/2007 del Parlamento Europeo y del Consejo, el Reglamento (CE) n.º 2007/2004 del Consejo y la Decisión 2005/267/CE del Consejo, DO L 251.

([904]) Véase también: Comisión Europea (2008), Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Examen de la creación de un sistema europeo de vigilancia de fronteras (EUROSUR), COM(2008) 68 final, Bruselas, 13 de febrero de 2008; Comisión Europea (2011), Evaluación de impacto que acompaña a la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea un Sistema Europeo de Vigilancia de Fronteras (Eurosur), documento de trabajo de los servicios de la Comisión, SEC(2011) 1536 final, Bruselas, de 12 de diciembre de 2011, p. 18.

([905]) Comisión Europea, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29 de noviembre de 2013.

([906]) Reglamento 1052/2013, considerando 13 y artículo 13.

De este modo, Eurosur garantiza el derecho a la protección de datos, en concreto al establecer que los intercambios de datos personales deben atenerse a los criterios y garantías recogidos en la Directiva sobre protección de datos para las autoridades policiales y de justicia penal y el Reglamento general de protección de datos ([907]).

Sistema de Información Aduanera

Otro importante sistema común de información establecido a escala de la UE es el Sistema de Información Aduanera (SIA) ([908]). En el proceso de creación del mercado interior, se abolieron todos los controles y trámites relativos a la circulación de mercancías en el territorio de la UE, con lo cual se incrementó el riesgo de fraude. Este riesgo se contrarrestó intensificando la cooperación entre las administraciones aduaneras de los Estados miembros. La finalidad del SIA es ayudar a los Estados miembros a prevenir, investigar y perseguir las infracciones graves de la normativa aduanera y agrícola de los Estados miembros y de la UE. El SIA se establece por medio de dos actos jurídicos, adoptados en virtud de diferentes bases jurídicas: El Reglamento (CE) n.º 515/97 del Consejo trata de la cooperación entre las distintas autoridades administrativas nacionales para combatir el fraude en el contexto de la unión aduanera y la política agrícola común, mientras que la Decisión 2009/917/JAI del Consejo tiene por objeto facilitar la prevención, investigación y persecución de las infracciones graves de las leyes aduaneras. Esto significa que el SIA no solo tiene que ver con la aplicación de la ley.

La información incluida en el SIA incluye datos personales relacionados con mercancías, medios de transporte, empresas, personas y retenciones, embargos o confiscaciones de mercancías y de dinero en efectivo. Las categorías datos que se pueden tratar están claramente definidas e incluyen el nombre, la nacionalidad, el sexo, el lugar y la fecha de nacimiento de los interesados, el motivo de la introducción de sus datos en el sistema y el número de matrícula del medio de transporte ([909]). Dicha información puede utilizarse únicamente con fines de observación,

([907]) Ibíd., considerando 13 y artículo 13.

([908]) Consejo de la Unión Europea (1995), Acto del Consejo, de 26 de julio de 1995, por el que se establece el Convenio relativo a la utilización de la tecnología de la información a efectos aduaneros, DO 1995 C 316, modificado por Consejo de la Unión Europea (2009); Reglamento n.º 515/97 de 13 de marzo de 1997 relativo a la asistencia mutua entre las autoridades administrativas de los Estados miembros y a la colaboración entre éstas y la Comisión con objeto de asegurar la correcta aplicación de las reglamentaciones aduanera y agraria, Decisión 2009/917/JAI, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros, DO 2009 L 323 (Decisión del SIA).

([909]) Véase la Decisión del SIA, artículos 24, 25 y 28.

informe o inspecciones específicas o para realizar análisis estratégicos u operativos relacionados con personas sospechosas de infringir las disposiciones aduaneras.

El acceso al SIA se concede a las autoridades nacionales aduaneras, fiscales, agrícolas, sanitarias y policiales, así como a Europol y Eurojust.

El tratamiento de datos personales debe cumplir las normas específicas establecidas en el Reglamento n.º 515/97 y en la Decisión 2009/917/JAI del Consejo, así como las disposiciones del Reglamento general de protección de datos, del Reglamento de protección de datos de las instituciones de la UE, del Convenio 108 modernizado y de la Recomendación sobre la policía. El SEPD tiene la responsabilidad de velar por que el SIA cumpla lo dispuesto en el Reglamento (CE) n.º 45/2001. Convoca una reunión al menos una vez al año con todas las autoridades nacionales de control de la protección de datos que tienen competencias de supervisión en relación con el SIA.

Interoperabilidad entre los sistemas de información de la UE

El control de la migración, la gestión integrada de las fronteras exteriores de la Unión y la lucha contra el terrorismo y la delincuencia transfronteriza presentan retos importantes y han adquirido una complejidad cada vez mayor en un mundo globalizado. En los últimos años, la UE ha venido trabajando en un nuevo enfoque integrado para proteger y mantener la seguridad sin comprometer sus valores y libertades fundamentales. En este esfuerzo, es clave la eficacia en el intercambio de información entre los servicios de seguridad nacionales y entre los Estados miembros y los organismos pertinentes de la UE ([910]). Los sistemas existentes de información para el control de las fronteras y la seguridad interior tienen sus respectivos objetivos, estructura institucional, interesados y usuarios. La UE viene trabajando para corregir los déficits de funcionalidad de la gestión fragmentada de los datos de la Unión entre los distintos sistemas de información, como SIS II, VIS y Eurodac,

([910]) Comisión Europea (2016), Comunicación de la Comisión al Parlamento Europeo y al Consejo: Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final, Bruselas, 6 de abril de 2016, Comisión Europea (2016), Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo: Aumentar la seguridad en un mundo definido por la movilidad: mejora del intercambio de información para luchar contra el terrorismo y refuerzo de las fronteras exteriores, COM(2016) 602 final, Bruselas, 14 de septiembre de 2016, Comisión Europea (2016), Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la utilización del Sistema de Información de Schengen para el retorno de nacionales de terceros países en situación irregular. Véase también, Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo: Séptimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM (2017) 261 final, Bruselas, 16 de mayo de 2017.

explorando las posibilidades de interoperabilidad ([911]). El principal objetivo es garantizar que las autoridades policiales, aduaneras y judiciales competentes dispongan sistemáticamente de la información necesaria para desempeñar sus funciones, manteniendo al mismo tiempo un equilibrio con respecto a los derechos a la privacidad, la protección de datos y otros derechos fundamentales.

La interoperabilidad es «la capacidad de los sistemas de información para intercambiar datos y permitir la puesta en común de la información» ([912]). Este intercambio no debe comprometer las normas estrictamente necesarias de acceso y uso garantizadas por el Reglamento general de protección de datos, la Directiva sobre protección de datos para las autoridades policiales y de justicia penal, la Carta de los Derechos Fundamentales de la Unión Europea y todas las demás normas aplicables. Ninguna solución integrada de gestión de los datos debe afectar a los principios de limitación de la finalidad, protección de datos desde el diseño o protección de datos por defecto ([913]).

Además de mejorar las funcionalidades de los tres principales sistemas de información (SIS II, VIS y Eurodac), la Comisión ha propuesto la creación de un cuarto sistema centralizado de control fronterizo destinado a los nacionales de terceros países: el Sistema de Entradas y Salidas (SES) ([914]), que se estima que estará operativo en 2020 ([915]). La Comisión también ha realizado una propuesta sobre la creación de

([911]) Consejo de la Unión Europea (2005), El Programa de la Haya: consolidación de la libertad, la seguridad y la justicia en la Unión Europea, DO 2005 C 53, Comisión Europea (2010), Comunicación de la Comisión al Parlamento Europeo y al Consejo: Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia, COM(2010) 385 final; Comisión Europea (2016), Comunicación de la Comisión al Parlamento Europeo y al Consejo: Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM(2016) 205 final, Bruselas, 6 de abril de 2016, Comisión Europea (2016), Decisión de la Comisión de 17 de junio de 2016 por la que se crea el Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad, DO 2016 C 257.

([912]) Comisión Europea (2016), Comunicación de la Comisión al Parlamento Europeo y al Consejo: Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM (2016) 205 final, Bruselas, 6 de abril de 2016, p. 14.

([913]) Ibíd., pp. 4-5.

([914]) Comisión Europea (2016), Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece un Sistema de Entradas y Salidas (SES) para registrar los datos de entrada y salida y de la denegación de entrada de los nacionales de terceros países que cruzan las fronteras exteriores de los Estados miembros de la Unión Europea, se determinan las condiciones de acceso al SES con fines coercitivos y se modifican el Reglamento (CE) n.º 767/2008 y el Reglamento (UE) n.º 1077/2011, COM(2016) 194 final, Bruselas, 6 de abril de 2016.

([915]) Comisión Europea (2016), Comunicación de la Comisión al Parlamento Europeo y al Consejo: Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad, COM (2016) 205 final, Bruselas, 6 de abril de 2016, p. 5.

un Sistema Europeo de Información y Autorización de Viajes (SEIAV) ([916]), que recopilará información sobre las personas que viajen a la Unión Europea exentas de la obligación de visado con el fin de facilitar la realización de controles previos de seguridad y migración irregular.

([916]) Comisión Europea (2016), Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea un Sistema Europeo de Información y Autorización de Viajes (SEIAV) y por el que se modifican los Reglamentos (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/794 y (UE) 2016/1624, COM (2016) 731 final, 16 de noviembre de 2016.

9

Tipos específicos de datos y sus correspondientes normas de protección de datos

UE	Materias tratadas	CdE
Reglamento general de protección de datos Directiva sobre la privacidad y las comunicaciones electrónicas	**Comunicaciones electrónicas**	Convenio 108 modernizado Recomendación sobre los servicios de telecomunicación
Reglamento general de protección de datos, artículo 89	**Relaciones laborales**	Convenio 108 modernizado Recomendación sobre el empleo TEDH, *Copland contra Reino Unido*, n.º 62617/00, 2007.
Reglamento general de protección de datos, artículo 9, apartado 2, letra h) y letra i).	**Datos médicos**	Convenio 108 modernizado Recomendación sobre datos médicos TEDH, *Z. contra Finlandia*, n.º 22009/93, 1997
Reglamento sobre los ensayos clínicos	**Ensayos clínicos**	
Reglamento general de protección de datos, artículo 6, apartado 4, y artículo 89	**Estadísticas**	Convenio 108 modernizado Recomendación sobre datos estadísticos
Reglamento (CE) n.º 223/2009 relativo a la estadística europea TJUE, C-524/06, *Huber contra Bundesrepublik Deutschland* [GS], 2008	**Estadística oficial**	Convenio 108 modernizado Recomendación sobre datos estadísticos

UE	Materias tratadas	CdE
Directiva 2014/65/CE relativa a los mercados de instrumentos financieros Reglamento (UE) n.º 648/2012 relativo a los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones Reglamento (CE) n.º 1060/2009 sobre las agencias de calificación crediticia Directiva 2007/64/CE sobre servicios de pago en el mercado interior	**Datos financieros**	Convenio 108 modernizado Recomendación 90(19) sobre los datos de carácter personal utilizados con fines de pago y otras operaciones conexas TEDH, *Michaud contra Francia*, n.º 12323/11, 2012

Se han adoptado instrumentos jurídicos especiales a escala europea, en diversas instancias, que aplican de forma más detallada las normas generales del Convenio 108 modernizado o del Reglamento general de protección de datos a situaciones específicas.

9.1. Comunicaciones electrónicas

Puntos clave

- En la Recomendación del CdE de 1995 se incluyen normas específicas en materia de protección de datos en el ámbito de las telecomunicaciones, que hacen especial referencia a los servicios telefónicos.
- El tratamiento de datos personales relativos a la prestación de servicios de comunicaciones a escala de la UE está regulado por la Directiva sobre la privacidad y las comunicaciones electrónicas.
- La confidencialidad de las comunicaciones electrónicas afecta no solo al contenido de la comunicación sino también a los metadatos, como la información sobre quienes se comunican entre sí, en qué momento y durante cuánto tiempo, así como los datos de localización, como por ejemplo desde dónde se han comunicado los datos.

Las redes de comunicaciones tienen un mayor riesgo potencial de injerencias injustificadas en el ámbito personal de los usuarios, ya que ofrecen posibilidades técnicas añadidas de escucha y vigilancia de las comunicaciones a través de dichas redes. En consecuencia, se consideró necesario adoptar disposiciones especiales en materia de protección de datos para hacer frente a los riesgos especiales que tienen los usuarios de los servicios de comunicaciones.

En 1995, el **CdE** emitió una Recomendación sobre protección de datos en el ámbito de los servicios de telecomunicación, especialmente en lo que se refiere a los servicios telefónicos ([917]). De acuerdo con esta Recomendación, recogida y el tratamiento de datos personales en el contexto de las telecomunicaciones deberían realizarse únicamente para los fines de conexión de los usuarios a la red y puesta a disposición de un servicio de telecomunicación determinado y para los fines de facturación y verificación del pago, así como para garantizar una realización técnica óptima y el desarrollo de la red de servicio.

También se prestó especial atención al uso de las redes de comunicaciones para enviar mensajes de marketing directo. Como norma general, los mensajes de marketing directo no podrán estar dirigidos a ningún abonado que haya optado expresamente por no recibir mensajes publicitarios. Los dispositivos de llamadas automáticas de transmisión de mensajes publicitarios pregrabados únicamente podrán utilizarse si el abonado ha dado su consentimiento expreso. La legislación nacional deberá establecer normas detalladas en este ámbito.

En el **marco jurídico de la UE**, tras un primer intento en 1997, se adoptó en 2002 una Directiva sobre privacidad y las comunicaciones electrónicas, que fue modificada en 2009, a fin de completar y concretar las disposiciones de la Directiva de protección de datos para el sector de las telecomunicaciones ([918]).

La aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas se limita a los servicios de comunicaciones en las redes electrónicas públicas.

La Directiva sobre la privacidad y las comunicaciones electrónicas distingue tres categorías de datos principales generados durante una comunicación:

([917]) Consejo de Europa, Comité de Ministros (1995), Recomendación Rec (95)4 a los Estados miembros sobre la protección de los datos de carácter personal en el ámbito de los servicios de telecomunicación, especialmente en lo que se refiere a los servicios telefónicos, 7 de febrero de 1995.

([918]) 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 2002 L 201, modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n.º 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO 2009 L 337.

- los datos que constituyen el contenido de los mensajes enviados durante la comunicación y que son estrictamente confidenciales;

- los datos necesarios para establecer y mantener la comunicación —los llamados metadatos, que en la Directiva reciben el nombre de «datos de tráfico»—, como la información relativa a las partes de la comunicación, la hora y la duración de la comunicación;

- los metadatos contienen datos específicamente relacionados con la localización del dispositivo de comunicación, los denominados datos de localización, que son al mismo tiempo datos sobre la localización de los usuarios de los dispositivos de comunicación, especialmente en lo que respecta a los usuarios de dispositivos de comunicaciones móviles.

Los datos de tráfico pueden ser utilizados por el proveedor de servicios únicamente para los fines de facturación y prestación técnica del servicio. Con el consentimiento del interesado, sin embargo, estos datos pueden ser revelados a otros responsables del tratamiento que ofrezcan servicios con valor añadido, como indicar al usuario cuál es la estación de metro o farmacia más próxima a su localización, o la previsión meteorológica para dicha localización.

De conformidad al artículo 15 de la Directiva sobre privacidad y comunicaciones electrónicas, el resto de accesos a los datos sobre comunicaciones en redes electrónicas, como el acceso con fines de investigación de delitos, deberá cumplir los requisitos de las injerencias justificadas en el derecho a la protección de datos establecidos en el artículo 8, apartado 2 del CEDH y confirmados por los artículos 8 y 52 de la Carta de los Derechos Fundamentales de la Unión Europea. Dicho acceso puede consistir en el acceso con el fin de investigar delitos.

En 2009 se modificó la Directiva sobre la privacidad y las comunicaciones electrónicas ([919]) para incorporar lo siguiente:

([919]) Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n.º 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO 2009 L 337.

- Las restricciones al envío de correos electrónicos con fines de marketing directo se ampliaron a los servicios de mensajes cortos, servicios de mensajería multimedia y otros tipos de aplicaciones similares; los correos electrónicos de marketing están prohibidos salvo que se obtenga el consentimiento previo. A falta de dicho consentimiento, únicamente se podrán enviar correos electrónicos de marketing a clientes anteriores cuando estos hayan facilitado su dirección de correo electrónico y no se hayan opuesto a ello.

- Se estableció que los Estados miembros tenían la obligación de disponer de recursos judiciales contra las violaciones de la prohibición de comunicaciones no solicitadas ([920]).

- Ya no se permite el uso de *cookies*, programas informáticos que controlan y registran las acciones de los usuarios de ordenadores, sin el consentimiento de dichos usuarios. La legislación nacional debe regular de forma más detallada cómo se debe expresar y obtener el consentimiento para ofrecer protección suficiente ([921]).

En caso de que se produzca una violación de los datos como consecuencia de un acceso no autorizado, pérdida o destrucción de los datos, la autoridad de control competente deberá ser informada de inmediato. Los abonados deberán ser informados cuando puedan sufrir daños y perjuicios como consecuencia de una violación de datos ([922]).

La Directiva de conservación de datos ([923]) obligaba a los proveedores de servicios de comunicaciones a conservar metadatos. Sin embargo, esta Directiva fue anulada por el TJUE (para obtener más detalles, véase la sección 8.3).

([920]) Véase la Directiva modificada, artículo 13.

([921]) Ibíd., artículo 5; véase asimismo Grupo de Trabajo del Artículo 29 (2012), *Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies*, WP 194, Bruselas, 7 de junio de 2012.

([922]) Véase, asimismo, Grupo de Trabajo del Artículo 29 (2011), Documento de trabajo 1/2011 relativo al actual marco jurídico sobre las violaciones de datos de carácter personal y que presenta recomendaciones sobre las acciones que deben llevarse a cabo en un futuro, WP 184, Bruselas, 5 de abril de 2011.

([923]) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios en comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DO 2006 L 105.

Perspectivas

En enero de 2017, la Comisión Europea adoptó una nueva propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas en sustitución de la antigua Directiva sobre la privacidad y las comunicaciones electrónicas. El objetivo seguiría siendo la protección de «los derechos y las libertades fundamentales de las personas físicas y jurídicas en el ámbito de la prestación y utilización de servicios de comunicaciones electrónicas y, en particular, los derechos al respeto de la vida privada y las comunicaciones y la protección de las personas físicas en lo que respecta al tratamiento de datos personales». Además, la nueva propuesta se propone garantizar la libre circulación de datos de comunicaciones electrónicas y servicios de comunicaciones electrónicas en la Unión ([924]). Mientras el Reglamento general de protección de datos aborda fundamentalmente el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, el Reglamento propuesto pretende incorporar el artículo 7 de la Carta al Derecho derivado de la UE.

El Reglamento vendría a adaptar las disposiciones de la Directiva anterior a las nuevas tecnologías y a la realidad del mercado y establecería un marco integral y coherente con el Reglamento general de protección de datos. En este sentido, El Reglamento sobre la privacidad y las comunicaciones electrónicas sería *lex specialis* para el Reglamento general de protección de datos, y lo adaptaría a los datos de comunicaciones electrónicas que constituyen datos personales. El nuevo Reglamento comprende el tratamiento de «datos de comunicaciones electrónicas», incluidos los contenidos y metadatos de comunicaciones electrónicas que no son necesariamente datos personales. El alcance territorial se limita a la Unión Europea, incluso cuando los datos obtenidos en la UE sean objeto de tratamiento en terceros países, y se extiende a los proveedores de servicios de comunicaciones de transmisión libre (OTT, por sus siglas en inglés), que son proveedores de servicios que suministran contenidos, servicios o aplicaciones a través de internet sin la participación directa del operador de la red o proveedor de servicios de internet (ISP, por sus siglas en inglés). Algunos ejemplos de este tipo de proveedores son Skype (llamadas de voz y vídeo), WhatsApp (mensajería), Google (búsqueda), Spotify (música) o Netflix (contenidos de vídeo). Los mecanismos de control del cumplimiento del Reglamento general de protección de datos se aplicarían al nuevo Reglamento.

([924]) 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) 10 final, artículo 1.

Está previsto que se adopte el Reglamento sobre la privacidad y las comunicaciones electrónicas antes del 25 de mayo de 2018, y para entonces el Reglamento general de protección de datos será aplicable en los 28 Estados miembros. Sin embargo, esto está condicionado al acuerdo del Parlamento Europeo y del Consejo ([925]).

9.2. Datos de empleo

Puntos clave

- En la Recomendación del CdE relativa a los datos de empleo se incluyen normas específicas de protección de datos en las relaciones laborales.
- En el Reglamento general de protección de datos únicamente se hace una referencia específica a las relaciones laborales en el contexto del tratamiento de datos sensibles.
- La validez del consentimiento, que debe ser libre, como base jurídica para el tratamiento de datos sobre los empleados puede ser dudosa, considerando el desequilibrio económico que existe entre el empresario y los empleados. Las circunstancias del consentimiento deben valorarse de manera cuidadosa.

El tratamiento de datos en el contexto del empleo está sujeto a la legislación general de la UE sobre la protección de los datos personales. Sin embargo, hay un Reglamento ([926]) que regula específicamente la protección del tratamiento de los datos personales por las instituciones europeas en el contexto del empleo (entre otras cosas). En el Reglamento general de protección de datos, las relaciones laborales se mencionan específicamente en el artículo 9, apartado 2, que establece que se podrán tratar los datos personales cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral.

En virtud del Reglamento general de protección de datos, el empleado debe poder distinguir con claridad los datos en cuyo tratamiento o conservación consiente libremente y los fines para los que se conservan dichos datos. Los empleados también

([925]) Para más información, véase Comisión Europea (2017), «La Comisión propone estrictas normas de privacidad para todas las comunicaciones electrónicas y actualiza las normas sobre protección de datos para las instituciones de la UE», nota de prensa de 10 de enero de 2017.

([926]) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, DO 2001 L 8.

deben ser informados de sus derechos y del periodo de tiempo durante el que se conservarán los datos, antes de que puedan dar su consentimiento. En el caso de que se produzca una violación de la seguridad de los datos personales que pueda entrañar un alto riesgo para los derechos y libertades de las personas físicas, el empresario deberá comunicar dicha violación al empleado. El artículo 88 del Reglamento permite a los Estados miembros establecer normas más concretas para garantizar la protección de los derechos y libertades de los empleados en lo que respecta a sus datos personales en el contexto laboral.

Ejemplo: En el asunto *Worten* ([927]), los datos incluían un registro del tiempo de trabajo que contenía los periodos de trabajo diario y los periodos de descanso, que constituyen datos personales. La legislación nacional puede obligar al empleador a poner el registro del tiempo de trabajo a disposición de las autoridades nacionales competentes para la supervisión de las condiciones de trabajo. De este modo se tendría acceso inmediato a los datos personales pertinentes. Sin embargo, la autoridad nacional necesita acceder a los datos personales para poder supervisar la legislación sobre condiciones de trabajo ([928]).

Por lo que respecta al **CdE**, la Recomendación de datos de empleo se adoptó en 1989 y se revisó en 2015 ([929]). Esta Recomendación trata del tratamiento de datos personales en el contexto del empleo tanto en el sector público como en el privado. El tratamiento debe cumplir con determinados principios y restricciones, como el principio de transparencia y consulta con los representantes de los trabajadores antes de establecer sistemas de control en el trabajo. La Recomendación también establece que los empleadores deben aplicar medidas preventivas, como filtros, en lugar de controlar el uso de internet que realizan los trabajadores.

Un documento de trabajo del Grupo de Trabajo del Artículo 29 recoge una encuesta sobre los problemas de protección de datos más frecuentes en el contexto laboral ([930]). El Grupo de Trabajo analizó la importancia del consentimiento como base

([927]) TJUE, C-342/12, *Worten – Equipamentos para o Lar SA contra Autoridade para as Condições de Trabalho (ACT)*, 30 de mayo de 2013, apartado 19.

([928]) Ibíd., apartado 43.

([929]) Consejo de Europa, Comité de Ministros (2015), Recomendación Rec(2015)5 a los Estados miembros sobre el tratamiento de datos personales en el contexto del empleo, abril de 2015.

([930]) Grupo de Trabajo del Artículo 29 (2017), *Dictamen 2/2017 sobre una mayor armonización de las disposiciones relativas a la información*, WP 249, Bruselas, 8 de junio de 2017.

jurídica para el tratamiento de los datos laborales ([931]). El resultado fue que el desequilibrio económico existente entre el empleador que solicita el consentimiento y el empleado que lo otorga suscita a menudo dudas sobre si el consentimiento se ha otorgado libremente o no. Por tanto, las circunstancias que rodean al consentimiento tomado como base jurídica del tratamiento de datos deberán tomarse en consideración atentamente a la hora de valorar la validez del consentimiento en el contexto laboral.

Un problema de protección de datos que se da con frecuencia en el entorno laboral típico actual es el alcance legítimo del control de las comunicaciones electrónicas de los empleados en el lugar de trabajo. A menudo se afirma que este problema puede resolverse fácilmente prohibiendo el uso privado de los servicios de comunicación en el trabajo. Dicha prohibición general podría resultar, sin embargo, desproporcionada y poco realista. Las sentencias del TEDH en los casos *Copland contra Reino Unido* y *Bărbulescu contra Rumanía* tienen especial interés en este contexto.

Ejemplo: En *Copland contra Reino Unido* ([932]), el uso del teléfono, correo electrónico e internet por parte de una empleada de una universidad fue objeto de seguimiento en secreto, a fin de averiguar si estaba haciendo un uso excesivo de los servicios de dicha institución con fines personales. El TEDH dictaminó que las llamadas telefónicas desde las instalaciones profesionales están amparadas por los conceptos de vida privada y correspondencia. Por tanto, las llamadas y los correos electrónicos enviados desde el trabajo, así como la información derivada del seguimiento del uso personal de internet, están bajo la protección del artículo 8 del CEDH. En el caso de la demandante, no existían disposiciones que regulasen las circunstancias en que los empleadores pudieran controlar el uso del teléfono, correo electrónico e internet por parte de los empleados. Por tanto, la injerencia no se había producido de conformidad con la ley. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

([931]) Grupo de Trabajo del Artículo 29 (2005), Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, WP 114, Bruselas, 25 de noviembre de 2005.

([932]) TEDH, *Copland contra Reino Unido*, n.º 62617/00, 3 de abril de 2007.

Ejemplo: En *Bărbulescu contra Rumanía* ([933]), el demandante había sido despedido por utilizar la conexión a internet de su empleador en horario laboral, vulnerando el reglamento interno. Su empleador controlaba sus comunicaciones. Los registros, que mostraban mensajes de carácter puramente privado, se presentaron durante el juicio nacional. El TEDH resolvió que el artículo 8 era de aplicación y dejó abierta la cuestión de si el restrictivo reglamento del empleador dejaba al demandante una expectativa razonable de privacidad, pero en cualquier caso determinó que las instrucciones del empleador no podían reducir a cero la vida social privada en el lugar de trabajo.

En lo que respecta al fondo del asunto, se debía otorgar a los Estados Contratantes un amplio margen de apreciación para determinar la necesidad de establecer un marco jurídico que reglamentase las condiciones en las que un empleador podía regular las comunicaciones no profesionales de sus empleados, electrónicas o de otra índole, en el lugar de trabajo. No obstante, las autoridades nacionales debían asegurarse de que la introducción por parte de un empleador de medidas de vigilancia de la correspondencia y otras comunicaciones, al margen del alcance y duración de las mismas, fuera acompañada de garantías adecuadas y suficientes contra los abusos. Era esencial respetar la proporcionalidad y disponer de garantías procesales contra la arbitrariedad y el TEDH señaló una serie de factores pertinentes en las circunstancias en cuestión. Estos factores incluían, entre otros, el alcance de la vigilancia por parte del empleador y el grado de invasión de la privacidad del empleado, las consecuencias para el empleado y si se habían establecido garantías adecuadas. Además, las autoridades nacionales debían garantizar que un empleado cuyas comunicaciones hubieran sido objeto de vigilancia dispusiera de un recurso ante un órgano judicial con jurisdicción para determinar, al menos en el fondo, cómo se habían respetado los criterios establecidos y si las medidas impugnadas eran lícitas.

En este caso, el TEDH resolvió que existía una violación del artículo 8 porque las autoridades nacionales no habían protegido adecuadamente el derecho del demandante al respeto de su vida privada y su correspondencia y, en consecuencia, no habían alcanzado un equilibrio justo entre los intereses enfrentados.

([933]) TEDH, *Bărbulescu contra Rumanía* [GS], n.º 61496/08, 5 de septiembre de 2017, apartado 121.

Según la Recomendación del CdE sobre empleo, los datos personales recogidos con fines laborales deberán ser obtenidos directamente del empleado concreto.

Los datos personales recogidos para la contratación deben limitarse a la información necesaria para evaluar la idoneidad de los candidatos y su potencial profesional.

La Recomendación también menciona de forma específica los datos sobre juicios de valor relacionados con el desempeño o el potencial de los empleados concretos. Los datos sobre juicios de valor deben estar basados en evaluaciones lícitas y honestas y no deben ser insultantes en su formulación. Así lo exigen los principios de tratamiento leal de los datos y de exactitud de los datos.

Un aspecto concreto de la legislación de protección de datos en la relación entre empleado y empleador es el papel que desempeñan los representantes de los trabajadores. Estos representantes solo podrán recibir los datos personales de los trabajadores en la medida en que sea necesario para que ellos puedan representar los intereses de los trabajadores o si dichos datos son necesarios para cumplir o supervisar las obligaciones establecidas en convenios colectivos.

Los datos personales sensibles recogidos con fines laborales solo podrán ser objeto de tratamiento en casos concretos y de acuerdo con las garantías establecidas en la legislación nacional. Los empleadores solo podrán preguntar a los empleados o candidatos a puestos de trabajo por su estado de salud o someterles a exámenes médicos cuando esto sea necesario. Esta necesidad puede concurrir para determinar su idoneidad para el empleo, para cumplir los requisitos de la medicina preventiva, para proteger los intereses vitales del interesado o de otros empleados y personas físicas, para que se puedan otorgar beneficios sociales o para responder a peticiones judiciales. Los datos de salud no podrán ser obtenidos de ninguna otra fuente que el propio empleado afectado, excepto cuando se haya obtenido un consentimiento expreso e informado o cuando así se establezca en la legislación nacional.

Con arreglo a la Recomendación sobre empleo, los empleados deberán ser informados sobre la finalidad del tratamiento de sus datos personales, el tipo de datos personales almacenados, las entidades a las que se comuniquen los datos periódicamente y la finalidad y la base jurídica de dichas comunicaciones. Solo se podrá acceder a las comunicaciones electrónicas en el lugar de trabajo por razones de seguridad u otras razones legítimas, y solo se permite dicho acceso una vez que los empleados hayan sido informados de que el empleador puede tener acceso a este tipo de comunicaciones.

Los empleados deben tener derecho de acceso a sus datos de empleo, así como un derecho de rectificación o de supresión. Si se tratan datos sobre juicios de valor, los empleados deben tener además derecho a impugnar dicho juicio. Sin embargo, estos derechos podrán estar limitados temporalmente con fines de investigación interna. Si se deniega al empleado el acceso, la rectificación o la supresión de sus datos personales de empleo, la legislación nacional deberá establecer procedimientos adecuados para impugnar dicha denegación.

9.3. Datos de salud

Punto clave

- Los datos médicos son datos sensibles y, por tanto, gozan de una protección específica.

Los datos personales relacionados con el estado de salud del interesado se califican como datos sensibles en virtud del artículo 9, apartado 1, del Reglamento general de protección de datos y en virtud del artículo 6 del Convenio 108 modernizado. En consecuencia, los datos de salud están sometidos a un régimen de tratamiento de datos más estricto que los datos no sensibles. El Reglamento general de protección de datos prohíbe el tratamiento de «datos personales relativos a la salud» (entendidos como «todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro» ([934]), así como de los datos genéticos y biométricos, a menos que se autorice en virtud del artículo 9, apartado 2. Ambos tipos de datos se han añadido a la lista de «categorías especiales de datos» ([935]).

Ejemplo: En *Z contra Finlandia* ([936]), el ex marido de la demandante, que estaba infectado por el VIH, había cometido una serie de delitos sexuales. Posteriormente fue condenado por homicidio, con motivo de que había expuesto a sus víctimas al riesgo de infección por VIH a sabiendas. El tribunal

([934]) Reglamento general de protección de datos, considerando 35.

([935]) Ibíd., artículo 2.

([936]) TEDH, *Z contra Finlandia*, n.º 22009/93, 25 de febrero de 1997, apartados 94 y 112; véase también TEDH, *M.S. contra Suecia*, n.º 20837/92, 27 de agosto de 1997; TEDH, *L.L. contra Francia*, n.º 7508/02, 10 de octubre de 2006; TEDH, *I contra Finlandia*, n.º 20511/03, 17 de julio de 2008; TEDH, *K.H. y otros contra Eslovaquia*, n.º 32881/04, 28 de abril de 2009; TEDH, *Szuluk contra Reino Unido*, n.º 36936/05, 2 junio de 2009.

nacional ordenó mantener la confidencialidad de la sentencia íntegra y de las actuaciones judiciales durante un periodo de diez años, a pesar de las peticiones por parte de la demandante de que se aplicase un periodo de confidencialidad más prolongado. El tribunal de apelación denegó dichas peticiones, e incluyó en su sentencia los nombres completos tanto de la demandante como de su ex marido. El TEDH dictaminó que esta injerencia no se consideraba necesaria en una sociedad democrática, porque la protección de los datos médicos tenía un carácter esencial en el disfrute del derecho al respeto de la vida privada y familiar, en particular en relación con la información sobre infecciones por VIH, dado el estigma vinculado a esta enfermedad en muchas sociedades. Por tanto, el Tribunal concluyó que el hecho de autorizar el acceso a la sentencia del tribunal de apelación, en la que se establecía la identidad y la afección médica de la demandante, tan solo diez años después de publicarse el fallo, constituiría una violación del artículo 8 del TEDH.

En el **Derecho de la UE**, el artículo 9, apartado 2, letra h) del Reglamento general de protección de datos permite el tratamiento de datos médicos cuando resulte necesario para los fines de prevención o diagnóstico médicos, prestación de asistencia sanitaria o tratamientos médicos o gestión de servicios sanitarios. Sin embargo, el tratamiento se permite únicamente cuando es realizado por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente.

En el **Derecho del CdE**, La Recomendación del CdE sobre datos médicos de 1997 aplica los principios del Convenio 108 al tratamiento de datos en el ámbito médico de forma más detallada ([937]). Las normas propuestas están en consonancia con las del Reglamento general de protección de datos que hacen referencia a los fines legítimos del tratamiento de datos médicos, las necesarias obligaciones de secreto profesional de las personas que emplean los datos de salud y los derechos de los interesados de transparencia, acceso, rectificación y supresión. Además, los datos médicos que sean tratados de forma lícita por los profesionales sanitarios no podrán ser transferidos a las autoridades policiales salvo que existan «garantías suficientes para evitar una difusión que contravenga el respeto a [...] la vida privada, garantizado en virtud del artículo 8 del CEDH» ([938]). La legislación nacional también debe

([937]) Consejo de Europa, Comité de Ministros (1997), Recomendación Rec(97)5 a los Estados miembros relativa a la protección de los datos médicos, 13 de febrero de 1997.

([938]) TEDH, *Avilkina y otros contra Rusia*, n.º 1585/09, 6 de junio de 2013, apartado 53.

«formularse con suficiente precisión y ofrecer una protección jurídica adecuada contra la arbitrariedad» ([939]).

Además, la Recomendación sobre datos médicos incluye disposiciones especiales relativas a los datos médicos de los niños no nacidos y las personas incapacitadas, así como sobre el tratamiento de datos genéticos. Se reconoce expresamente que la investigación científica es motivo para conservar datos durante más tiempo del necesario, aunque esto suele requerir que los datos sean anonimizados. El artículo 12 de la Recomendación sobre datos médicos propone una normativa detallada para las situaciones en que los investigadores precisen de datos personales y los datos anonimizados resulten insuficientes.

La seudonimización puede ser un medio adecuado para satisfacer las necesidades científicas y, al mismo tiempo, proteger los intereses de los pacientes afectados. El concepto de la seudonimización en el contexto de la protección de datos se explica con más detalle en la sección 2.1.1.

La Recomendación del CdE de 2016 sobre los datos obtenidos de pruebas genéticas también se aplica al tratamiento en el campo de la medicina ([940]). Esta recomendación es de gran importancia para la salud electrónica, donde se utilizan las TIC para facilitar la atención médica. Un ejemplo es enviar los resultados de la prueba de paternidad de un paciente de un profesional sanitario a otro. Esta Recomendación tiene por objeto proteger los derechos de las personas cuyos datos personales se tratan con fines de contratación de seguros de protección contra riesgos que afectan a la salud, integridad física, edad o fallecimiento de una persona. Las aseguradoras necesitan justificar el tratamiento de los datos relacionados con la salud y este debe ser proporcionado a la naturaleza e importancia del riesgo considerado. El tratamiento de este tipo de datos depende del consentimiento del interesado. Las aseguradoras también deben establecer garantías al respecto de la conservación de datos relacionados con la salud.

Los ensayos clínicos —que tienen por objeto evaluar los efectos de nuevos fármacos en pacientes en entornos de investigación documentados— tienen considerables implicaciones en materia de protección de datos. Los ensayos clínicos de medicamentos de uso humano están regulados por el Reglamento (UE) n.º 536/2014 del

([939]) TEDH, *L.H. contra Letonia*, n.º 52019/07, 29 de abril de 2014, apartado 59.

([940]) Consejo de Europa, Comité de Ministros (2016), Recomendación Rec(2016)8 a los Estados miembros sobre el tratamiento de datos personales relacionados con la salud para finalidades de aseguramiento, incluyendo los datos derivados de test genéticos, 26 de octubre de 2016.

Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (Reglamento sobre los ensayos clínicos) ([941]). Los principales elementos del Reglamento sobre los ensayos clínicos son:

- un procedimiento de aplicación agilizado a través del portal de la UE ([942]);
- plazos para evaluar las solicitudes de ensayos clínicos ([943]);
- un comité ético que forme parte de la evaluación, de acuerdo con la legislación de los Estados miembros (y el Derecho europeo que define los periodos de tiempo aplicables) ([944]); y
- mayor transparencia de los ensayos clínicos y sus resultados ([945]).

El Reglamento general de protección de datos especifica que, para los fines del consentimiento en participar en actividades de investigación científica en ensayos clínicos, se aplica el Reglamento (UE) n.º 536/2014 ([946]).

En el ámbito de la UE están pendientes de aprobación muchas otras iniciativas legislativas y de otra índole en materia de datos personales en el sector sanitario ([947]).

Historiales médicos electrónicos

El historial médico electrónico es «un historial médico completo o una documentación similar del estado de salud física y mental pasado y actual de un individuo, en formato electrónico, que permite acceder fácilmente a estos datos para un

([941]) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (Reglamento sobre ensayos clínicos), DO 2014 L 158.

([942]) Reglamento sobre los ensayos clínicos, artículo 5, apartado 1.

([943]) Ibíd., artículo 5, apartados 2 a 5.

([944]) Ibíd., artículo 2, apartado 11.

([945]) Ibíd., artículo 9, apartado 1 y considerando 67.

([946]) Reglamento general de protección de datos, considerandos 156 y 161.

([947]) SEPD (2013), Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión relativa al Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI, Bruselas, 27 de marzo de 2013.

tratamiento médico y otros fines conexos» ([948]). Los historiales médicos electrónicos son versiones electrónicas de la historia médica de los pacientes y pueden incluir datos clínicos relativos a estas personas, como su historia médica anterior, problemas y afecciones, medicaciones y tratamientos, así como resultados e informes de exámenes y análisis de laboratorio. Los médicos generalistas, farmacéuticos y otros profesionales sanitarios pueden acceder a estos archivos electrónicos, que pueden ser desde historiales completos hasta meros extractos o resúmenes. El concepto de «salud electrónica» también tiene que ver con estos historiales sanitarios.

Ejemplo: El Sr. A contrata una póliza de seguro con la empresa B, la aseguradora. Esta última obtendrá de A cierta información relacionada con la salud, como problemas de salud o enfermedades actuales. La aseguradora deberá conservar los datos personales relacionados con la salud de A separados de otros datos. La aseguradora también deberá conservar los datos personales relacionados con la salud separados de otros datos personales. Esto implica que solo el responsable del expediente de A tendrá acceso a los datos relacionados con la salud de A.

No obstante, los archivos de salud electrónicos plantean algunos problemas de protección de datos, como su accesibilidad, adecuada conservación y acceso por el interesado.

Además de los historiales médicos electrónicos, la Comisión Europea publicó el 10 de abril de 2014 un Libro verde sobre sanidad móvil, en el que se indica que la sanidad móvil constituye un sector emergente y en rápida evolución, que tiene el potencial de participar en la transformación de la atención sanitaria y de incrementar su calidad y su eficacia. El término cubre la práctica de la medicina y la prestación de servicios sanitarios mediante dispositivos móviles, como teléfonos móviles, dispositivos de seguimiento de pacientes, asistentes digitales personales y otros dispositivos inalámbricos (por ejemplo, aplicaciones de bienestar) que pueden conectarse a dispositivos o sensores médicos ([949]). Este documento describe los riesgos que puede entrañar el desarrollo de la sanidad móvil para la protección de los datos de carácter personal y establece que, dada la naturaleza sensible de los datos sanitarios, las soluciones de sanidad móvil deberán contener garantías de seguridad específicas y apropiadas para los datos del paciente, como el cifrado, y mecanismos

([948]) Recomendación de la Comisión, de 2 de julio de 2008, sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos, apartado 3, letra c).

([949]) Comisión Europea (20140), *Libro verde sobre sanidad móvil,* COM(2014) 219 final, Bruselas, 10 de abril de 2014.

adecuados de autenticación del paciente para mitigar los riesgos para la seguridad. El cumplimiento de la normativa sobre la protección de datos personales, que incluye la obligación de proporcionar información al interesado, la seguridad de los datos y el principio de licitud del tratamiento de los datos personales, es vital para generar confianza en las soluciones de sanidad móvil ([950]). Con este fin, el sector ha elaborado un Código de Conducta basado en las aportaciones de una gran variedad de partes interesadas, entre las que hay representantes expertos en protección de datos, autorregulación y corregulación, TIC y atención sanitaria ([951]). En el momento de redactarse el presente manual, se había presentado el proyecto de código de conducta al Grupo de Trabajo del Artículo 29 para que formulase observaciones sobre él, a la espera de su aprobación formal.

9.4. Tratamiento de datos con fines de investigación y fines estadísticos

Puntos clave

- Los datos recogidos con fines estadísticos o de investigación científica o histórica no pueden utilizarse para ningún otro fin.
- Los datos recogidos de forma legítima con cualquier fin pueden utilizarse ulteriormente con fines estadísticos o de investigación científica o histórica, siempre que existan garantías adecuadas. Estas garantías pueden ser la anonimización o seudonimización de los datos antes de su transmisión a terceros.

El Derecho de la UE contempla el tratamiento de datos con fines estadísticos y de investigación científica o histórica, siempre que se establezcan garantías adecuadas para los derechos y libertades de los interesados. Dichas garantías pueden incluir la seudonimización ([952]). El Derecho de la UE o el Derecho nacional podrán establecer ciertas excepciones a los derechos de los interesados cuando sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines legítimos de la investigación ([953]). Se pueden introducir excepciones al derecho de acceso por el interesado, al derecho de rectificación, al derecho de limitación del tratamiento y al derecho de oposición.

([950]) Ibíd., p. 8.

([951]) Draft Code of Conduct on privacy for mobile health applications, 7 de junio de 2016.

([952]) Reglamento general de protección de datos, artículo 89, apartado 1.

([953]) Ibíd., artículo 89, apartado 2.

Aunque los datos lícitamente recogidos por un responsable con cualquier fin pueden ser reutilizados por dicho responsable para sus propios fines estadísticos o de investigación científica o histórica, los datos tendrían que ser anonimizados o sujetos a medidas como la seudonimización, en función del contexto, antes de transmitirlos a un tercero para los fines estadísticos o de investigación científica o histórica, salvo que el interesado consienta en ello o que esté específicamente recogido en el Derecho nacional. Los datos objeto de seudonimización siguen estando sujetos al Reglamento general de protección de datos, a diferencia de los datos anónimos ([954]).

Así pues, el Reglamento da un tratamiento especial a la investigación respecto de las normas generales de protección de datos para evitar que se limite el desarrollo de la investigación y cumplir con el objetivo de crear un espacio europeo de investigación, como se establece en el artículo 179 del TFUE. Contempla una interpretación amplia del tratamiento de datos personales con fines de investigación científica, que incluye la demostración y el desarrollo tecnológicos, la investigación básica, la investigación aplicada y la investigación de financiación privada. También reconoce la importancia de recopilar datos de registros con fines de investigación y lo difícil que puede ser establecer debidamente la finalidad ulterior del tratamiento de los datos personales con fines científicos en el momento de recoger los datos ([955]). Por este motivo, el Reglamento permite el tratamiento de datos con estos fines, sin el consentimiento del interesado, siempre que existan garantías adecuadas.

Un ejemplo importante de uso de datos con fines estadísticos son las estadísticas oficiales, obtenidas por las oficinas de estadística nacionales y de la UE de conformidad con la legislación nacional y europea sobre estadística oficial. De acuerdo con esta legislación, los ciudadanos y las empresas suelen estar obligados a comunicar datos a las autoridades estadísticas competentes. Los funcionarios que trabajan en las oficinas de estadística están vinculados por obligaciones especiales de secreto profesional que deben cumplir adecuadamente, ya que resultan fundamentales para el elevado nivel de confianza ciudadana que hace falta para poner datos a disposición de las autoridades estadísticas ([956]).

El Reglamento (CE) n.º 223/2009 relativo a la estadística europea (Reglamento de la estadística europea) contiene normas fundamentales para la protección de datos en el contexto de la estadística oficial y puede considerarse, por tanto, pertinente

([954]) Ibíd., considerando 26.

([955]) Ibíd., considerandos 33, 157 y 159.

([956]) Ibíd., artículo 90.

para las disposiciones sobre la estadística oficial adoptadas a escala nacional ([957]). El Reglamento mantiene el principio de que la actividad estadística oficial necesita una base jurídica suficientemente clara ([958]).

Ejemplo: En *Huber contra Bundesrepublik Deutschland* ([959]), un empresario austriaco que se había trasladado a Alemania se quejó de que la recogida de datos personales de nacionales extranjeros por parte de las autoridades alemanas y su conservación en un registro central (AZR), también con fines estadísticos, violaba sus derechos en virtud de la Directiva de protección de datos. Considerando que la Directiva 95/46 tiene por objeto garantizar un nivel equivalente de protección de datos en todos los Estados miembros, el TJUE dictaminó que, a fin de garantizar un alto nivel de protección en la UE, el significado del concepto de necesidad recogido en el artículo 7, letra e) no puede variar según los Estados miembros. Por tanto, se trata de un concepto que tiene su propio significado independiente en el Derecho de la UE y debe interpretarse de manera que refleje plenamente el objetivo de la Directiva 95/46. El TJUE, señalando que los fines estadísticos requieren únicamente el tratamiento de información anónima, resolvió que el registro alemán no era compatible con el requisito de necesidad establecido en el artículo 7, letra e).

En el contexto del **CdE**, se puede realizar un tratamiento ulterior de los datos con fines científicos, históricos o estadísticos, siempre que sea en interés público y aplicando garantías adecuadas ([960]). También se pueden limitar los derechos de los interesados cuando el tratamiento de datos se realice con fines estadísticos, siempre que no exista un riesgo reconocible de violación de sus derechos y libertades ([961]).

([957]) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas, DO 2009 L 87, en su versión modificada por el Reglamento (UE) 2015/759 del Parlamento Europeo y del Consejo, de 29 de abril de 2015, por el que se modifica el Reglamento (CE) n.º 223/2009, relativo a la estadística europea, DO 2015 L 123.

([958]) Este principio se establecerá de forma más detallada en el Código de buenas prácticas de las estadísticas europeas de Eurostat, que deberá ofrecer, con arreglo a lo dispuesto en el artículo 11 del Reglamento de la estadística europea, orientaciones éticas sobre cómo elaborar las estadísticas oficiales, incluido el uso considerado que debe hacerse de los datos personales.

([959]) TJUE, C-524/06, *Heinz Huber contra Bundesrepublik Deutschland* [GS], 16 de diciembre de 2008, especialmente el apartado 68.

([960]) Convenio 108 modernizado, artículo 5, apartado 4, letra b).

([961]) Ibíd., artículo 11, apartado 2.

La Recomendación sobre datos estadísticos adoptada en 1997 trata de la realización de la actividad estadística en los sectores público y privado ([962]).

Los datos recogidos por un responsable con fines estadísticos no podrán utilizarse para otros fines. Los datos recogidos con fines no estadísticos deberán estar disponibles para su uso estadístico posterior. La Recomendación sobre datos estadísticos permite también comunicar los datos a terceros siempre que sea únicamente con fines estadísticos. En estos casos, las partes deberán acordar por escrito el alcance del uso legítimo ulterior con fines estadísticos. Dado que lo anterior no puede sustituir al consentimiento del interesado —cuando sea necesario—, deberán existir garantías adecuadas en la legislación nacional para reducir al mínimo el riesgo de que se haga un uso indebido de los datos personales, como la obligación de anonimizar o seudonimizar los datos antes de comunicarlos.

Los profesionales de la investigación estadística deben estar sujetos a obligaciones especiales de secreto profesional —como suele ocurrir en el caso de las estadísticas oficiales— conforme al Derecho nacional. Esto deberá extenderse también a los entrevistadores y a otros recopiladores de datos personales cuando hayan sido contratados para recopilar datos de los interesados o de otras personas.

Si una encuesta estadística que emplea datos personales no está autorizada por la ley, puede que los interesados deban dar su consentimiento al uso de sus datos para que la encuesta sea legítima, o puede que deban tener la posibilidad de oponerse. En el caso de que se recojan datos personales con fines estadísticos por medio de entrevistadores, se les deberá informar con claridad de si tienen o no la obligación de facilitar datos con arreglo a la legislación nacional.

Si una encuesta estadística no puede realizarse con datos anónimos y resulta necesario utilizar datos personales, los datos recogidos con este fin deberán anonimizarse lo antes posible. Los resultados de la encuesta estadística no deberán permitir, cuando menos, que se identifique a ningún interesado, salvo que ello no entrañe un riesgo manifiesto.

Una vez finalizado el análisis estadístico, los datos personales utilizados deberán ser suprimidos o anonimizados. En este tipo de casos, la Recomendación sobre datos estadísticos aconseja que los datos identificativos se conserven por separado de

([962]) Consejo de Europa, Comité de Ministros (1997), Recomendación Rec(97)18 a los Estados miembros relativa a la protección de datos de carácter personal recogidos y tratados con fines estadísticos, 30 de septiembre de 1997.

otros datos personales. Esto implica, por ejemplo, que la clave de cifrado o la lista que contenga los sinónimos identificativos debe conservarse por separado del resto de datos.

9.5. Datos financieros

Puntos clave

- A pesar de que los datos financieros no se consideran datos sensibles en virtud del Convenio 108 o del Reglamento general de protección de datos, su tratamiento requiere garantías especiales que garanticen la exactitud y la seguridad de los datos.
- En particular, los sistemas de pago electrónico necesitan incorporar medidas de protección de datos, es decir, protección de la privacidad o de los datos desde el diseño y por defecto.
- En este ámbito pueden plantearse problemas específicos de protección de datos debido a la necesidad de aplicar mecanismos de autenticación adecuados.

Ejemplo: En *Michaud contra Francia* ([963]), el demandante, un abogado francés, impugnaba su obligación, con arreglo a la legislación francesa, de informar sobre las sospechas relativas a posibles actividades de blanqueo de capitales por parte de sus clientes. El TEDH observó que el hecho de exigir a los abogados que faciliten a las autoridades administrativas información sobre otra persona que haya llegado a su poder a través de sus comunicaciones profesionales constituía una injerencia en el derecho de los abogados al respeto de su vida privada y correspondencia, con arreglo al artículo 8 del CEDH, ya que ese concepto englobaba las actividades de carácter profesional o comercial. Sin embargo, dicha injerencia había sido realizada de conformidad con la ley y perseguía un fin legítimo, en concreto la prevención de desórdenes y actos delictivos. Dado que los abogados solo están sujetos a la obligación de denunciar actividades sospechosas en circunstancias muy concretas, el TED dictaminó que esta obligación era proporcionada. Concluyó que no había existido una violación del artículo 8.

([963]) TEDH, *Michaud contra Francia*, n.º 12323/11, 6 de diciembre de 2012. Véase también TEDH, *Niemietz contra Alemania*, n.º 13710/88, 16 de diciembre de 1992, apartado 29; y TEDH, *Halford contra Reino Unido*, n.º 20605/92, 25 de junio de 1997, apartado 42.

Ejemplo: En *M.N. y otros contra San Marino* ([964]), el demandante, ciudadano italiano, formalizó un acuerdo fiduciario con una empresa investigada. Esto hizo que la empresa fuera objeto de una búsqueda e incautación de copias de documentación (electrónica). El demandante presentó una reclamación ante el tribunal de San Marino asegurando no tener ningún vínculo con los presuntos delitos. Sin embargo, el tribunal declaró su reclamación inadmisible, ya que no era una «parte interesada». El TEDH dictaminó que el demandante se había encontrado en una situación de desventaja significativa en lo que respecta a la protección judicial en comparación con las «partes interesadas», pero aun así sus datos fueron objeto de las operaciones de búsqueda e incautación. Por tanto, el Tribunal resolvió que se había violado el artículo 8.

Ejemplo: En *G.S.B. contra Suiza* ([965]), se enviaron los datos bancarios del demandante a las autoridades tributarias estadounidenses en virtud del acuerdo de cooperación administrativa existente entre Suiza y los Estados Unidos. El TEDH dictaminó que la transmisión no constituía violación del artículo 8 del CEDH porque la injerencia en el derecho del demandante a la privacidad estaba establecida por la ley, perseguía un fin legítimo y era proporcionada al interés público en juego.

El **CdE** desarrolló la aplicación del marco jurídico general de protección de datos (establecido en el Convenio 108) en el contexto de los pagos a través de la Recomendación Rec (90)19 de 1990 ([966]). Dicha recomendación aclara el alcance de la recogida y el uso lícitos de los datos en el contexto de los pagos, en particular, mediante tarjetas de pago. También realiza recomendaciones detalladas a los legisladores nacionales sobre las normas aplicables a la revelación de datos de pago a terceros, sobre los límites de la conservación de datos, sobre transparencia, seguridad de los datos y flujos de datos transfronterizos, y sobre control y recursos jurídicos. El CdE también ha emitido un Dictamen sobre la transferencia de datos fiscales ([967]), que incluye recomendaciones y cuestiones que deben tenerse en cuenta a la hora de realizar transferencias de datos fiscales.

([964]) TEDH, *M.N. y otros contra San Marino*, n.º 28005/12, 7 de julio de 2015;

([965]) *G.S.B. contra Suiza*, n.º 28601/11, 22 de diciembre de 2015.

([966]) Consejo de Europa, Comité de Ministros (1990), *Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations*, 13 de septiembre de 1990.

([967]) Consejo de Europa, Comité consultivo de la Convención 108 (2014), Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, 4 de junio de 2014.

El TEDH permite la transmisión de datos financieros —especialmente, los datos de la cuenta bancaria de una persona física— conforme al artículo 8 del CEDH, si está establecida por ley, persigue un fin legítimo y es proporcionada al interés público en juego ([968]).

En el ámbito del **Derecho de la UE**, los sistemas de pago electrónico que conllevan el tratamiento de datos personales deben cumplir el Reglamento general de protección de datos. Por tanto, estos sistemas deben garantizar la protección de los datos desde el diseño y por defecto. La protección de datos desde el diseño obliga al responsable del tratamiento a adoptar medidas técnicas y organizativas adecuadas para aplicar los principios de protección de datos. La protección de datos por defecto implica que el responsable del tratamiento debe asegurarse de que únicamente los datos personales que sean necesarios para un fin determinado puedan ser objeto de tratamiento por defecto (véase la sección 4.4). En relación con los datos financieros, el TJUE dictaminó que los datos fiscales transferidos pueden ser constitutivos de datos personales ([969]). El Grupo de Trabajo del Artículo 29 publicó directrices sobre este tema para los Estados miembros, que incluyen criterios para garantizar el cumplimiento de las normas de protección de datos en los intercambios automáticos de datos personales con fines tributarios ([970]). Además, se han promulgado distintos instrumentos jurídicos para regular los mercados financieros y las actividades de las entidades de crédito y empresas de inversión ([971]). Otros instrumentos jurídicos ayudan a luchar contra las operaciones con información privilegiada y la manipulación del mercado ([972]). Los principales aspectos que afectan a la protección de datos son:

- la conservación de los registros sobre transacciones financieras;

([968]) TEDH, *G.S.B. contra Suiza*, n.º 28601/11, 22 de diciembre de 2015.

([969]) TJUE, C-201/14, *Smaranda Bara y otros contra Casa Națională de Asigurări de Sănătate y otros*, 1 de octubre de 2015, apartado 29.

([970]) Grupo de Trabajo del Artículo 29 (2015), Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes, 14/EN WP 230.

([971]) Directiva 2014/65/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE, DO 2014 L 173; Reglamento (UE) n.º 600/2014 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativo a los instrumentos financieros y por el que se modifica el Reglamento (UE) n.º 648/2012, DO 2014 L 173; Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la supervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE, DO 2013 L 176.

([972]) Reglamento (UE) n.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre el abuso de mercado) y por el que se derogan la Directiva 2003/6/CE del Parlamento Europeo y del Consejo y las Directivas 2003/124/CE, 2003/125/CE y 2004/72/CE de la Comisión, DO 2014 L 173.

- la transferencia de datos personales a terceros países;
- el registro de conversaciones telefónicas o de comunicaciones electrónicas, lo cual incluye la facultad de las autoridades competentes de solicitar los registros telefónicos y de tráfico de datos;
- la divulgación de datos personales, lo cual incluye la publicación de sanciones;
- las facultades de supervisión e investigación de las autoridades competentes, que incluyen las inspecciones *in situ* y el acceso a locales privados con el fin de proceder a la incautación de documentos;
- los mecanismos de notificación de incumplimientos, es decir, los sistemas de denuncia de irregularidades; y
- la cooperación entre las autoridades competentes de los Estados miembros y la Autoridad Europea de Valores y Mercados (ESMA).

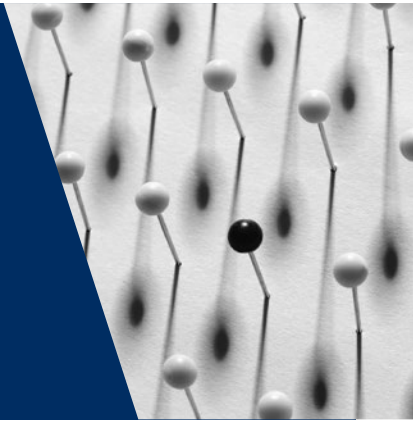
También existen otras cuestiones de estos ámbitos que se abordan de forma específica, como la recopilación de datos sobre la situación financiera de los interesados ([973]) o el pago transfronterizo mediante transferencias bancarias, las cuales acarrean inevitablemente la circulación de datos personales ([974]).

([973]) Reglamento (CE) n.º 1060/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre las agencias de calificación crediticia, DO 2009 L 302, en su versión modificada más recientemente por la Directiva 2014/51/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, por la que se modifican las Directivas 2003/71/CE y 2009/138/CE y los Reglamentos (CE) n.º 1060/2009, (UE) n.º 1094/2010 y (UE) n.º 1095/2010 con respecto a las facultades de la Autoridad Europea de Supervisión (Autoridad Europea de Seguros y Pensiones de Jubilación) y la Autoridad Europea de Supervisión (Autoridad Europea de Valores y Mercados), DO 2014 L 153; Reglamento (UE) n.º 462/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, por el que se modifica el Reglamento (CE) n.º 1060/2009 sobre las agencias de calificación crediticia, DO 2013 L 146.

([974]) Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE, DO 2007 L 319, en su versión modificada por la Directiva 2009/111/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, por la que se modifican las Directivas 2006/48/CE, 2006/49/CE y 2007/64/CE en lo que respecta a los bancos afiliados a un organismo central, a determinados elementos de los fondos propios, a los grandes riesgos, al régimen de supervisión y a la gestión de crisis, DO 2009 L 302.

10

Retos modernos en la protección de los datos personales



La era digital —o la era de las tecnologías de la información— se caracteriza por el uso generalizado de ordenadores, internet y tecnologías digitales. Implica la recogida y el tratamiento de ingentes cantidades datos, incluidos los datos de carácter personal. La recogida y el tratamiento de datos personales en una economía globalizada implica que cada vez hay más flujos de datos transfronterizos. Este tratamiento puede aportar beneficios visibles y significativos a nuestra vida cotidiana: los motores de búsqueda facilitan el acceso a volúmenes considerables de información y conocimientos, las redes sociales permiten que personas de todo el mundo se comuniquen, expresen opiniones y movilicen apoyo a causas sociales, ambientales y políticas, mientras que las empresas y los consumidores se benefician de técnicas de marketing efectivas y eficientes que estimulan la economía. La tecnología y el tratamiento de datos personales son también herramientas indispensables para las autoridades estatales en su lucha contra la delincuencia y el terrorismo. Del mismo modo, los macrodatos —la recogida, conservación y análisis de grandes cantidades de información para detectar patrones y predecir comportamientos— «pueden ser fuente de gran valor para la sociedad y mejorar la productividad, el funcionamiento del sector público y la participación social» ([975]).

Pese a sus múltiples beneficios, la era digital también plantea problemas para la privacidad y la protección de datos, ya que se recogen y se tratan grandes cantidades de datos personales de maneras cada vez más complejas y opacas. El avance tecnológico ha dado lugar a la aparición de grandes conjuntos de datos que se pueden cotejar y analizar fácilmente en busca de patrones o para adoptar decisiones

([975]) Consejo de Europa, Comité consultivo de la Convención 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Estrasburgo, 23 de enero de 2017.

basadas en algoritmos, que permiten tener una visión sin precedentes del comportamiento humano y de la vida privada ([976]).

Las nuevas tecnologías tienen mucha fuerza y pueden ser muy peligrosas si caen en malas manos. Un ejemplo del gran impacto que pueden tener estas tecnologías sobre los derechos de las personas físicas es que las autoridades estatales puedan llevar a cabo actividades de vigilancia masiva haciendo uso de ellas. En 2013, las revelaciones de Edward Snowden sobre el funcionamiento de programas de vigilancia a gran escala de las comunicaciones telefónicas y a través de internet en algunos Estados generaron gran inquietud por los peligros que entrañan las actividades de vigilancia para la privacidad, la gobernanza democrática y la libertad de expresión. La vigilancia masiva y las tecnologías que permiten la conservación y el tratamiento globalizados de datos personales y el acceso a datos en bloque puede afectar a la propia esencia del derecho a la privacidad ([977]). Además, pueden tener efectos negativos sobre la cultura política y efectos alarmantes para la democracia, la creatividad y la innovación ([978]). El mero temor a que el Estado pueda estar constantemente vigilando y analizando el comportamiento y las acciones de los ciudadanos puede disuadir a estos de expresar su opinión sobre determinados asuntos y provocar recelos y cautelas ([979]). Estos problemas han llevado a algunas autoridades públicas, centros de investigación y organizaciones de la sociedad civil a analizar los efectos que pueden tener las nuevas tecnologías en la sociedad. En 2015, el Supervisor Europeo de Protección de Datos puso en marcha varias iniciativas para valorar cómo afectan los macrodatos y la internet de las cosas a la ética. En particular, ha creado un grupo consultivo externo que tiene por objeto estimular «un debate abierto y documentado sobre ética digital, que permita a la UE aprovechar los beneficios de la tecnología para la sociedad y la economía y, al mismo tiempo, refuerce los

([976]) Parlamento Europeo (2017), Resolución sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, P8_TA-PROV(2017)0076, Estrasburgo, 14 de marzo de 2017.

([977]) Véase Naciones Unidas, Asamblea General, *Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*, Ben Emmerson, A/69/397, 23 de septiembre de 2014, apartado 59. Véase también TEDH, *Factsheet on Mass surveillance*, julio de 2017.

([978]) SEPD (2015), *Hacer frente a los desafíos que se plantean en relación con los macrodatos*, Dictamen 7/2015, Bruselas, 19 de noviembre de 2015.

([979]) Véase en particular TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros* [GS], 8 de abril de 2014, apartado 37.

derechos y libertades de las personas, en su particular, sus derechos a la privacidad y a la protección de datos» ([980]).

El tratamiento de datos personales también es un potente instrumento en manos de las grandes empresas. Hoy en día, puede revelar información detallada sobre la salud o las finanzas de una persona, información que posteriormente es utilizada por las grandes empresas para tomar decisiones de importancia para las personas físicas, como la prima aplicada sobre su seguro de enfermedad o su solvencia. Las técnicas de tratamiento de datos también pueden afectar a los procesos democráticos, cuando son utilizadas por políticos o empresas para influir en las elecciones: por ejemplo, mediante la «microsegmentación» de las comunicaciones de los votantes. En otras palabras, mientras la privacidad se percibió en principio como un derecho para proteger a las personas físicas contra injerencias injustificadas por parte de las autoridades públicas, en la era moderna también puede verse amenazada por el poder de agentes privados. Esto genera dudas sobre el uso de las tecnologías y el análisis predictivo para tomar decisiones que afectan a la vida cotidiana de los ciudadanos y refuerza la necesidad de velar por que el tratamiento de datos personales respete los requisitos de los derechos fundamentales.

La protección de datos está intrínsecamente relacionada con el cambio tecnológico, social y político. Por tanto, sería imposible elaborar una lista exhaustiva de futuros desafíos. En este capítulo se analizan determinados aspectos relacionados con los macrodatos, las redes sociales de internet y el mercado único digital de la Unión Europea. No se trata de realizar una evaluación exhaustiva de estos ámbitos desde la perspectiva de la protección de datos, sino de poner de relieve la multitud de posibles interacciones entre actividades humanas nuevas o revisadas y la protección de datos.

([980]) SEPD, Decisión de 3 de diciembre de 2015 por la que se establece un grupo consultivo externo sobre las dimensiones éticas de la protección de datos («el Grupo Consultivo sobre Ética»), 3 de diciembre de 2015, considerando 5.

10.1. Los macrodatos, los algoritmos y la inteligencia artificial

Puntos clave

- Las revolucionarias innovaciones que tienen lugar en el ámbito de las TIC están creando una nueva forma de vida, donde las relaciones sociales y los servicios empresariales, privados y públicos están interconectados digitalmente, con lo que se generan cantidades de datos cada vez más grandes, muchos de los cuales son datos personales.
- Los gobiernos, las empresas y los ciudadanos operan en una economía cada vez más dependiente de los datos, donde los propios datos se han convertido en valiosos activos.
- El concepto de macrodatos se refiere tanto a los datos como a su analítica.
- Los datos personales tratados aplicando la analítica de macrodatos están regulados por la legislación de la UE y del CdE.
- Las excepciones a las normas y los derechos de protección de datos se limitan a derechos concretos y situaciones específicas en las que resultaría imposible hacer respetar un derecho o sería necesario un esfuerzo desproporcionado por parte de los responsables del tratamiento.
- En general está prohibido adoptar decisiones de forma totalmente automatizada, salvo en casos concretos.
- El conocimiento y el control por parte de las personas físicas son claves para garantizar el respeto de sus derechos.

En este mundo cada vez más digitalizado, cada actividad deja una traza digital que se puede recopilar, tratar y evaluar o analizar. Con las nuevas tecnologías de la información y la comunicación, cada vez se recogen y se registran más y más datos ([981]). Hasta hace poco tiempo, no había ninguna tecnología capaz de analizar o evaluar el ingente volumen de datos o extraer conclusiones útiles. Los datos eran simplemente demasiado numerosos para ser evaluados, demasiado complejos, deficientemente estructurados y evolucionaban con excesiva rapidez como para determinar tendencias y hábitos.

([981]) Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Hacia una economía de los datos próspera, COM (2014) 442 final, Bruselas, 2 de julio de 2014.

10.1.1. Definición de macrodatos, algoritmos e inteligencia artificial

Macrodatos

El término «macrodatos» (del inglés, *big data*) está de moda y puede referirse a varios conceptos, según el contexto. Habitualmente comprende «la creciente capacidad tecnológica para recoger, tratar y extraer nuevos conocimientos, de carácter predictivo, de datos de gran volumen, velocidad y variedad» ([982]). Por tanto, el concepto de macrodatos se refiere tanto a los propios datos como a su análisis.

Las **fuentes** de los datos son de varios tipos e incluyen a las personas y sus datos personales, máquinas o sensores, información meteorológica, imágenes obtenidas por satélite, fotos y vídeos digitales o señales de GPS. Sin embargo, buena parte de los datos son de carácter personal: cualquier cosa, desde un nombre, una foto, una dirección de correo electrónico, datos bancarios, datos de rastreo de GPS, publicaciones en sitios web de redes sociales, información médica o la dirección IP de un ordenador ([983]).

Por macrodatos también se entiende el **tratamiento**, análisis y evaluación de los volúmenes de datos y la información disponible, con el fin de obtener información útil para los fines del análisis de macrodatos. Esto significa que los datos recogidos pueden utilizarse con fines distintos de los previstos en un principio, p. ej. para obtener tendencias estadísticas o desarrollar servicios más adaptados, como la publicidad. De hecho, en los casos en que sí existen tecnologías capaces de recoger, tratar y evaluar macrodatos, es posible combinar y reevaluar cualquier tipo de información: transacciones financieras, solvencia, tratamiento médico, consumo privado, actividad profesional, rastreo e itinerarios utilizados, uso de internet, tarjetas electrónicas y *smartphones*, videovigilancia o seguimiento de las comunicaciones. El análisis de los macrodatos representa una nueva dimensión cuantitativa de los

([982]) Consejo de Europea, Comité consultivo del Convenio 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, 23 de enero de 2017, p. 2; Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Hacia una economía de los datos próspera, COM(2014) 442 final, Bruselas, 2 de julio de 2014, p. 4; Unión Internacional de Telecomunicaciones (2015), Recomendación Y.3600, «Big data - Requisitos y capacidades basados en la computación en la nube».

([983]) Hoja informativa de la Comisión Europea sobre la reforma de la protección de datos de la UE y los macrodatos; Consejo de Europa, Comité consultivo del Convenio 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, 23 de enero de 2017, p. 2.

datos, que se puede evaluar y utilizar en tiempo real, por ejemplo, para prestar servicios adaptados a los consumidores.

Algoritmos e inteligencia artificial

La inteligencia artificial (IA) se refiere a la inteligencia de las máquinas que actúan como «agentes inteligentes». Como agentes inteligentes, algunos dispositivos, con ayuda de programas informáticos, pueden percibir su entorno y actuar en función de unos algoritmos. El término IA se aplica cuando una máquina imita funciones «cognitivas» —como el aprendizaje y la solución de problemas— que normalmente se asociarían al ser humano ([984]). Para imitar la toma de decisiones, las modernas tecnologías y software utilizan algoritmos que son utilizados por los dispositivos para tomar «decisiones automatizadas». La mejor forma de describir un algoritmo es que se trata de un procedimiento paso a paso para realizar cálculos, tratamientos de datos, evaluaciones y razonamientos y decisiones automatizados.

Del mismo modo que la analítica de los macrodatos, la IA —y las decisiones automatizadas que produce— requiere la recopilación y el tratamiento de grandes cantidades de datos. Estos datos pueden obtenerse del propio dispositivo (calor de los frenos, combustible, etc.) o del entorno que lo rodea. La elaboración de perfiles, por ejemplo, es un proceso que puede basarse en la toma de decisiones automatizadas en función de patrones o factores predeterminados.

Ejemplo: Elaboración de perfiles y publicidad dirigida

La elaboración de perfiles basados en los macrodatos implica buscar patrones que reflejen «características de un tipo de personalidad»; por ejemplo, cuando las empresas de comercio electrónico proponen productos que «también te pueden interesar» basándose en información recopilada de los productos que un cliente ha incluido anteriormente en una cesta de compra. A mayor cantidad de datos, más claro será el mosaico. El *smartphone*, por ejemplo, es un potente cuestionario que las personas físicas cumplimentan con cada uso, de forma consciente o inconsciente.

([984]) Stuart Russel y Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, pp. 27, 32-58, 968-972; Stuart Russel y Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, p. 2.

La psicografía moderna —la ciencia del estudio de la personalidad— utiliza el método OCEAN, en virtud del cual determina el tipo de carácter del usuario. Las «Cinco Grandes» dimensiones del carácter tienen que ver con la Apertura (lo abierta que es la persona a la novedad), la Meticulosidad (lo perfeccionista que es la persona), la Extroversión (lo sociable que es la persona), la Simpatía (lo agradable que es la persona en el trato) y la Neurosis (lo vulnerable que es la persona). Esta información crea un perfil de la persona en cuestión, de sus necesidades y temores, de cómo se va a comportar, etc. Se complementa con otra información acerca de la persona, obtenida de cualquier fuente disponible, de intermediarios de datos, redes sociales (incluidos los «me gusta» en publicaciones y fotos), de la música que escucha por internet, o de datos de GPS y rastreo.

El volumen de perfiles que se crean por medio de las técnicas de análisis de macrodatos se compara después para identificar patrones similares y construir grupos de personalidades. De este modo, se invierte la información acerca de las conductas y actitudes de determinadas personalidades. Con el acceso y uso de los macrodatos, se le da la vuelta al test de personalidad, de modo que ahora se utiliza la información sobre conductas y actitudes para describir la personalidad de la persona. Combinando la información sobre sus «me gusta» en las redes sociales, sus datos de rastreo, la música que escucha o las películas que ve, se puede obtener una imagen clara de la personalidad de una persona, de modo que las empresas pueden comunicar publicidad o información adaptada en función de la «personalidad» de esa persona. Sobre todo, esta información se puede tratar en tiempo real ([985]).

10.1.2. Cómo equilibrar los beneficios y los riesgos de los macrodatos

Con las modernas técnicas de tratamiento se pueden manejar grandes volúmenes de datos, importar otros nuevos rápidamente, tratar la información en tiempo real —es decir, con un corto tiempo de respuesta (incluso en el caso de solicitudes complejas)—, contemplar la posibilidad de realizar múltiples solicitudes simultáneas y analizar diferentes tipos de información (fotos, textos o números). Estas

([985]) Las técnicas de tratamiento y los nuevos programas informáticos disponibles evalúan la información sobre lo que le gusta a una persona, lo que mira cuando compra en línea o lo que añade a un carro de compra en línea en tiempo real y pueden proponer «productos» que puedan ser de interés para ella en virtud de la información recogida.

innovaciones tecnológicas permiten estructurar, tratar y evaluar volúmenes de datos e información en tiempo real ([986]). Al incrementar exponencialmente las cantidades de datos disponibles y analizados, se pueden conseguir ahora resultados que serían imposibles en un análisis a menor escala. Los macrodatos han ayudado a desarrollar un nuevo campo de negocio, en el que pueden surgir nuevos servicios para empresas y consumidores por igual. El valor de los datos personales de los ciudadanos de la UE tiene un potencial de crecimiento de hasta casi un billón de euros anuales hasta 2020 ([987]). Por tanto, los macrodatos pueden ofrecer nuevas **oportunidades** derivadas de la evaluación de datos masivos para obtener nuevas perspectivas sociales, económicas o científicas que puedan beneficiar a las personas físicas, a las empresas y a los gobiernos ([988]).

La analítica de los macrodatos puede revelar patrones entre diferentes fuentes y conjuntos de datos, y habilitar perspectivas útiles en campos como la ciencia y la medicina. Así ocurre, por ejemplo, en campos como la salud, la seguridad del suministro de alimentos, los sistemas de transporte inteligentes, la eficiencia energética o la ordenación urbana. Este análisis en tiempo real de la información puede utilizarse para mejorar los sistemas establecidos. En la investigación, se puede obtener nueva información combinando grandes cantidades de datos y evaluaciones estadísticas, sobre todo en disciplinas en las que, hasta la fecha, muchos datos solo se han evaluado manualmente. Se pueden desarrollar nuevos tratamientos, adaptados a pacientes concretos a partir de comparaciones con el volumen de información disponible. Las empresas confían en que el análisis de los macrodatos les permitirá obtener una ventaja competitiva, generar ahorros potenciales y crear nuevos

([986]) El desarrollo de programas informáticos para el tratamiento de macrodatos todavía está en una fase inicial. No obstante, recientemente se han desarrollado programas analíticos, en especial para el análisis de datos masivos en tiempo real, relativos a las actividades de las personas físicas. La posibilidad de analizar y tratar macrodatos de manera estructurada ofrece nuevas maneras de elaborar perfiles y publicidad dirigida. Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Hacia una economía de los datos próspera, COM(2014) 442 final, Bruselas, 2 de julio de 2014; Hoja informativa de la Comisión Europea sobre la reforma de la protección de datos de la UE y los macrodatos; y Consejo de Europa, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, 23 de enero de 2017, p. 2.

([987]) Hoja informativa de la Comisión Europea sobre la reforma de la protección de datos de la UE y los macrodatos.

([988]) Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (2014), *Resolution on Big Data*; Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Hacia una economía de los datos próspera, COM(2014) 442 final, Bruselas, 2 de julio de 2014, p. 2; Hoja informativa de la Comisión Europea sobre la reforma de la protección de datos de la UE y los macrodatos; y Consejo de Europa, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, 23 de enero de 2017, p. 1.

ámbitos de negocio a través de un servicio individualizado y directo para el cliente. Los organismos gubernamentales confían en lograr mejoras en el ámbito de la justicia penal. La Estrategia de la Comisión para el Mercado Único Digital en Europa reconoce el potencial de las tecnologías y los servicios basados en datos y de los macrodatos para catalizar el crecimiento económico, la innovación y la digitalización en la UE ([989]).

Sin embargo, los macrodatos también entrañan **riesgos**, generalmente asociados con sus «tres V»: volumen, velocidad y variedad de los datos tratados. El volumen se refiere a la cantidad de datos tratados, la variedad al número y diversidad de tipos de datos y la velocidad a la rapidez del tratamiento de los datos. Cuando la analítica de macrodatos se aplica a grandes conjuntos de datos para extraer nuevos conocimientos de carácter predictivo para tomar decisiones que afectan a personas o grupos de personas físicas, surgen consideraciones específicas en materia de protección de datos ([990]). Los riesgos para la protección de datos y la privacidad que entrañan los macrodatos se han puesto de relieve en los dictámenes del SEPD y del Grupo de Trabajo del Artículo 29, en las resoluciones del Parlamento Europeo y en los documentos de políticas del Consejo de Europa ([991]).

Estos riesgos pueden incluir el tratamiento indebido de los macrodatos por las personas que tienen acceso al volumen de información mediante manipulación, discriminación u opresión de determinadas personas o grupos de personas en la sociedad ([992]). Cuando se recogen, tratan y evalúan grandes volúmenes de datos personales acerca del comportamiento individual, su explotación puede dar lugar a importantes violaciones de los derechos y libertades fundamentales que van más allá del derecho a la privacidad. Es imposible determinar exactamente hasta qué

([989]) Parlamento Europeo, Resolución de 14 de marzo de 2017 sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley [2016/2225(INI)].

([990]) Consejo de Europa, Comité consultivo del Convenio 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, 23 de enero de 2017, p. 2.

([991]) Véase, por ejemplo, EDPS (2015), *Hacer frente a los desafíos que se plantean en relación con los macrodatos*, Dictamen 7/2015, 19 de noviembre de 2015; SEPD (2016), *Aplicación coherente de los derechos fundamentales en la era de los macrodatos*, Dictamen 8/2016, 23 de septiembre de 2016; Parlamento Europeo (2016), Resolución sobre implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley , P8_TA(2017)0076, Estrasburgo, 14 de marzo de 2017; Consejo de Europa, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Estrasburgo, 23 de enero de 2017.

([992]) Conferencia Internacional de Comisionados de Protección de Datos y Privacidad (2014), Resolution on Big Data.

punto se pueden ver afectados los datos personales y la privacidad. El Parlamento Europeo ha observado la falta de una metodología para realizar una evaluación empírica del impacto total de los macrodatos, pero existen pruebas que indican que el análisis de los macrodatos puede tener un importante impacto horizontal tanto en el sector público como en el privado ([993]).

El Reglamento general de protección de datos incluye disposiciones relativas al derecho a no ser objeto de decisiones automatizadas, incluida la elaboración de perfiles ([994]). El problema de la privacidad surge cuando el ejercicio del derecho de oposición requiere intervención humana, lo cual permite a los interesados expresar su punto de vista e impugnar la decisión ([995]). Esto puede dar lugar a problemas para garantizar un nivel adecuado de protección de los datos personales, por ejemplo, cuando no sea posible la intervención humana o cuando los algoritmos sean demasiado complejos y la cantidad de datos manejados demasiado grande como para facilitar a las personas físicas justificaciones de determinadas decisiones o información previa para obtener su consentimiento. Un ejemplo de uso de la IA y de las decisiones automatizadas se encuentra en el reciente desarrollo de aplicaciones hipotecarias o en los procesos de selección de personal. Las solicitudes no se admiten o se rechazan por el hecho de que los solicitantes no cumplan determinados parámetros o factores.

10.1.3. Problemas relacionados con la protección de los datos

En términos de protección de datos, los principales problemas tienen que ver, por una parte, con el volumen y variedad de los datos personales tratados y, por otra, con el tratamiento y sus resultados. La introducción de complejos algoritmos y software para transformar datos masivos en un recurso para tomar decisiones afecta a personas físicas y grupos en particular, sobre todo en los casos de elaboración de perfiles o aplicación de etiquetas y, en última instancia, crea muchos problemas de protección de datos ([996]).

([993]) Parlamento Europeo, Resolución de 14 de marzo de 2017 sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley [2016/2225(INI)].

([994]) Reglamento general de protección de datos, artículo 22.

([995]) Ibíd., artículo 22, apartado 3.

([996]) Consejo de Europa, Comité consultivo del Convenio 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, 23 de enero de 2017, p. 2.

Identificación de los responsables y encargados del tratamiento y su responsabilidad

Los macrodatos y la IA suscitan varias cuestiones en relación con la identificación de los responsables y encargados del tratamiento y su responsabilidad: cuando se recogen y se procesan tantos datos, ¿quién es su propietario? Cuando los datos son tratados por máquinas y programas informáticos inteligentes, ¿quién es el encargado del tratamiento? ¿Cuáles son las responsabilidades exactas de cada agente que interviene en el tratamiento? ¿Y con qué fines pueden utilizarse los macrodatos?

La cuestión de la responsabilidad en el contexto de la IA adquirirá una complejidad aún mayor cuando un sistema de IA tome una decisión basada en el tratamiento de datos que él mismo haya desarrollado. El Reglamento general de protección de datos establece un marco jurídico para la responsabilidad del responsable y del encargado del tratamiento. El tratamiento ilícito de datos personales da lugar a responsabilidad por parte del responsable y del encargado del tratamiento ([997]). La inteligencia artificial y las decisiones automatizadas plantean dudas sobre quién será el responsable de las violaciones que afecten a la privacidad de los interesados cuando no se pueda atribuir con certeza la complejidad y cantidad de los datos tratados. Cuando la IA y los algoritmos se consideran productos, surgen problemas entre la responsabilidad personal, que está regulada por el Reglamento general de protección de datos, y la responsabilidad por el producto, que no lo está ([998]). Para ello harán falta normas sobre la responsabilidad que llenen los vacíos existentes entre la responsabilidad personal y la responsabilidad por el producto en el caso de la robótica y la IA, incluidas las decisiones automatizadas, por ejemplo ([999]).

Impacto sobre los principios de protección de datos

La naturaleza, el análisis y el uso de los macrodatos, según se ha explicado anteriormente, dificultan notablemente la aplicación de algunos de los principios fundamentales tradicionales de la legislación europea sobre protección de datos ([1000]). Estos

([997]) Reglamento general de protección de datos, artículos 77-79 y artículo 82.

([998]) Parlamento Europeo, *European Civil Law Rules in Robotics*, Dirección General de Políticas Internas de la Unión (octubre de 2016), p. 14.

([999]) Discurso de Roberto Viola en el seminario de medios sobre el Derecho europeo sobre robótica celebrado en el Parlamento Europeo. (DISCURSO 16.2.2017); Anuncio del Parlamento Europeo sobre la petición a la comisión de una propuesta sobre normas de responsabilidad civil aplicables a la robótica y a la IA.

([1000]) Consejo de Europa, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Estrasburgo, 23 de enero de 2017.

retos tienen que ver sobre todo con los principios de licitud, minimización de datos, limitación de la finalidad y transparencia.

El principio de minimización de datos requiere que los datos personales sean adecuados, pertinentes y limitados a lo que sea necesario para los fines de su tratamiento. Sin embargo, el modelo de negocio de los macrodatos puede ser la antítesis de la minimización de datos, ya que necesita un volumen de datos en constante aumento, a menudo para fines sin especificar.

Lo mismo cabe decir del principio de limitación de la finalidad, que establece que los datos deben ser tratados con fines especificados y no pueden destinarse a fines incompatibles con el fin inicial, a menos que el tratamiento tenga una razón jurídica, como por ejemplo el consentimiento del interesado (véase la sección 4.1.1).

Por último, los macrodatos también desafían el principio de exactitud de los datos, ya que las aplicaciones de macrodatos tienden a recopilar datos de diversas fuentes sin que exista la posibilidad de verificar o mantener la exactitud de los datos recogidos ([1001]).

Normas y derechos específicos

La norma general sigue siendo que los datos personales tratados por medio de la analítica de macrodatos están comprendidos en el ámbito de aplicación de la legislación sobre protección de datos. Sin embargo, el **Derecho de la UE y el del CdE** han introducido disposiciones o excepciones específicas para casos concretos en relación con el tratamiento de datos con algoritmos complejos.

En el Derecho del CdE, el Convenio 108 modernizado reconoce nuevos derechos al interesado que le permiten un control más efectivo de sus datos personales en la era del Big Data. Éste es el caso del artículo 9 (1) (a), (c) y (d) del Convenio 108 modernizado sobre el derecho a no estar sujeto a una decisión que le afecte de modo significativo basada únicamente en un tratamiento automatizado sin que su opinión sea tenida en cuenta, el derecho a obtener bajo petición conocimiento del razonamiento que subyace bajo el tratamiento automatizado cuando los resultados de dicho tratamiento le sean aplicables, así como el derecho a oponerse al citado tratamiento automatizado. Otras disposiciones del Convenio 108 modernizado, sobre todo en

([1001]) SEPD (2016), Aplicación coherente de los derechos fundamentales en la era de los macrodatos, Dictamen 8/2016, 23 de septiembre de 2016, p. 8.

materia de transparencia y obligaciones adicionales son elementos complementarios de los mecanismos de protección establecidos en dicho Convenio para responder a los retos de la era digital.

En el Derecho de la UE, aparte de los casos enumerados en el artículo 23 del RGPD, debe garantizarse la **transparencia** de todos los tratamientos de datos personales. Es especialmente importante en relación con los servicios de internet y otros tratamientos de datos complejos automatizados, como el uso de algoritmos para tomar decisiones. En este caso, las características de los sistemas de tratamiento de datos deben hacer posible que los interesados puedan entender realmente lo que está ocurriendo con sus datos. Para garantizar un tratamiento leal y transparente, el Reglamento general de protección de datos obliga al responsable a facilitar al interesado información significativa sobre la lógica aplicada a las decisiones automatizadas, incluida la elaboración de perfiles ([1002]). En su Recomendación sobre la protección y promoción del derecho a la libertad de expresión y el derecho a la vida privada con respecto a la neutralidad de la red, el Comité de Ministros del Consejo de Europa recomienda que los proveedores de servicios de internet «faciliten a los usuarios información clara, completa y pública con respecto a las prácticas de gestión del tráfico que puedan afectar al acceso de los usuarios y a la distribución de contenidos, aplicaciones o servicios» ([1003]). En todos los Estados miembros, las autoridades competentes deben preparar informes sobre prácticas de gestión del tráfico de internet de manera abierta y transparente, que deberán ponerse a disposición del público de forma gratuita ([1004]).

Los responsables del tratamiento deben **informar** a los interesados —tanto si ellos mismos han facilitado los datos como si no— no solo específicamente en relación con los datos recogidos y el tratamiento previsto (véase la sección 6.1.1), sino también, cuando proceda, sobre la existencia de procesos de decisión automatizados, de modo que dispongan de «información significativa sobre la lógica aplicada» ([1005]), los objetivos y las posibles consecuencias de tales procesos. El Reglamento general de protección de datos también aclara (solo en los casos en que los datos personales no se hayan obtenido del propio interesado) que el responsable del tratamiento no está

([1002]) Reglamento general de protección de datos, artículo 13, apartado 2, letra f).

([1003]) Consejo de Europa, Comité de Ministros (2016), Recommendation CM/Rec(2016)1 of the Committee of Ministers to the Member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, 13 de enero de 2016, apartado 5.1.

([1004]) Ibíd., apartado 5.2.

([1005]) Reglamento general de protección de datos, artículo 13, apartado 2, letra f) y artículo 14, apartado 2, letra g).

obligado a facilitar al interesado esta información cuando «la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado» ([1006]). Sin embargo, tal como pone de relieve el Grupo de Trabajo del Artículo 29 en sus *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, la complejidad del tratamiento no debe impedir que el formulario del responsable del tratamiento facilite al interesado explicaciones claras sobre los objetivos del tratamiento y la analítica utilizada en el mismo ([1007]).

No existe una exención similar a los derechos del interesado de **acceso**, **rectificación** y **supresión** de sus datos personales, ni de su derecho a **limitar** el tratamiento. Sin embargo, la obligación del responsable del tratamiento de notificar al interesado cualquier rectificación o supresión de sus datos personales (véase la sección 6.1.4) también se puede levantar cuando dicha notificación «sea imposible o exija un esfuerzo desproporcionado» ([1008]).

Los interesados también tienen derecho a **oponerse**, en virtud del artículo 21 del RGPD (véase la sección 6.1.6), a cualquier tratamiento de sus datos personales, también en los casos de análisis de macrodatos. Aunque los responsables del tratamiento pueden quedar exentos de esta obligación si son capaces de demostrar que existen motivos legítimos imperiosos, esta exención no es aplicable al tratamiento con fines de mercadotecnia directa.

Los responsables del tratamiento también pueden acogerse a excepciones específicas cuando se traten datos personales con fines de archivo en interés público, con fines de investigación científica o histórica o con fines estadísticos ([1009]).

En relación con **la elaboración de perfiles y las decisiones automatizadas**, el RGPD ha introducido disposiciones específicas: El artículo 22, apartado 1, estipula que el interesado «tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él». Tal como se subraya en las directrices del Grupo de Trabajo del Artículo 29, este artículo impone una prohibición general a las decisiones totalmente

([1006]) Ibíd., artículo 14, apartado 5, letra b).

([1007]) Grupo de Trabajo del Artículo 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 de octubre de 2017, p. 14.

([1008]) Reglamento general de protección de datos, artículo 19.

([1009]) Ibíd., artículo 89, apartados 2 y 3.

automatizadas ([1010]). Los responsables del tratamiento solo pueden quedar exentos de esta prohibición en tres casos concretos, cuando la decisión: 1) sea necesaria para el cumplimiento de un contrato entre el interesado y el responsable; 2) esté permitida por una ley de ámbito nacional o de la UE, o 3) esté basada en el consentimiento explícito ([1011]).

Control por parte del interesado

La complejidad y la falta de transparencia de la analítica de macrodatos puede obligar a reconsiderar los conceptos del control de los datos personales por parte del interesado. Esto debe adaptarse al contexto social y tecnológico concreto, teniendo en cuenta la falta de conocimiento por parte de las personas físicas. Por tanto, la protección de datos en relación con los macrodatos debe basarse en un concepto más general de control sobre el uso de los datos, conforme al cual se produzca una evolución del control por el interesado hacia un proceso más complejo de múltiples evaluaciones de impacto de los riesgos relacionados con el uso de los datos ([1012]).

La calidad de una aplicación de macrodatos dependerá de la medida en que sea capaz de predecir los deseos o comportamientos de los sujetos de las pruebas (o consumidores). Los actuales modelos predictivos basados en análisis de macrodatos están sujetos a un perfeccionamiento constante. Los últimos avances no solo incluyen el uso de los datos para clasificar personalidades (es decir, conductas y actitudes), sino también el análisis del comportamiento a través del análisis de patrones de voz y la intensidad con la que se escriben los mensajes o la temperatura corporal. Toda esta información puede utilizarse en tiempo real y, por ejemplo, compararla con el conocimiento obtenido de las evaluaciones de macrodatos para valorar la solvencia durante una reunión con el representante de un banco, por ejemplo. La evaluación no se basa en los méritos de la persona que solicita el crédito, sino más bien en las características conductuales determinadas a partir del análisis y evaluación de macrodatos, es decir, si el candidato habla con voz firme o halagadora y su lenguaje o temperatura corporal.

([1010]) Grupo de Trabajo del Artículo 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 de octubre de 2017, p. 9.

([1011]) Reglamento general de protección de datos, artículo 22, apartado 2.

([1012]) Consejo de Europa, Comité consultivo del Convenio 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, T-PD(2017)01, Estrasburgo, 23 de enero de 2017.

La elaboración de perfiles y la publicidad dirigida no tienen por qué constituir necesariamente un problema si las personas son **conscientes** de que reciben anuncios adaptados. La elaboración de perfiles se convierte en un problema cuando se utiliza para manipular a las personas, es decir, para buscar determinadas personalidades o grupos de personas para hacer campaña política. Por ejemplo, es posible dirigirse a grupos de votantes indecisos con mensajes políticos adaptados a su «personalidad» o sus actitudes. Otro problema podría ser que se utilicen dichos perfiles para denegar a determinadas personas el acceso a bienes y servicios. Una garantía que puede servir de protección contra el abuso de los macrodatos y la información personal es la seudonimización (véase la sección 2.1.1) ([1013]). Los casos en que los datos personales están verdaderamente anonimizados, es decir, cuando no hay información que deje rastros que la relacionen con el interesado, quedan fuera del ámbito de aplicación del Reglamento general de protección de datos. El consentimiento de los interesados y las personas físicas en el tratamiento de macrodatos también plantea un reto para la legislación sobre protección de datos. Esto comprende el consentimiento a ser objeto de anuncios adaptados y de la elaboración de perfiles, que pueden justificarse por razones de «experiencia del cliente», y el consentimiento al uso de grandes volúmenes de datos personales para perfeccionar y desarrollar herramientas analíticas basadas en la información. El conocimiento o desconocimiento del tratamiento de macrodatos genera varias dudas en relación con los medios de que disponen los interesados para ejercer sus derechos, dado que el tratamiento de macrodatos puede basarse en datos seudonimizados y anonimizados sujetos a algoritmos. Aunque los datos seudonimizados están comprendidos en el ámbito de aplicación del Reglamento general de protección de datos, este Reglamento no se aplica a los datos anonimizados. El control y el conocimiento por parte del interesado de sus datos personales es crucial en la analítica de macrodatos: sin estos elementos, no tendrá una idea clara de quién es el responsable o encargado del tratamiento y no podrá ejercer sus derechos de manera efectiva.

([1013]) Ibíd., p. 2.

10.2. La web 2.0 y 3.0: las redes sociales y la internet de las cosas

Puntos clave

- Los servicios de redes sociales (SRS) son plataformas de comunicación en línea que permiten a las personas crear redes de usuarios que comparten intereses comunes.
- La internet de las cosas es la conexión de los objetos a internet y la interconexión de los propios objetos entre ellos.
- El consentimiento de los interesados es la base jurídica más frecuente para que el tratamiento de datos que realizan los responsables en las redes sociales sea lícito.
- Los usuarios de las redes sociales gozan de una protección general por la «exención doméstica», si bien esta excepción puede levantarse en determinados contextos.
- Los proveedores de redes sociales no están protegidos por la «exención doméstica».
- La privacidad desde el diseño y por defecto son cruciales para garantizar la seguridad de los datos en este campo.

10.2.1. Definición de la web 2.0 y 3.0

Servicios de redes sociales

En principio, internet se concibió como una red para interconectar ordenadores y transmitir mensajes con capacidades limitadas para intercambiar datos, donde los sitios web simplemente ofrecían a las personas la posibilidad de ver sus contenidos de forma pasiva ([1014]). En la era de la web 2.0, internet se transformó en un foro que permite a los usuarios interactuar, colaborar y generar datos. Esta era se caracteriza por el notable éxito y uso generalizado de los servicios de redes sociales, que ahora forman parte esencial de la vida diaria de millones de personas.

Los servicios de redes sociales (SRS) —conocidos simplemente como «redes sociales»— pueden definirse con carácter general como «plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten

([1014]) Comisión Europea (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

intereses comunes» ([1015]). Para unirse o crear una red, se solicita a los usuarios que faciliten datos personales y creen su perfil. Los SNS permiten a los usuarios generar «contenidos» digitales, que van desde fotografías y vídeos hasta enlaces a periódicos y publicaciones personales para expresar sus opiniones. A través de estas plataformas de comunicación en línea, los usuarios pueden interactuar y comunicarse con otros usuarios. Es muy importante el hecho de que la mayoría de las redes sociales más populares no requieran el pago de tasas de registro. En lugar de obligar a los usuarios a pagar por utilizar la red, los proveedores de SRS obtienen la mayor parte de sus ingresos de la publicidad dirigida. Los anunciantes pueden beneficiarse en gran medida de la información personal que se revela diariamente en estos sitios. Conocer la edad, el sexo, la localización y los intereses de un usuario permite que sus anuncios lleguen a las personas «adecuadas».

El Consejo de Ministros del CdE ha adoptado una recomendación sobre la protección de los derechos humanos en relación a los servicios de redes sociales ([1016]) que trata en una sección específica sobre protección de datos y que ha sido complementado en 2018 con otra recomendación sobre el papel y responsabilidades de los intermediarios de internet ([1017]).

Ejemplo: Nora está muy contenta porque su pareja le ha propuesto matrimonio. Quiere compartir la buena noticia con sus amigos y familiares y decide escribir una emotiva publicación en una red social expresando su alegría y cambia el estado de su relación a «comprometida». En los días posteriores, cuando inicia sesión en su cuenta, Nora ve anuncios sobre vestidos de boda y floristerías. ¿Por qué?

Cuando crean un anuncio en Facebook, las empresas que venden vestidos de boda y las floristerías seleccionan determinados parámetros para poder llegar a personas como Nora. Cuando el perfil de Nora indica que es una mujer, que está comprometida y que vive en París cerca del barrio donde se encuentran las tiendas de vestidos y floristerías, inmediatamente ve estos anuncios.

([1015]) Grupo de Trabajo del Artículo 29 (2009), *Dictamen 5/2009 sobre las redes sociales en línea*, WP 163, Bruselas, 12 de junio de 2009, p. 4.

([1016]) Consejo de ministros del CdE, recomendación CM/Rec(2012)4, de 4 de abril de 2012.

([1017]) Consejo de ministros del CdE, recomendación CM/Rec(2018)2, de 7 de marzo de 2018.

La internet de las cosas

La internet de las cosas (IdC) representa el siguiente paso en el desarrollo de internet: la era de la web 3.0. Con la IdC, se pueden interconectar dispositivos a través de internet para que interactúen entre ellos. De este modo, los objetos y las personas pueden interconectarse a través de las redes de comunicaciones y facilitar información sobre su estado o sobre el estado de su entorno ([1018]). La IdC y los dispositivos conectados son ya una realidad y cabe esperar que aumenten sustancialmente en los próximos años con el desarrollo adicional de dispositivos inteligentes que permitirán crear ciudades inteligentes, hogares inteligentes y empresas inteligentes.

Ejemplo: La IdC puede ser especialmente beneficiosa para la atención sanitaria. Las empresas ya han creado dispositivos, sensores y aplicaciones que permiten llevar a cabo el seguimiento de la salud de un paciente. Gracias a un botón de alarma que se puede llevar encima y otros sensores inalámbricos instalados en distintos puntos del hogar, es posible observar la rutina diaria de las personas ancianas que viven solas y generar alertas si se detectan alteraciones importantes en su actividad cotidiana. Los sensores de detección de caídas, por ejemplo, son muy utilizados por las personas mayores. Estos sensores pueden detectar caídas con precisión y advertir al médico o a la familia de la persona afectada.

Ejemplo: Barcelona es uno de los ejemplos más conocidos de ciudad inteligente. Desde 2012, el Ayuntamiento ha implantado tecnologías innovadoras destinadas a crear un sistema inteligente de tránsito público, gestión de residuos, estacionamientos y alumbrado urbano. Por ejemplo, para mejorar la gestión de los residuos, la ciudad utiliza contenedores inteligentes que permiten controlar los niveles de residuos para optimizar los itinerarios de recogida. Cuando los contenedores están casi llenos, transmiten señales a través de la red de comunicaciones móviles a la aplicación informática utilizada por la empresa responsable de la gestión de residuos. De este modo, la empresa puede planificar el mejor itinerario de recogida, establecer prioridades u ordenar que se recojan únicamente los contenedores que efectivamente necesitan vaciarse.

([1018]) Comisión Europea, documento de trabajo de los servicios de la Comisión, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19 de abril de 2016.

10.2.2. Cómo equilibrar los beneficios y los riesgos de los macrodatos

La enorme expansión y éxito de los SRS en el último decenio indica que tienen **importantes beneficios**. Por ejemplo, la publicidad dirigida (descrita en el ejemplo resaltado) es una forma especialmente innovadora de que las empresas lleguen a su audiencia y les ofrece un mercado más específico. También puede que interese a los consumidores que les presenten anuncios que les resulten más pertinentes e interesantes. Lo más importante, sin embargo, es que las redes sociales pueden tener efectos positivos en la sociedad y en la realización de cambios. Permiten a los usuarios comunicarse, interactuar, organizar grupos y eventos sobre cuestiones que les afectan.

Del mismo modo, cabe esperar que la IdC aporte importantes beneficios a la economía y forme parte de la estrategia de la UE para desarrollar un mercado único digital. Se calcula que, en la UE, el número de conexiones IdC llegará a ser de hasta 6 000 millones en 2020. Cabe prever que esta expansión de la conectividad reporte importantes beneficios económicos mediante el desarrollo de innovadores servicios y aplicaciones, una mejor atención sanitaria, un mejor conocimiento de las necesidades de los consumidores y una mayor eficiencia.

Al mismo tiempo, dada la ingente cantidad de datos personales que generan los usuarios de las redes sociales y que posteriormente son tratados por los operadores de los servicios, la expansión de los SRS lleva aparejada una **creciente inquietud** por la protección de la privacidad y los datos personales. Los SNS pueden amenazar el derecho a la vida privada y el derecho a la libertad de expresión. Este tipo de amenazas pueden ser: «falta de garantías legales y procesales en procesos que puedan dar lugar a la exclusión de usuarios; protección inadecuada de niños y jóvenes contra contenidos o comportamientos nocivos; falta de respeto por los derechos de los demás; falta de ajustes predeterminados que protejan la privacidad; falta de transparencia sobre los fines de la recogida y tratamiento de los datos personales» ([1019]). La legislación europea sobre protección de datos ha intentado responder a los problemas que generan las redes sociales en relación con la privacidad y la protección de datos. Principios como el consentimiento, la protección de la privacidad y los datos desde el diseño y por defecto, así como los derechos de los interesados, son

([1019]) Consejo de Europa, Recommendation Rec(2012)4 to Member States on the protection of human rights with regard to social networking services, 4 de abril de 2012.

especialmente importantes en el contexto de las redes sociales y los servicios que proporcionan.

En el contexto de la IdC, el inmenso volumen de datos personales generados por los distintos dispositivos interconectados también entraña riesgos para la privacidad y la protección de datos. Aunque la transparencia es un principio importante de la legislación europea sobre protección de datos, debido a la multitud de dispositivos conectados no siempre está claro quién puede recoger, acceder y utilizar los datos recogidos por dispositivos IdC ([1020]). Sin embargo, de acuerdo con el Derecho de la UE y del CdE, el principio de transparencia establece la obligación de que los responsables del tratamiento mantengan a los interesados informados acerca del uso de sus datos, en un lenguaje claro y sencillo. Los riesgos, normas, garantías y derechos al respecto del tratamiento de sus datos personales deben quedar claros para todas las personas afectadas. Los dispositivos conectados por la IdC y la multiplicidad de operaciones de tratamiento y datos que conllevan también podrían plantear dificultades desde el punto de vista del requisito del consentimiento claro e informado al tratamiento de datos, cuando dicho tratamiento esté basado en contenidos. Las personas físicas suelen desconocer el funcionamiento técnico de este tipo de tratamiento y, por tanto, las consecuencias de su consentimiento.

Otra importante preocupación es la seguridad, dato que los dispositivos conectados son especialmente vulnerables a riesgos de este tipo. Los dispositivos conectados tienen distintos niveles de seguridad. Dado que operan más allá de la infraestructura informática estándar, puede que carezcan de la capacidad adecuada de tratamiento y conservación para alojar programas informáticos de seguridad o emplear técnicas como el cifrado, la seudonimización o la anonimización para proteger los datos personales de los usuarios.

Ejemplo: En Alemania, los organismos reguladores decidieron prohibir un juguete conectado a internet debido a la gran inquietud generada por la repercusión que pudiera tener el juguete sobre el respeto de la vida privada de los niños. Los reguladores consideraron que una muñeca conectada a internet llamada Cayla constituía en la práctica un dispositivo espía oculto. La muñeca funcionaba enviando el audio de las preguntas del menor que jugaba con ella a una aplicación instalada en un dispositivo digital, que traducía ese audio a texto y buscaba la respuesta en internet. A continuación,

([1020]) Supervisor Europeo de Protección de Datos (2017), *Understanding the Internet of Things*.

la aplicación enviaba una respuesta a la muñeca, que la decía en voz alta. Por medio de esta muñeca, las comunicaciones del menor, así como las de los adultos cercanos, podían ser grabadas y transmitidas a la aplicación. Si los fabricantes de la muñeca no hubieran adoptado medidas de seguridad adecuadas, la muñeca podría haber sido utilizada por cualquiera para escuchar conversaciones.

10.2.3. Problemas relacionados con la protección de los datos

Consentimiento

En Europa, el tratamiento de datos personales solo es lícito si está permitido por la legislación europea sobre protección de datos. Para los proveedores de SRS, el consentimiento de los interesados constituye, en general, una base lícita para el tratamiento de los datos. El consentimiento debe ser una manifestación de voluntad libre, específica, informada e inequívoca (véase la sección 4.1.1) ([1021]). «Manifestación de voluntad libre» significa, en esencia, que los interesados deben tener la capacidad de realizar una elección auténtica. El consentimiento es «específico» e «informado» cuando es inteligible y se refiere de forma clara y precisa a todo el ámbito de aplicación, fines y consecuencias del tratamiento de datos. En el contexto de las redes sociales, cabe poner en cuestión si el consentimiento es libre, específico e informado para todos los tipos de tratamiento realizados por el operador del SRS y por terceros.

Ejemplo: Para integrarse en un SRS, a menudo los usuarios deben aceptar distintos tipos de tratamiento de sus datos personales, sin que se les proporcionen las necesarias especificaciones u opciones alternativas. Un ejemplo sería la necesidad de consentir en recibir publicidad conductual para registrarse en un SNS. Como señala el Grupo de Trabajo del Artículo 29 en su Dictamen sobre la definición de consentimiento, «Considerando la importancia que han adquirido algunas redes sociales, ciertas categorías de usuarios (como los adolescentes) aceptarán la recepción de publicidad comportamental para evitar el riesgo de ser parcialmente excluidos de las

([1021]) Reglamento general de protección de datos, artículos 4 y 7; Convenio 108 modernizado, artículo 5.

interacciones sociales. El usuario debería estar en condiciones de dar su consentimiento libre y específico para recibir la publicidad comportamental, independientemente de su acceso al servicio de la red social» ([1022]).

De acuerdo con el Reglamento general de protección de datos, los datos personales de los niños menores de dieciséis años no pueden, en principio, someterse a tratamiento con base en su consentimiento ([1023]). Si para el tratamiento es necesario el consentimiento, deberá ser otorgado por el titular de la patria potestad o tutela sobre el niño. Los niños merecen protección específica debido al hecho de que puede que sean menos conscientes de los riesgos y consecuencias que conlleva el tratamiento de sus datos. Esto es muy importante en el contexto de las redes sociales, ya que los niños son más vulnerables a algunos de los efectos negativos que puede tener el uso de dichas redes, como el ciberacoso o el robo de identidad.

La seguridad y la protección de la privacidad y los datos desde el diseño y por defecto

El tratamiento de datos personales conlleva riesgos intrínsecos para la seguridad, dada la constante posibilidad de que se produzca una violación de la seguridad que dé lugar, de forma accidental o ilícita, a la destrucción, pérdida, alteración, acceso no autorizado o revelación de los datos personales tratados. De acuerdo con la legislación europea sobre protección de datos, los responsables y encargados del tratamiento están obligados a aplicar las medidas técnicas y organizativas oportunas para evitar cualquier injerencia no autorizada en las operaciones de tratamiento de datos. Los proveedores de servicios de redes sociales comprendidos en el ámbito de aplicación de la normativa europea de protección de datos también deben cumplir esta obligación.

Los principios de la protección de la privacidad y los datos desde el diseño y por defecto obligan a los responsables a mantener la seguridad en el diseño de sus productos y a aplicar automáticamente una configuración adecuada de protección de la privacidad y los datos. Esto significa que, cuando una persona decide unirse a una red social, el proveedor del servicio no puede poner automáticamente toda la información acerca del nuevo usuario del servicio a disposición de todos sus usuarios. Al

([1022]) Grupo de Trabajo del Artículo 29 (2011), *Dictamen 15/2011 sobre la definición del consentimiento*, WP 187, 13 de julio de 2011, p. 18.

([1023]) Véase el Reglamento general de protección de datos, artículo 8. Los Estados miembros pueden establecer una edad menor por ley, siempre que no sea inferior a trece años.

unirse al servicio, la configuración por defecto de protección de la privacidad y los datos debe ser tal que la información solo esté a disposición de los contactos elegidos por el usuario. Solo debe ser posible ampliar el acceso a personas que no pertenezcan a esa lista cuando el usuario tome la decisión de modificar manualmente la configuración por defecto de protección de la privacidad y los datos. Esto también puede tener influencia en aquellos casos en que se produzca una violación de la seguridad a pesar de las medidas adoptadas. En esos casos, los proveedores de servicios deben avisar a los usuarios afectados cuando ello pueda entrañar un riesgo elevado para los derechos y libertades del interesado ([1024]).

La protección de la privacidad y los datos desde el diseño y por defecto es especialmente importante en el contexto de los SRS ya que, además de los riesgos de acceso no autorizado que conlleva la mayoría de tipos de tratamiento, el hecho de compartir información personal en las redes sociales entraña riesgos adicionales para la seguridad. A menudo estos riesgos tienen su origen en que el usuario no sabe *quién* puede acceder a su información y cómo pueden utilizarla esas personas. Con el uso generalizado de las redes sociales, ha aumentado el número de incidentes y víctimas de robo de identidad.

Ejemplo: El robo de identidad es un fenómeno por el que una persona obtiene información, datos o documentos pertenecientes a otra persona (la víctima) y utiliza esta información para hacerse pasar por la víctima con el fin de obtener bienes y servicios en nombre de esta última. Veamos por ejemplo el caso de Paul, que posee una cuenta en una red social. Paul es profesor y miembro activo de su comunidad, muy extrovertido y no especialmente preocupado por la configuración de protección de la privacidad y los datos de su cuenta en la red social. Tiene una lista muy amplia de contactos, que a veces incluye a personas a las que no conoce en persona necesariamente. Dado que trabaja en un colegio importante y ha adquirido cierta popularidad entrenando al equipo de fútbol, cree que lo más probable es que estas personas sean padres de alumnos o amigos del colegio. La dirección de correo electrónico y la fecha de cumpleaños están visibles en su red social. Además, Paul publica normalmente fotos de su perro Toby, que acompaña de frases como «Toby y yo en nuestro paseo matutino». Paul no se ha dado cuenta de que una de las preguntas de seguridad más frecuentes para proteger

([1024]) Ibíd., artículo 34.

su correo electrónico o su teléfono móvil es «cómo se llama tu mascota». Utilizando la información disponible en el perfil de Paul en la red social, Nick consigue piratear fácilmente las cuentas de Paul.

Derechos de las personas físicas

Los proveedores de SRS deben respetar los derechos de las personas físicas (véase la sección 6.1), incluido el derecho a ser información sobre la finalidad del tratamiento y cómo pueden utilizarse los datos personales con fines de mercadotecnia directa. Las personas también deben tener derecho de acceso a los datos personales que hayan generado en la plataforma de la red social y solicitar su supresión. Aunque las personas hayan consentido en el tratamiento de sus datos personales y subido información a la red, deben poder pedir que «sean olvidados» si ya no quieren recibir los servicios de la red social. El derecho a la portabilidad de los datos permite además a los usuarios recibir una copia de los datos personales que hayan facilitado al proveedor de servicios de la red social en un formato estructurado, de uso común y lectura mecánica y transferir sus datos de un proveedor de servicios de redes sociales a otro ([1025]).

Responsables del tratamiento

Una duda difícil de resolver que suele surgir en el contexto de las redes sociales es la cuestión de quién es el responsable del tratamiento, es decir, quién es la persona que tiene la obligación y la responsabilidad de cumplir las normas de protección de datos. Los proveedores de servicios de redes sociales tienen la consideración de responsables del tratamiento en virtud de la legislación europea sobre protección de datos. Esto es evidente porque la definición de «responsable» es muy amplia y porque estos proveedores de servicios determinan los fines y los medios del tratamiento de los datos personales compartidos por las personas físicas. En virtud del Derecho de la UE, si ofrecen servicios a los interesados en la UE, los responsables deben cumplir las disposiciones del Reglamento general de protección de datos, aunque no estén radicados en la Unión.

Sin embargo, ¿pueden también los usuarios de los servicios de redes sociales tener la consideración de responsables del tratamiento? Cuando las personas físicas tratan datos personales «en el curso de una actividad exclusivamente personal

([1025]) Reglamento general de protección de datos, artículo 20.

o doméstica», las normas de protección de datos no son de aplicación. Esto es conocido en la legislación europea sobre protección de datos como la «exención doméstica». No obstante, puede que, en algunos casos, un usuario de una red social no pueda acogerse a la exención doméstica.

Los usuarios comparten voluntariamente su información personal en internet. Sin embargo, la información así compartida suele incluir información personal de otras personas.

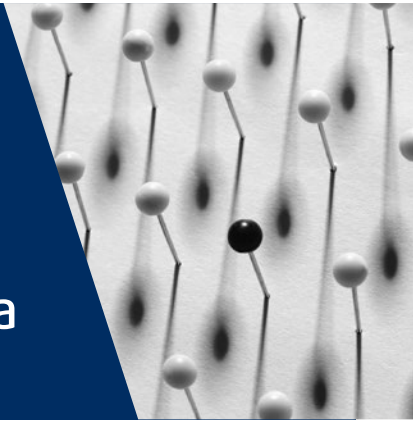
Ejemplo: Paul tiene una cuenta en una red social muy popular. Paul quiere ser actor y utiliza su cuenta para publicar fotos, vídeos y mensajes en los que explica su pasión por el arte. La popularidad es importante para su futuro; por tanto, ha decidido que su perfil no solo debe estar disponible para su lista de contactos conocidos, sino también para todos los usuarios de internet, sean miembros de la red o no. ¿Puede Paul publicar fotos y vídeos en los que aparece con su amiga Sarah sin contar con el consentimiento de ella? Como profesora de educación primaria, Sarah intenta mantener su vida privada al margen de su empleador, de sus alumnos y de los padres de estos. Imaginemos un caso en el que Sarah, que no utiliza las redes sociales, averigua por su amigo común Nick que se ha publicado en internet una foto de ella con Paul en una fiesta. En ese caso, el tratamiento de datos por parte de Paul no estará comprendido en el ámbito de aplicación de la legislación europea, ya que se acoge a la «exención doméstica».

Sin embargo, es crucial que los usuarios sean conscientes de que subir información de otras personas sin obtener su consentimiento puede violar los derechos a la privacidad y la protección de datos de esas personas. Aunque se aplique la exención doméstica —por ejemplo, si un usuario tiene un perfil que solo es público para la lista de contactos que ha seleccionado—, la publicación de información personal de otras personas puede hacer que incurra en responsabilidades. Aunque las normas de protección de datos no sean de aplicación debido a la exención doméstica, es posible que sí se apliquen otras normas nacionales, como las que regulan la difamación o la violación de la personalidad. Por último, solo los usuarios de los SRS están protegidos por la exención doméstica: los responsables y encargados que facilitan los medios para este tratamiento privado deben regirse por la legislación de la UE sobre protección de datos ([1026]).

([1026]) Ibíd., considerando 18.

Con la reforma de la Directiva sobre la privacidad y las comunicaciones electrónicas, las normas de protección de datos, privacidad y seguridad que se aplican a los proveedores de servicios de telecomunicaciones en el marco jurídico vigente también se aplicarán a las comunicaciones entre máquinas y a los servicios de comunicaciones electrónicas, incluidos, por ejemplo, los servicios de transmisión libre (OTT).

Bibliografía recomendada



Capítulo 1

Araceli Mangas, M. (ed.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Viena, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. «Four fundamental rights: finding the balance», *International Data Privacy Law*, Vol. 6, No. 3, pp. 195-209.

González Fuster, G. y Gellert, G. (2012), «The fundamental right of data protection in the European Union: in search of an uncharted right», *International Review of Law, Computers and Technology*, Vol. 26 (1), pp. 73-82.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. y Nouwt, S. (Eds.) (2009), *Reinventing Data Protection*, Springer.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), «EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation».

Kranenborg, H. (2015), «Google and the Right to be Forgotten», *European Data Protection Law Review*, Vol. 1, No. 1, pp. 70-79.

Lynskey, O. (2014), «Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order», *International and Comparative Law Quarterly*, Vol. 63, No. 3, pp. 569-597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Kokott, J. y Sobotta, C. (2013), «The distinction between privacy and data protection in the case law of the CJEU and the ECtHR», *International Data Privacy Law*, Vol. 3, No. 4, pp. 222-228.

EDRi, *An introduction to data protection*, Bruselas.

Frowein, J. y Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlín, N. P. Engel Verlag.

Grabenwarter, C. y Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Múnich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. y Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Múnich, C. H. Beck.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. y Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Amberes, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. y Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruselas, Emile Bruylant.

Simitis, S. (1997), «Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?», *Neue Juristische Wochenschrift*, No. 5, pp. 281-288.

Warren, S. y Brandeis, L. (1890), «The right to privacy», *Harvard Law Review,* Vol. 4, No. 5, pp. 193-220.

White, R. y Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Capítulo 2

Acquisty, A. y Gross R. (2009), «Predicting Social Security numbers from public data», *Proceedings of the National Academy of Science*, 7 de julio de 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. y Blondel V. D. (2013), «Unique in the Crowd: the Privacy Bounds of Human Mobility», *Nature Scientific Reports*, Vol. 3, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, París, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. y Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londres, Sweet & Maxwell.

Ohm, P. (2010), «Broken promises of privacy: Responding to the surprising failure of anonymization», *UCLA Law Review*, Vol. 57, No. 6, pp. 1701-1777.

Samarati, P. y Sweeney, L. (1998), «Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression», Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), «K-Anonymity: A Model for Protecting Privacy», *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, Vol. 10, No. 5, pp. 557-570.

Tinnefeld, M., Buchner, B. y Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Múnich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

Capítulos 3 a 6

Brühann, U. (2012), «Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr», en: Grabitz, E., Hilf, M. y Nettesheim, M. (eds.), *Das Recht der Europäischen Union*, Band IV, A. 30, Múnich, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cádiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrucken, Éditions universitaires européennes.

Curren, L. y Kaye, J. (2010), «Revoking consent: a 'blind spot' in data protection law?», *Computer Law & Security Review*, Vol. 26, No. 3 pp. 273-283.

Dammann, U. y Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. y Papakonstantinou, V. (2012), «The Police and Criminal Justice Data Protection Directive: Comment and Analysis», *Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1-5.

De Hert, P. y Papakonstantinou, V. (2012), «The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals», *Computer Law & Security Review*, Vol. 28, N º 2, pp. 130-142.

Feretti, Federico (2012), «A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after

the Lisbon treaty: Taking rights seriously», *European Review of Private Law*, Vol. 20, No. 2, pp. 473-506.

FRA (Agencia de los Derechos Fundamentales de la Unión Europea) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburgo, Oficina de Publicaciones de la Unión Europea (Oficina de Publicaciones).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Edición Conferencia), Viena, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburgo, Oficina de Publicaciones.

Irish Health Information and Quality Authority (2010), Guidance on Privacy Impact Assessment in Health and Social Care.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. y Saxby, S. (2011), «30 years on – The review of the Council of Europe Data Protection Convention 108», *Computer Law & Security Review*, Vol. 27, No 3, pp. 223-231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Capítulo 7

Supervisor Europeo de Protección de Datos (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. y Nouwt, S. (2009), *Reinventing data protection?*, Berlín, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

Grupo de Trabajo del Artículo 29 (2005), *Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995*.

Capítulo 8

Blasi Casagran, C. (2016), *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Londres, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlín, Springer.

Europol (2012), *Data Protection at Europol*, Luxemburgo, Oficina de Publicaciones.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, La Haya, Eurojust.

De Hert, P. y Papakonstantinou, V. (2012), «The Police and Criminal Justice Data Protection Directive: Comment and Analysis», *Computers & Law Magazine of SCL*, Vol. 22, No. 6, pp. 1-5.

Drewer, D. y Ellermann, J. (2012), «Europol's data protection framework as an asset in the fight against cybercrime», *ERA Forum*, Vol. 13, No. 3, pp. 381-395.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlín, Springer.

Gutwirth, S., Poullet, Y. y De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. y Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), «Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem», *European Law Review*, Vol. 36, No. 5, pp. 722-776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Capítulo 9

Büllesbach, A., Gijrath, S., Poullet, Y. y Hacon, R. (2010), *Concise European IT law*, Ámsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. y Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. y De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. y Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Konstadinides, T. (2011), «Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem», *European Law Review*, Vol. 36, No. 5, pp. 722-776.

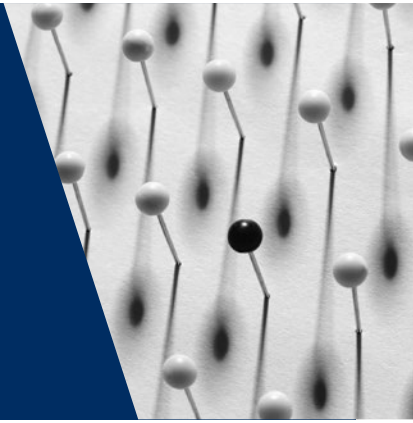
Rosemary, J. y Hamilton, A. (2012), *Data protection law and practice*, Londres, Sweet & Maxwell.

Capítulo 10

El Emam, K. y Álvarez, C. (2015), «A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques», *International Data Privacy Law*, Vol. 5, No. 1, pp. 73-87.

Mayer-Schönberger, V. y Cate, F. (2013), «Notice and consent in a world of Big Data», *International Data Privacy Law*, Vol. 3, No. 2, pp. 67-73.

Rubistein, I. (2013), «Big Data: The End of Privacy or a New Beginning?», *International Data Privacy Law*, Vol. 3, No. 2, pp. 74-87.



Jurisprudencia

Jurisprudencia seleccionada del Tribunal Europeo de Derechos Humanos

Acceso a los datos personales

Gaskin contra Reino Unido, n.º 10454/83, 7 de julio de 1989
Godelli contra Italia, n.º 33783/09, 25 de septiembre de 2012
K.H. y otros contra Eslovaquia, n.º 32881/04, 28 de abril de 2009
Leander contra Suecia, n.º 9248/81, 26 de marzo de 1987
M.K. contra Francia, n.º 19522/09, 18 de abril de 2013
Odièvre contra Francia [GS], n.º 42326/98, 13 de febrero de 2003

Ponderación de la protección de datos con la libertad de expresión y el derecho a la información

Axel Springer AG contra Alemania [GS], n.º 39954/08, 7 de febrero de 2012
Bohlen contra Alemania, n.º 53495/09, 19 de febrero de 2015
Couderc y Hachette Filipacchi Associés contra Francia [GS], n.º 40454/07, 10 de noviembre de 2015
Magyar Helsinki Bizottság contra Hungría [GS], n.º 18030/11, 8 de noviembre de 2016
Müller y otros contra Suiza, n.º 10737/84, 24 de mayo de 1988
Vereinigung bildender Künstler contra Austria, n.º 68345/01, 25 de enero de 2007
Von Hannover contra Alemania (n.º 2) [GS], números 40660/08 y 60641/08, 7 de febrero de 2012

Satakunnan Markkinapörssi Oy y Satamedia Oy contra Finlandia [GS], n.º 931/13, 27 de junio de 2017

Ponderación entre la protección de datos y la libertad de religión

Sinan Işık contra Turquía, n.º 21924/05, 2 de febrero de 2010

Desafíos de la protección de datos en línea

K.U. contra Finlandia, n.º 2872/02, 2 de diciembre de 2008

Consentimiento del interesado

Elberte contra Letonia, n.º 61243/08, 13 de enero de 2015
Sinan Işık contra Turquía, n.º 21924/05, 2 de febrero de 2010
Y contra Turquía, n.º 648/10, 17 de febrero de 2015

Correspondencia

Amann contra Suiza [GS], n.º 27798/95, 16 de febrero de 2000
Association for European Integration and Human Rights y Ekimdzhiev contra Bulgaria, n.º 62540/00, 28 de junio de 2007
Bernh Larsen Holding AS y otros contra Noruega, n.º 24117/08, 14 de marzo de 2013
Cemalettin Canli contra Turquía, n.º 22427/04, 18 de noviembre de 2008
D.L. contra Bulgaria, n.º 7472/14, 19 de mayo de 2016
Dalea contra Francia, n.º 964/07, 2 de febrero de 2010
Gaskin contra Reino Unido, n.º 10454/83, 7 de julio de 1989
Haralambie contra Rumanía, n.º 21737/03, 27 de octubre de 2009
Khelili contra Suiza, n.º 16188/07, 18 de octubre de 2011
Leander contra Suecia, n.º 9248/81, 26 de marzo de 1987
Malone contra Reino Unido, n.º 8691/79, 2 de agosto de 1984
Rotaru contra Rumanía [GS], n. 28341/95, 4 de mayo de 2000
S. y Marper contra Reino Unido [GS], números 30562/04 y 30566/04, 4 de diciembre de 2008
Shimovolos contra Rusia, n.º 30194/09, 21 de junio de 2011
Silver y otros *contra Reino Unido*, números 5947/72, 6205/73, 7052/75, 7061/75, 7107/75 y 7113/75, 25 de marzo de 1983
The Sunday Times contra Reino Unido, n.º 6538/74, 26 de abril de 1979

Bases de datos de antecedentes penales

Aycaguer contra Francia, n.º 8806/12, 22 de junio de 2017
B.B. contra Francia, n.º 5335/06, 17 de diciembre de 2009
Brunet contra Francia, n.º 21010/10, 18 de septiembre de 2014
M.K. contra Francia, n.º 19522/09, 18 de abril de 2013
M.M. contra Reino Unido, n.º 24029/07, 13 de noviembre de 2012

Seguridad de los datos

Haralambie contra Rumanía, n.º 21737/03, 27 de octubre de 2009
K.H. y otros contra Eslovaquia, n.º 32881/04, 28 de abril de 2009

Bases de datos de ADN

S. y Marper contra Reino Unido [GS], números 30562/04 y 30566/04, 4 de diciembre de 2008

Datos de GPS

Uzun contra Alemania, n.º 35623/05, 2 de septiembre de 2010

Datos de salud

Avilkina y otros contra Rusia, n.º 1585/09, 6 de junio de 2013
Biriuk contra Lituania, n.º 23373/03, 25 de noviembre de 2008
I contra Finlandia, n.º 20511/03, 17 de julio de 2008
L.H. contra Letonia, n.º 52019/07, 29 de abril de 2014
L.L. contra Francia, n.º 7508/02, 10 de octubre de 2006
M.S. contra Suecia, n.º 20837/92, 27 de agosto de 1997
Szuluk contra Reino Unido, n.º 36936/05, 2 de junio de 2009
Y contra Turquía, n.º 648/10, 17 de febrero de 2015
Z contra Finlandia, n.º 22009/93, 25 de febrero de 1997

Identidad

Ciubotaru contra Moldavia, n.º 27138/04, 27 de abril de 2010
Godelli contra Italia, n.º 33783/09, 25 de septiembre de 2012
Odièvre contra Francia [GS], n.º 42326/98, 13 de febrero de 2003

Información relacionada con las actividades profesionales

G.S.B. contra Suiza, n.º 28601/11, 22 de diciembre de 2015.

M.N. y otros contra San Marino, n.º 28005/12, 7 de julio de 2015
Michaud contra Francia, n.º 12323/11, 6 de diciembre de 2012
Niemietz contra Alemania, n.º 13710/88, de 16 de diciembre de 1992

Intervención de las comunicaciones

Amann contra Suiza [GS], n.º 27798/95, 16 de febrero de 2000
Brito Ferrinho Bexiga Villa-Nova contra Portugal, n.º 69436/10, 1 de diciembre de 2015
Copland contra Reino Unido, n.º 62617/00, 3 de abril de 2007
Halford contra Reino Unido, n.º 20605/92, 25 de junio de 1997
Iordachi y otros contra Moldavia, n.º 25198/02, de 10 de febrero de 2009
Kopp contra Suiza, n.º 23224/94, 25 de marzo de 1998
Liberty y otros contra Reino Unido, n.º 58243/00, 1 de julio de 2008
Malone contra Reino Unido, n.º 8691/79, 2 de agosto de 1984
Mustafa Sezgin Tanrıkulu contra Turquía, n.º 27473/06, 18 de julio de 2017
Pruteanu contra Rumanía, n.º 30181/05, 3 de febrero de 2015
Szuluk contra Reino Unido, n.º 36936/05, 2 de junio de 2009

Obligaciones para los garantes de obligaciones

B.B. contra Francia, n.º 5335/06, 17 de diciembre de 2009
I contra Finlandia, n.º 20511/03, 17 de julio de 2008
Mosley contra Reino Unido, n.º 48009/08, 10 de mayo de 2011

Datos personales

Amann contra Suiza [GS], n.º 27798/95, 16 de febrero de 2000
Uzun contra Alemania, n.º 35623/05, 2010
Bernh Larsen Holding AS y otros contra Noruega, n.º 24117/08, 14 de marzo de 2013

Fotografías

Sciacca contra Italia, n.º 50774/99, 11 de enero de 2005
Von Hannover contra Alemania, n.º 59320/00, 24 de junio de 2004

Derecho a ser olvidado

Segerstedt-Wiberg y otros contra Suecia, n.º 62332/00, 6 de junio de 2006
Satakunnan Markkinapörssi Oy y Satamedia Oy contra Finlandia [GS], n.º 931/13, 27 de junio de 2017

Derecho de oposición

Leander contra Suecia, n.º 9248/81, 26 de marzo de 1987
M.S. contra Suecia, n.º 20837/92, 27 de agosto de 1997
Mosley contra Reino Unido, n.º 48009/08, 10 de mayo de 2011
Rotaru contra Rumanía [GS], n. 28341/95, 4 de mayo de 2000
Sinan Işık contra Turquía, n.º 21924/05, 2 de febrero de 2010

Categorías sensibles de datos

Brunet contra Francia, n.º 21010/10, 18 de septiembre de 2014
I contra Finlandia, n.º 20511/03, 17 de julio de 2008
Michaud contra Francia, n.º 12323/11, 6 de diciembre de 2012
S. y Marper contra Reino Unido [GS], números 30562/04 y 30566/04, 4 de diciembre de 2008

Supervisión y ejecución (papel de los diferentes actores, incluidas las autoridades de control)

I contra Finlandia, n.º 20511/03, 17 de julio de 2008
K.U. contra Finlandia, n.º 2872/02, 2 de diciembre de 2008
Von Hannover contra Alemania, n.º 59320/00, 24 de junio de 2004
Von Hannover contra Alemania (n.º 2) [GS], números 40660/08 y 60641/08, 7 de febrero de 2012

Métodos de vigilancia

Allan contra Reino Unido, n.º 48539/99, 5 de noviembre de 2002
Association for European Integration and Human Rights y Ekimdzhiev contra Bulgaria, n.º 62540/00, 28 de junio de 2007
Bărbulescu contra Rumanía [GS], n.º 61496/08, 5 de septiembre de 2017
D.L. contra Bulgaria, n.º 7472/14, 19 de mayo de 2016
Dragojević contra Croacia, n.º 68955/11, 15 de enero de 2015
Karabeyoğlu contra Turquía, n.º 30083/10, 7 de junio de 2016
Klass y otros contra Alemania, n.º 5029/71, 6 de septiembre de 1978
Rotaru contra Rumanía [GS], n. 28341/95, 4 de mayo de 2000
Szabó y Vissy contra Hungría, n.º 37138/14, 12 de enero de 2016
Taylor-Sabori contra Reino Unido, n.º 47114/99, 22 de octubre de 2002
Uzun contra Alemania, n.º 35623/05, 2 de septiembre de 2010
Versini-Campinchi y Crasnianski contra Francia, n.º 49176/11, 16 de junio de 2016
Vetter contra Francia, n.º 59842/00, 31 de mayo de 2005

Vukota-Bojić contra Suiza, n.º 61838/10, 18 de octubre de 2016
Roman Zakharov contra Rusia [GS], n.º 47143/06, 4 de diciembre de 2015

Videovigilancia

Köpke contra Alemania, n.º 420/07, 5 de octubre de 2010
Peck contra Reino Unido, n.º 44647/98, 28 de enero de 2003

Muestras de voz

Wisse contra Francia, n.º 71611/01, 20 de diciembre de 2005
P.G. y J.H. contra Reino Unido, n.º 44787/98, 25 de septiembre de 2001

Jurisprudencia seleccionada del Tribunal de Justicia de la Unión Europea

Jurisprudencia relacionada con la Directiva de protección de datos

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contra Rīgas pašvaldības SIA «Rīgas satiksme»*, 4 de mayo de 2017.
[Principio de tratamiento lícito: interés legítimo de un tercero]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni*, 9 de marzo de 2017.
[Derecho a la supresión de los datos personales; derecho a oponerse al tratamiento]

Asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB contra Post- och telestyrelsen* y *Secretary of State for the Home Department contra Tom Watson y otros* [GS], 21 de diciembre de 2016.
[Confidencialidad de las comunicaciones electrónicas; proveedores de servicios de comunicaciones electrónicas; obligación relativa a la conservación general e indiscriminada de los datos de tráfico y localización; ausencia de revisión previa por un tribunal o autoridad administrativa independiente: Carta de los Derechos Fundamentales de la Unión Europea; compatibilidad con el Derecho de la UE]

C-582/14, Patrick Breyer contra Bundesrepublik Deutschland, 19 de octubre de 2016
[Definición de «datos personales»; direcciones de protocolo de internet; conservación de datos por un proveedor de servicios de redes en línea; legislación nacional que no permite que se tenga en cuenta el interés legítimo del responsable del tratamiento]

C-362/14, *Maximillian Schrems contra Data Protection Commissioner* [GS], 6 de octubre de 2015.
[Principio del tratamiento lícito; derechos fundamentales; invalidez de la Decisión de puerto seguro; facultades de las autoridades de control independientes]

C-230/14, *Weltimmo s. r. o. contra Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 de octubre de 2015.
[Facultades de las autoridades de control nacionales]

C-201/14, *Smaranda Bara y otros contra Casa Națională de Asigurări de Sănătate y otros*, 1 de octubre de 2015
[Derecho a ser informado del tratamiento de datos personales]

C-212/13, *František Ryneš contra Úřad pro ochranu osobních údajů*, 11 de diciembre de 2014
[Concepto de «tratamiento de datos» y «responsable del tratamiento»]

C-473/12, *Institut professionnel des agents immobiliers (IPI) contra Geoffrey Englebert y otros*, 7 de noviembre de 2013.
[Derecho a ser informado del tratamiento de datos personales]

T-462/12 R, *Pilkington Group Ltd contra Comisión Europea*, Auto del Presidente del Tribunal General, 11 de marzo de 2013

C-342/12, *Worten – Equipamentos para o Lar SA contra Autoridade para as Condições de Trabalho (ACT)*, 30 de mayo de 2013
[Concepto de «datos personales»; registro del tiempo de trabajo; principios relativos a la calidad de los datos y criterios para hacer que el tratamiento de datos sea legítimo; acceso por la autoridad nacional responsable de vigilar las condiciones de trabajo; obligación del empleador de facilitar el registro de tiempo de trabajo para que se pueda consultar de inmediato]

Asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros* [GS], 8 de abril de 2014.
[Violación del Derecho primario de la UE por la Directiva de conservación de datos; tratamiento lícito; limitación de la finalidad y de la conservación]

C-288/12, *Comisión Europea contra Hungría* [GS], 8 de abril de 2014
[Legitimidad de la destitución del supervisor nacional de protección de datos]

Asuntos acumulados C-141/12 y C-372/12, *YS contra Minister voor Immigratie, Integratie en Asiel, y Minister vor Immigratie, Integratie en Asiel contra M y S*, 17 de julio de 2014.
[Alcance del derecho de acceso de un interesado; protección de las personas físicas con respecto al tratamiento de datos personales; concepto de «datos personales»; datos relativos al solicitante de un permiso de residencia y análisis jurídico contenido

en un documento administrativo preparatorio de la decisión; Carta de los Derechos Fundamentales de la Unión Europea]

C-131/12, *Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* [GS], 13 de mayo de 2014

[Obligaciones de los proveedores de motores de búsqueda de abstenerse, a petición del interesado, de mostrar datos personales en los resultados de búsqueda; aplicabilidad de la Directiva sobre protección de datos; concepto de «tratamiento de datos»; significado de «responsables del tratamiento»; ponderación de la protección de datos con la libertad de expresión; el derecho a ser olvidado]

C-614/10, *Comisión Europea contra República de Austria* [GS], 16 de octubre de 2012

[Independencia de una autoridad nacional de control]

Asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, 24 de noviembre de 2011

[Aplicación correcta del artículo 7, letra f), de la Directiva de protección de datos, «intereses legítimos de otras personas», en la legislación nacional]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) contra Netlog NV*, 16 de febrero de 2012

[Obligación de los proveedores de redes sociales de prevenir el uso ilícito de las obras musicales y audiovisuales por parte de los usuarios de la red]

C-70/10, *Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 de noviembre de 2011

[Sociedad de la información; derechos de autor; internet; programas informáticos «*peer-to-peer*»; proveedores de servicios de internet; instalación de un sistema de filtrado de las comunicaciones electrónicas para evitar que se compartan archivos que violen los derechos de autor; ausencia de una obligación general de vigilar la información transmitida]

C-543/09, *Deutsche Telekom AG contra Bundesrepublik Deutschland*, 5 de mayo de 2011.

[Necesidad de consentimiento renovado]

TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen* [GS], 9 de noviembre de 2010
[Concepto de «datos personales»; proporcionalidad de la obligación legal de publicar datos personales sobre los beneficiarios de ciertos fondos agrícolas de la UE]

C-553/07, *College van burgemeester en wethouders van Rotterdam contra M. E. E. Rijkeboer*, 7 de mayo de 2009
[Derecho de acceso del interesado]

C-518/07, *Comisión Europea contra República Federal de Alemania* [GS], 9 de marzo de 2010
[Independencia de una autoridad nacional de control]

C-73/07, *Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy* [GS], 16 de diciembre de 2008
[Concepto de «actividades periodísticas» en el sentido del artículo 9 de la Directiva de protección de datos]

C-524/06, *Heinz Huber contra Bundesrepublik Deutschland* [GS], 16 de diciembre de 2008
[Legitimidad de la conservación de datos sobre extranjeros en un registro estadístico]

C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU* [GS], 29 de enero de 2008
[Concepto de «datos personales»; obligación de los proveedores de acceso a internet de divulgar la identidad de los usuarios de los programas de intercambio de archivos denominado «KaZaA» a la asociación de protección de la propiedad intelectual]

C-101/01, *Procedimiento penal entablado contra Bodil Lindqvist*, 6 de noviembre de 2003
[Categorías especiales de datos personales]

Asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof contra Österreichischer Rundfunk y otros* y *Christa Neukomm y Joseph Lauermann contra Österreichischer Rundfunk*, 20 de mayo de 2003
[Proporcionalidad de la obligación legal de publicar datos personales sobre los salarios de los empleados de determinadas categorías de las instituciones del sector público]

C-434/16, *Peter Nowak contra Data Protection Commissioner*, Conclusiones de la Abogado General Kokott, 20 de julio de 2017
[Concepto de datos personales; acceso al propio examen; correcciones del examinador]

C-291/12, *Michael Schwarz contra Stadt Bochum*, 17 de octubre de 2013.
[Petición de decisión prejudicial; espacio de libertad, seguridad y justicia; pasaporte biométrico; impresiones dactilares; base jurídica; proporcionalidad]

Jurisprudencia relativa a la Directiva 2016/681

Dictamen 1/15 del Tribunal [GS], 26 de julio de 2017
[Base jurídica; proyecto de acuerdo entre Canadá y la Unión Europea relativo a la transferencia y al tratamiento de datos del registro de nombres de los pasajeros; compatibilidad del proyecto de acuerdo con el artículo 16 del TFUE y con los artículos 7 y 8 y el artículo 52, apartado 1 de la Carta de los Derechos Fundamentales de la Unión Europea]

Jurisprudencia relacionada con el Reglamento de protección de datos de las instituciones de la UE

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) contra Autoridad Europea de Seguridad Alimentaria (EFSA), Comisión Europea*, 16 de julio de 2015
[Acceso a los documentos]

C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd.* [GS], 29 de junio de 2010.
[Acceso a los documentos]

Jurisprudencia relativa a la Directiva 2002/58/CE

C-536/15, *Tele2 (Netherlands) BV y otros contra Autoriteit Consument en Markt (ACM)*, 15 de marzo de 2017
[Principio de no discriminación; puesta a disposición de los datos personales relativos a los abonados para los fines de la prestación de servicios de información sobre números de abonados y guías accesibles al público; consentimiento del abonado; distinción

en función del Estado miembro en el que se presten los servicios de información sobre números de abonados y guías accesibles al público]

Asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB contra Post- och telestyrelsen* y *Secretary of State for the Home Department contra Tom Watson y otros* [GS], 21 de diciembre de 2016.

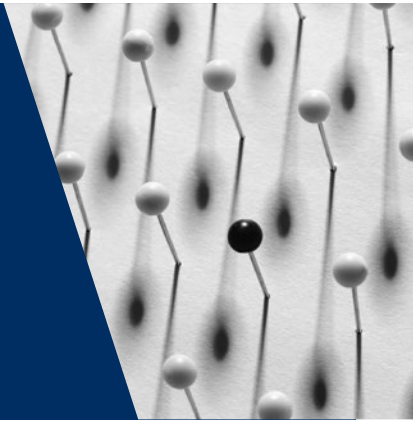
[Confidencialidad de las comunicaciones electrónicas; proveedores de servicios de comunicaciones electrónicas; obligación relativa a la conservación general e indiscriminada de los datos de tráfico y localización; ausencia de revisión previa por un tribunal o autoridad administrativa independiente: Carta de los Derechos Fundamentales de la Unión Europea; compatibilidad con el Derecho de la UE]

C-70/10, *Scarlet Extended SA contra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* 24 de noviembre de 2011

[Sociedad de la información; derechos de autor; internet; programas informáticos «*peer-to-peer*»; proveedores de servicios de internet; instalación de un sistema de filtrado de las comunicaciones electrónicas para evitar que se compartan archivos que violen los derechos de autor; ausencia de una obligación general de vigilar la información transmitida]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB / Perfect Communication Sweden AB*, 19 de abril de 2012.

[Derechos de autor y derechos relacionados; tratamiento de datos por internet; violación de un derecho exclusivo; audiolibros facilitados a través de un servidor FTP por internet por una dirección IP suministrada por un proveedor de servicios de internet; orden judicial dictada contra el proveedor de servicios de internet para que facilite el nombre y la dirección del usuario de la dirección IP]



Índice

Jurisprudencia del Tribunal de Justicia de la Unión Europea

Jurisprudencia del Tribunal Europeo de Derechos Humanos

Jurisprudencia de los órganos jurisdiccionales nacionales

En internet hay mucha información acerca de la Agencia de los Derechos Fundamentales de la Unión Europea. Se puede acceder a ella a través del sitio web de la FRA en: fra.europa.eu

Más información sobre la jurisprudencia del Tribunal Europeo de Derechos Humanos en el sitio web del Tribunal: echr.coe.int. El portal de búsqueda HUDOC permite acceder a sentencias y resoluciones en inglés o francés, así como a traducciones a otros idiomas, resúmenes jurídicos, notas de prensa y otra información sobre el trabajo del Tribunal (https://hudoc.echr.coe.int/spa).

Cómo obtener las publicaciones del Consejo de Europa

La editorial del Consejo de Europa «Council of Europe Publishing» produce obras en todas las esferas de referencia de la organización, incluidos los derechos humanos, ciencia jurídica, salud, ética, asuntos sociales, medio ambiente, educación, cultura, deporte, juventud y patrimonio arquitectónico. Se pueden solicitar libros y publicaciones electrónicas de su extenso catálogo a través de internet (http://book.coe.int/).

Una sala de lectura virtual permite a los usuarios consultar extractos de las principales obras recién publicadas o los textos completos de algunos documentos oficiales de forma gratuita.

En el sitio web de la Oficina de Tratados hay información sobre los Convenios del Consejo de Europa, y puede accederse al texto completo de estos: http://conventions.coe.int/

Ponerse en contacto con la Unión Europea

En persona

En la Unión Europea existen cientos de centros de información Europe Direct. Puede encontrar la dirección del centro más cercano en: https://europa.eu/european-union/contact_es

Por teléfono o por correo electrónico

Europe Direct es un servicio que responde a sus preguntas sobre la Unión Europea. Puede acceder a este servicio:
— marcando el número de teléfono gratuito: 00 800 6 7 8 9 10 11 (algunos operadores pueden cobrar por las llamadas);
— marcando el siguiente número de teléfono: +32 22999696; o
— por correo electrónico: https://europa.eu/european-union/contact_es

Buscar información sobre la Unión Europea

En línea

Puede encontrar información sobre la Unión Europea en todas las lenguas oficiales de la Unión en el sitio web Europa: https://europa.eu/european-union/index_es

Publicaciones de la Unión Europea

Puede descargar o solicitar publicaciones gratuitas y de pago de la Unión Europea en: https://publications.europa.eu/es/publications
Si desea obtener varios ejemplares de las publicaciones gratuitas, póngase en contacto con Europe Direct o su centro de información local (https://europa.eu/european-union/contact_es).

Derecho de la Unión y documentos conexos

Para acceder a la información jurídica de la Unión Europea, incluido todo el Derecho de la Unión desde 1952 en todas las versiones lingüísticas oficiales, puede consultar el sitio web EUR-Lex: http://eur-lex.europa.eu

Datos abiertos de la Unión Europea

El portal de datos abiertos de la Unión Europea (http://data.europa.eu/euodp/es) permite acceder a conjuntos de datos de la Unión. Los datos pueden descargarse y reutilizarse gratuitamente con fines comerciales o no comerciales.

El rápido avance de las tecnologías de la información ha aumentado la necesidad de una protección sólida de los datos personales, y el derecho a dicha protección está garantizado por instrumentos de la Unión Europea (UE) y del Consejo de Europa (CdE). Salvaguardar este importante derecho implica nuevos e importantes retos, a medida que los avances tecnológicos amplían las fronteras de campos tales como la vigilancia, la intervención de las comunicaciones y la conservación de los datos. Este manual está concebido para que los profesionales jurídicos no especializados en protección de datos conozcan este campo emergente del Derecho. En él se ofrece una visión general de los marcos jurídicos aplicables de la UE y del CdE. También se explica la jurisprudencia clave y se resumen sentencias importantes, tanto del Tribunal de Justicia de la Unión Europea (TJUE) como del Tribunal Europeo de Derechos Humanos (TEDH). Además, presenta escenarios hipotéticos que ilustran de forma práctica los diversos problemas encontrados en este campo en constante evolución.

FRA – AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA
Schwarzenbergplatz 11 – 1040 Viena – AUSTRIA
Tel. +43 158030-0 – Fax +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

TRIBUNAL EUROPEO DE DERECHOS HUMANOS CONSEJO DE EUROPA
67075 Estrasburgo Cedex – FRANCIA
Tel. +33 (0) 3 88 41 20 18 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int – @ECHRPublication

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS
Rue Wiertz 60 – 1047 Bruselas – BÉLGICA
Tel. +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

Oficina de Publicaciones de la Unión Europea